GROUPES ET GÉOMÉTRIE, EXERCICES

GROUPES ET GÉOMÉTRIE, EXERCICES

TABLE DES MATIÈRES

1. Exercices, groupes 1
1.1. Relations d'équivalence 1
1.2. Groupe $\mathbb{Z}$ 26
1.3. En construction 44
1.4. Premiers pas 88
1.5. Seconds pas 111
1.6. Actions de groupes, sous-groupes distingués 137
1.7. Groupe des permutations 221
1.8. Autour des théorèmes de Sylow 237
1.9. Structure des groupes abéliens de type fini 293
1.10. Produits semi-directs 314
1.11. Groupes libres 324
1.12. Représentations linéaires des groupes finis 331
1.13. À classer 368
1.14. Groupe des permutations 375
1.15. Autour des théorèmes de Sylow 390
1.16. Structure des groupes abéliens de type fini 447
1.17. Produits semi-directs 468
1.18. Groupes libres 478
1.19. Représentations linéaires des groupes finis 485
1.20. À classer 522

2. Exercices, groupes et géométrie 531
2.1. Groupes et géométrie 531
2.2. Géométrie 586

3. Appendice 2 : Exercices, anneaux et corps 601
3.1. Anneaux et morphismes entre anneaux 602
3.2. L'anneau $\mathbb{Z}$ 609
3.3. Anneau quotient et anneau produit 618

3.4. Anneaux de polynômes 629
3.5. Anneaux et corps 646
3.6. Anneaux principaux, anneaux euclidiens 653

Index 667

Bibliographie 669

CHAPITRE 1

EXERCICES, GROUPES

1.1. Relations d'équivalence

Exercice 1

1. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
2. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
3. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
4. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
5. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?

Éléments de réponse 1 à compléter

1. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1)\}$ ne définit pas une relation d'équivalence sur $\{0, 1, 2\}$.
2. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (2,2)\}$ définit une relation d'équivalence sur $\{0, 1, 2\}$.
3. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,2)\}$ ne définit pas une relation d'équivalence sur $\{0, 1, 2\}$.
4. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2)\}$ ne définit pas une relation d'équivalence sur $\{0, 1, 2\}$.
5. Le graphe $\Gamma = \{(0,0), (0,1), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$ définit une relation d'équivalence sur $\{0, 1, 2\}$.

Exercice 2

1. Le graphe $\Gamma = \{(0,0), (0,1), (1,1), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
2. Le graphe $\Gamma = \{(0,0), (0,1), (0,2), (1,1), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
3. Le graphe $\Gamma = \{(0,0), (0,1), (1,1), (1,2), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?
4. Le graphe $\Gamma = \{(0,0), (0,1), (0,2), (1,1), (1,2), (2,2)\}$ définit-il une relation d'équivalence sur $\{0, 1, 2\}$ (oui ou non et pourquoi) ?

à compléter

Éléments de réponse 2

1. Le graphe $\Gamma = \{(0,0), (0,1), (1,1), (2,2)\}$ définit une relation d'équivalence sur $\{0, 1, 2\}$.
2. Le graphe $\Gamma = \{(0,0), (0,1), (0,2), (1,1), (2,2)\}$ définit une relation d'équivalence sur $\{0, 1, 2\}$.
3. Le graphe $\Gamma = \{(0,0), (0,1), (1,1), (1,2), (2,2)\}$ ne définit pas une relation d'équivalence sur $\{0, 1, 2\}$.
4. Le graphe $\Gamma = \{(0,0), (0,1), (0,2), (1,1), (1,2), (2,2)\}$ ne définit pas une relation d'équivalence sur $\{0, 1, 2\}$.

Exercice 3

Soient E un ensemble fini non vide. Soit x un élément fixé de E.

1. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A = B$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?
2. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \subset B$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?
3. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \cap B = \emptyset$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?
4. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((A \cap B = \emptyset) \vee (A \cup B \neq \emptyset)\Big)$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?

5. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff x \in A \cup B$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?
6. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((x \in A \cap B) \vee (x \in \complement A \cap \complement B)\Big)$$
est-elle une relation d'équivalence sur $\mathcal{P}(E)$?

Éléments de réponse 3

Soient E un ensemble fini non vide. Soit x un élément fixé de E.

1. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A = B$$
est une relation d'équivalence sur $\mathcal{P}(E)$. En effet,
   - ◇ pour tout $A \in \mathcal{P}(E)$ nous avons $A = A$ soit $A\mathcal{R}A$, autrement dit $\mathcal{R}$ est réflexive.
   - ◇ soient $A,\, B \in \mathcal{P}(E)$ tels que $A\mathcal{R}B$, *i.e.* $A = B$, alors $B = A$ c'est-à-dire $B\mathcal{R}A$. En d'autres termes, $\mathcal{R}$ est symétrique.
   - ◇ soient $A,\, B,\, C \in \mathcal{P}(E)$ tels que $A\mathcal{R}B$ et $B\mathcal{R}C$; alors d'une part $A = B$ et d'autre part $B = C$. En particulier $A = C$, c'est-à-dire $A\mathcal{R}C$; ainsi $\mathcal{R}$ est transitive.
2. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \subset B$$
n'est pas une relation d'équivalence sur $\mathcal{P}(E)$. En effet, l'ensemble vide est en relation avec E (c'est-à-dire $\emptyset \subset E$) mais E n'est pas en relation avec l'ensemble vide (*i.e.* $E \not\subset \emptyset$) : la relation $\mathcal{R}$ n'est pas symétrique.
3. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \cap B = \emptyset$$
n'est pas une relation d'équivalence sur $\mathcal{P}(E)$. La relation $\mathcal{R}$ n'est pas réflexive ; en effet E n'est pas en relation avec lui-même puisque $E \cap E = E \neq \emptyset$.
4. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((A \cap B = \emptyset) \vee (A \cup B \neq \emptyset)\Big)$$
est une relation d'équivalence sur $\mathcal{P}(E)$.
5. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff x \in A \cup B$$
n'est pas une relation d'équivalence sur $\mathcal{P}(E)$. En effet, $\mathcal{R}$ n'est pas réflexive : $\emptyset$ n'est pas en relation avec lui-même car $x \notin \emptyset \cup \emptyset = \emptyset$.

6. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((x \in A \cap B) \vee (x \in \complement A \cap \complement B)\Big)$$

est une relation d'équivalence sur $\mathcal{P}(E)$.

Exercice 4

Soient E un ensemble fini non vide. Soit x un élément fixé de E.

1. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A = B$$

est-elle une relation d'ordre sur $\mathcal{P}(E)$?

2. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \subset B$$

est-elle une relation d'ordre sur $\mathcal{P}(E)$?

3. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \big(x \in (A \cap B)\big)$$

est-elle une relation d'ordre sur $\mathcal{P}(E)$?

4. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \big(x \in (A \cup B)\big)$$

est-elle une relation d'ordre sur $\mathcal{P}(E)$?

5. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((A = B) \vee (x \in A \cap B)\Big)$$

est-elle une relation d'ordre sur $\mathcal{P}(E)$?

Éléments de réponse 4

Soient E un ensemble fini non vide. Soit x un élément fixé de E.

1. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A = B$$

est une relation d'ordre sur $\mathcal{P}(E)$.

2. La relation $\mathcal{R}$ définie par

$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff A \subset B$$

est une relation d'ordre sur $\mathcal{P}(E)$.

3. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \big(x \in (A \cap B)\big)$$
n'est pas une relation d'ordre sur $\mathcal{P}(E)$.
4. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \big(x \in (A \cup B)\big)$$
n'est pas une relation d'ordre sur $\mathcal{P}(E)$.
5. La relation $\mathcal{R}$ définie par
$$\forall\, A,\, B \in \mathcal{P}(E) \quad A\mathcal{R}B \iff \Big((A = B) \vee (x \in A \cap B)\Big)$$
est une relation d'ordre sur $\mathcal{P}(E)$.

Exercice 5

1. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n \,|\, m$$
Est-ce une relation d'équivalence sur $\mathbb{N}$?
2. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 = m^2.$$
Est-ce une relation d'équivalence sur $\mathbb{N}$?
3. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm + 2n.$$
Est-ce une relation d'équivalence sur $\mathbb{N}$?
4. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 - m^2 = 2nm + 2n.$$
Est-ce une relation d'équivalence sur $\mathbb{N}$?
5. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm.$$
Est-ce une relation d'équivalence sur $\mathbb{N}$?

Éléments de réponse 5

1. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n \,|\, m$$
n'est pas une relation d'équivalence sur $\mathbb{N}$.

2. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 = m^2.$$
est une relation d'équivalence sur $\mathbb{N}$.
3. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm + 2n.$$
n'est pas une relation d'équivalence sur $\mathbb{N}$.
4. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 - m^2 = 2nm + 2n.$$
n'est pas une relation d'équivalence sur $\mathbb{N}$.
5. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n^2 + m^2 = 2nm.$$
est une relation d'équivalence sur $\mathbb{N}$.

Exercice 6

1. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n - m \geq 1.$$
Est-ce une relation d'ordre sur $\mathbb{N}$?
2. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n - m \leq 1.$$
Est-ce une relation d'ordre sur $\mathbb{N}$?
3. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m^2 = k - n^2.$$
Est-ce une relation d'ordre sur $\mathbb{N}$?
4. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m^2 = k + n^2.$$
Est-ce une relation d'ordre sur $\mathbb{N}$?
5. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m = kn.$$
Est-ce une relation d'ordre sur $\mathbb{N}$?

Éléments de réponse 6

1. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n - m \geq 1.$$
n'est pas une relation d'ordre sur $\mathbb{N}$.
2. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff n - m \leq 1.$$
n'est pas une relation d'ordre sur $\mathbb{N}$.
3. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m^2 = k - n^2.$$
n'est pas une relation d'ordre sur $\mathbb{N}$.
4. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m^2 = k + n^2.$$
est une relation d'ordre sur $\mathbb{N}$.
5. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par
$$\forall\, n,\, m \in \mathbb{N} \quad n\mathcal{R}m \iff \exists\, k \in \mathbb{N},\, m = kn.$$
est une relation d'ordre sur $\mathbb{N}$.

Exercice 7

1. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par : $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff x \leq y$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?
2. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par : $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff x^2 \leq y^2$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?
3. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff \lfloor x \rfloor \leq \lfloor y \rfloor$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?
4. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff \lfloor x \rfloor = \lfloor y \rfloor$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?
5. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff \sin(x) = \sin(y)$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?

6. Considérons la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par $\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff x - y \in \mathbb{N}$.
   a) Représenter graphiquement dans $\mathbb{R}^2$ le graphe de $\mathcal{R}$.
   b) $\mathcal{R}$ est-elle une relation d'ordre ? $\mathcal{R}$ est-elle une relation d'équivalence ?

Éléments de réponse 7

Exercice 8

1. Considérons la relation $\mathcal{R}$ sur $\mathbb{R}$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff x < y.$$
Est-ce une relation d'ordre sur $\mathbb{R}$?
2. Considérons la relation $\mathcal{R}$ sur $\mathbb{R}$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff \exp(x) \leq \exp(y).$$
Est-ce une relation d'ordre sur $\mathbb{R}$?
3. Considérons la relation $\mathcal{R}$ sur $\mathbb{R}$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff |x| \leq |y|.$$
Est-ce une relation d'ordre sur $\mathbb{R}$?
4. Considérons la relation $\mathcal{R}$ sur $\mathbb{R}$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff (x - y) \in \mathbb{N}.$$
Est-ce une relation d'ordre sur $\mathbb{R}$?
5. Considérons la relation $\mathcal{R}$ sur $\mathbb{R}$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x\mathcal{R}y \iff (x - y) \in \mathbb{Z}.$$
Est-ce une relation d'ordre sur $\mathbb{R}$?

Éléments de réponse 8

Exercice 9

1. Considérons sur $\mathbb{C}$ la relation $\mathcal{R}$ définie par
$$\forall\, z,\, z' \in \mathbb{C} \quad z\mathcal{R}z' \iff |z| = |z'|.$$
Est-ce une relation d'équivalence sur $\mathbb{C}$?
2. Considérons sur $\mathbb{C}$ la relation $\mathcal{R}$ définie par
$$\forall\, z,\, z' \in \mathbb{C} \quad z\mathcal{R}z' \iff \left|\frac{z}{z'}\right| = 1.$$
Est-ce une relation d'équivalence sur $\mathbb{C}$?

3. Considérons sur $\mathbb{C}$ la relation $\mathcal{R}$ définie par
$$\forall\, z,\, z' \in \mathbb{C} \quad z\mathcal{R}z' \iff \exp(z) = \exp(z').$$
Est-ce une relation d'équivalence sur $\mathbb{C}$?
4. Considérons sur $\mathbb{C}$ la relation $\mathcal{R}$ définie par
$$\forall\, z,\, z' \in \mathbb{C} \quad z\mathcal{R}z' \iff |z - z'| = 1.$$
Est-ce une relation d'équivalence sur $\mathbb{C}$?
5. Considérons sur $\mathbb{C}$ la relation $\mathcal{R}$ définie par
$$\forall\, z,\, z' \in \mathbb{C} \quad z\mathcal{R}z' \iff |\exp(z - z')| = 1$$
Est-ce une relation d'équivalence sur $\mathbb{C}$?

Éléments de réponse 9

Exercice 10

Nous définissons la relation $\mathcal{R}$ sur $\mathbb{N}$ par
$$\forall\, m,\, n \in \mathbb{N}^*, \quad m\mathcal{R}n \iff \Big(\exists\, k \in \mathbb{N}^*,\, m^k = n\Big)$$
Démontrer que $\mathcal{R}$ est une relation d'ordre.

Éléments de réponse 10

Exercice 11

Une relation binaire $\mathcal{R}$ dans un ensemble E est dite *circulaire* si pour tout $(a, b, c) \in E$
$$\Big(a\mathcal{R}b \text{ et } b\mathcal{R}c\Big) \Longrightarrow c\mathcal{R}a.$$
Montrer qu'une relation circulaire et réflexive est une relation d'équivalence.

Éléments de réponse 11

Exercice 12

Soient E et F deux ensembles ; soit f une application de E dans F. Définissons sur E la relation $\mathcal{R}$ par
$$\forall x,\, y \in E \quad x\mathcal{R}y \iff f(x) = f(y).$$
1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Soit Γ l'ensemble des couples $(\overline{x}, f(x))$ où x parcourt l'ensemble E. Montrer que Γ est le graphe d'une application de l'ensemble quotient $E/\mathcal{R}$ dans F. Nous notons g cette application.
3. Montrer que g est une application injective.
4. Soit f l'application de $\mathbb{Z}$ dans $\mathbb{N}$ qui à $n \in \mathbb{Z}$ associe n^2. Décrire $\overline{0}$ et $\overline{1}$.

5. Soit f l'application de $\mathbb{C}$ dans $\mathbb{C}$ qui à $z \in \mathbb{C}$ associe $f(z) = z^4$. Décrire $\overline{0}$ et $\overline{1}$.
6. Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à $x \in \mathbb{R}$ associe sa partie entière. Décrire $\overline{0}$ et $\overline{1}$.
7. Soit f l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à $x \in \mathbb{R}$ associe sa partie décimale. Décrire $\overline{0}$ et $\overline{\frac{1}{2}}$.

Éléments de réponse 12

Exercice 13

1. Sur $E = \mathbb{Z}$ considérons la relation $\mathcal{R}$ définie par : $x\mathcal{R}y \iff x = -y$. La relation $\mathcal{R}$ est-elle réflexive ? symétrique ? antisymétrique ? transitive ? une relation d'ordre ? une relation d'équivalence ?
2. Sur $E = \mathbb{R}$ considérons la relation $\mathcal{R}$ définie par : $x\mathcal{R}y \iff \cos^2 x + \sin^2 y = 1$. La relation $\mathcal{R}$ est-elle réflexive ? symétrique ? antisymétrique ? transitive ? une relation d'ordre ? une relation d'équivalence ?
3. Sur $E = \mathbb{N}$ considérons la relation $\mathcal{R}$ déifnie par : $x\mathcal{R}y \iff \exists\, p,\ q \geq 1,\ y = pxq$ (p et q sont des entiers). La relation $\mathcal{R}$ est-elle réflexive ? symétrique ? antisymétrique ? transitive ? une relation d'ordre ? une relation d'équivalence ?

Éléments de réponse 13

1. La relation $\mathcal{R}$ n'est pas réflexive, car 1 n'est pas en relation avec lui-même. En effet, $1 \neq -1$.

   La relation est symétrique, car $x = -y \iff y = -x$

   Elle n'est pas antisymétrique, car $1\mathcal{R} - 1$ et $-1\mathcal{R}1$, alors que $1 \neq -1$.

   Elle n'est pas transitive ; en effet, on a $1\mathcal{R} - 1$, $-1\mathcal{R}1$ mais 1 n'est pas en relation avec lui-même.

   Cette relation n'est ni une relation d'équivalence, ni une relation d'ordre.

2. De la formule $\cos^2 x + \sin^2 x = 1$, on déduit que la relation $\mathcal{R}$ est réflexive.

   Elle est aussi symétrique. En effet, si $x\mathcal{R}y$, *i.e.* $\cos^2 x + \sin^2 y = 1$, alors on a

$$\sin^2 x + \cos^2 x + \cos^2 y + \sin^2 y = (\cos^2 x + \sin^2 y) + (\cos^2 y + \sin^2 x) = 1 + (\cos^2 y + \sin^2 x)$$

   d'une part, et $\sin^2 x + \cos^2 x + \cos^2 y + \sin^2 y = 1 + 1 = 2$ d'autre part, ce qui entraîne bien $\cos^2 y + \sin^2 x = 1$ et donc la relation est symétrique.

   Elle n'est pas antisymétrique, car $0\mathcal{R}2\pi$ et $2\pi\mathcal{R}0$ alors que $0 \neq 2\pi$.

   Elle est transitive. Si xRy et yRz, on a $\cos^2 x + \sin^2 y = 1$ et $\cos^2 y + \sin^2 z = 1$ soit en sommant $\cos^2 x + (\cos^2 y + \sin^2 y) + \sin^2 z = 2$ ce qui implique $\cos^2 x + \sin^2 z = 1$.

   Étant donné que $\mathcal{R}$ est réflexive, symétrique et transitive c'est une relation d'équivalence.

3. La relation est réflexive (prendre $p = q = 1$), elle n'est pas symétrique car si $x\mathcal{R}y$, on a forcément $x \leq y$. Ainsi, on a $2\mathcal{R}4$ (prendre $p = 2$, $q = 1$), alors qu'on n'a pas $4\mathcal{R}2$.

   La relation est antisymétrique : si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors on a $x \leq y$ et $y \leq x$ et donc $x = y$.

   Enfin, la relation est transitive. Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors il existe des entiers p, q, a, $b \geq 1$ tels que $y = pxq$ et $z = ayb$. On en déduit $z = a(pxq)b = (apb)xbq$ et donc $x\mathcal{R}z$.

   La relation est une relation d'ordre.

Exercice 14

La relation $\mathcal{R}$ d'orthogonalité entre deux droites du plan est-elle symétrique ? réflexive ? transitive ?

Éléments de réponse 14

La relation $\mathcal{R}$

- ◇ n'est pas réflexive : une droite n'est pas orthogonale à elle-même.
- ◇ est symétrique : si $\mathcal{D}$ est orthogonale à $\mathcal{D}'$, alors $\mathcal{D}'$ est orthgonale à $\mathcal{D}$.
- ◇ n'est pas transitive : si $\mathcal{D}$ est orthogonale à $\mathcal{D}'$ et si $\mathcal{D}'$ est orthogonale à $\mathcal{D}''$, alors $\mathcal{D}$ et $\mathcal{D}''$ ne sont pas orthogonales (elles sont parallèles ou confondues).

Exercice 15

Sur $\mathbb{R}^2$, nous définissons la relation $\mathcal{R}$ par $(x, y)\mathcal{R}(x', y') \iff x = x'$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Déterminer la classe d'équivalence d'un élément $(x_0, y_0) \in \mathbb{R}^2$.

Éléments de réponse 15

1. La relation $\mathcal{R}$ est une relation d'équivalence. En effet, elle est
   - ◇ réflexive : $(x, y)\mathcal{R}(x, y)$ car $x = x$;
   - ◇ symétrique : si $(x, y)\mathcal{R}(x', y')$, alors $x = x'$ ce qui s'écrit aussi $x' = x$ et qui est équivalent à $(x', y')\mathcal{R}(x, y)$.
   - ◇ transitive : si $(x, y)\mathcal{R}(x', y')$ et si $(x', y')\mathcal{R}(x'', y'')$, alors on a $x = x'$ d'une part et $x' = x''$ d'autre part, donc $x = x''$ ce qui entraîne $(x, y)\mathcal{R}(x'', y'')$.
2. Chercher la classe d'équivalence de (x_0, y_0), c'est déterminer tous les couples (x, y) tels que $(x, y)\mathcal{R}(x_0, y_0)$. Mais

$$(x, y)\mathcal{R}(x_0, y_0) \iff x = x_0,$$

   autrement dit, x doit être égal à x_0 et y peut être quelconque. Nous en déduisons que la classe d'équivalence de (x_0, y_0) pour la relation d'équivalence $\mathcal{R}$ est $\{(x_0, y) \,|\, y \in \mathbb{R}\}$.

Exercice 16

Nous définissons sur $\mathbb{R}$ la relation $x\mathcal{R}y$ si et seulement si $x^2 - y^2 = x - y$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Calculer la classe d'équivalence d'un élément x de $\mathbb{R}$. Combien y a-t-il d'éléments dans cette classe ?

Éléments de réponse 16

1. Il suffit de remarquer que $x\mathcal{R}y \iff x^2 - x = y^2 - y \iff f(x) = f(y)$ avec $f\colon x \mapsto x^2 - x$. Il est alors aisé de vérifier en appliquant la définition que $\mathcal{R}$ est une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive.
2. Soit $x \in \mathbb{R}$. On cherche les éléments y de $\mathbb{R}$ tels que $x\mathcal{R}y$. On doit donc résoudre l'équation (en y) $x^2-y^2 = x-y$. Elle se factorise en $(x-y)(x+y)-(x-y) = 0 \iff (x-y)(x+y-1) = 0$. Ses solutions sont $y = x$ et $y = 1 - x$. La classe de x est donc égale à $\{x,\, 1 - x\}$. Elle est constituée de deux éléments, sauf si $x = 1 - x \iff x = \frac{1}{2}$. Dans ce cas, elle est égale à $\left\{\frac{1}{2}\right\}$.

Exercice 17

On munit l'ensemble $E = \mathbb{R}^2$ de la relation $\mathcal{R}$ définie par

$$(x, y)\mathcal{R}(x', y') \iff \exists\, a > 0,\ \exists\, b > 0 \text{ tels que } x' = ax \text{ et } y' = by.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Donner la classe d'équivalence des éléments $A = (1, 0)$, $B = (0, -1)$ et $C = (1, 1)$ de $\mathbb{R}^2$.
3. Déterminer les classes d'équivalence de $\mathcal{R}$.

Éléments de réponse 17

1. Nous vérifions les trois propriétés d'une relation d'équivalence :
   - ◇ $\mathcal{R}$ est symétrique : si $(x, y)\mathcal{R}(x', y')$, alors il existe a, $b > 0$ tels que $x' = ax$ et $y' = by$. Mais alors, $x = 1ax'$ et $y = 1by'$, avec $1a > 0$ et $1b > 0$ donc $(x', y')\mathcal{R}(x, y)$.
   - ◇ $\mathcal{R}$ est réflexive : on a en effet $x = 1 \cdot x$ et $y = 1 \cdot y$.
   - ◇ $\mathcal{R}$ est transitive : si $(x, y)\mathcal{R}(x', y')$ et si $(x', y')\mathcal{R}(x'', y'')$, alors il existe a, b, c, $d > 0$ tels que $x' = ax$, $y' = by$, $x'' = cx'$ et $y'' = dy'$. Mais alors, $x'' = (ac)x$ et $y'' = (bd)y$ avec $ac > 0$ et $bd > 0$. Nous en déduisons que $(x, y)\mathcal{R}(x'', y'')$.
2. Nous avons $(x, y)\mathcal{R}(1, 0)$ si et seulement si $(1, 0)\mathcal{R}(x, y)$ si et seulement s'il existe $a > 0$ et $b > 0$ tels que $x = a \times 1$ et $y = b \times 0 = 0$. Ainsi, la classe d'équivalence de $(1, 0)$ est $]0, +\infty[\times\{0\}$. Nous démontrons de la même façon que la classe d'équivalence de $(0, -1)$ est $\{0\}\times]-\infty, 0[$ et celle de $(1, 1)$ est $]0, +\infty[\times]0, +\infty[$.

3. La question précédente suggère qu'il y a exactement neuf classes d'équivalence : celles associées aux quatre quarts de plan, celles associées aux quatre demi-droites construites à partir des axes et du point O, et le point $(0,0)$ lui-même. Précisément, ces neuf classes d'équivalence sont
   - ◇ les classes d'équivalence respectives de $(1,1)$, $(1,-1)$, $(-1,-1)$, $(-1,1)$, à savoir respectivement $]0,+\infty[\times]0,+\infty[$, $]0,+\infty[\times]-\infty,0[$, $]-\infty,0[\times]-\infty,0[$ et $]-\infty,0[\times]0,+\infty[$.
   - ◇ les classes d'équivalence respectives de $(1,0)$, $(-1,0)$, $(0,1)$ et $(0,-1)$, à savoir respectivement $]0,+\infty[\times\{0\}$, $]-\infty,0[\times\{0\}$, $\{0\}\times]0,+\infty[$, $\{0\}\times]-\infty,0[$.
   - ◇ la classe d'équivalence de $(0,0)$, à savoir $\{(0,0)\}$.

   Remarquons que ces neuf ensmbles constituent bien une partition de $\mathbb{R}^2$, ce qui prouve que l'on a trouvé toutes les classes d'équivalence.

Exercice 18

Soit E un ensemble. On définit sur l'ensemble $\mathcal{P}(E)$ des parties de E la relation suivante : $A\mathcal{R}B$ si $A = B$ ou $A = \complement B$, où $\complement B$ désigne le complémentaire de B (dans E). Démontrer que $\mathcal{R}$ est une relation d'équivalence.

Éléments de réponse 18

Il suffit de vérifier que la définition d'une relation d'équivalence est satisfaite. Considérons trois parties A, B et C de E. Tout d'abord, on a bien $A\mathcal{R}A$: en effet, on a $A = A$. D'autre part, si $A\mathcal{R}B$, alors on distingue deux cas. Ou bien $A = B$, et dans ce cas $B = A$ et $B\mathcal{R}A$. Ou bien $A = \complement B$, mais dans ce cas, $B = \complement A$, et on a encore $B\mathcal{R}A$. Enfin, si $A\mathcal{R}B$ et $B\mathcal{R}C$, on peut distinguer quatre cas :

- ◇ Si $A = B$ et $B = C$, alors $A = C$.
- ◇ Si $A = B$ et $B = \complement C$, alors $A = \complement C$.
- ◇ Si $A = \complement B$ et $B = C$, alors $A = \complement C$.
- ◇ Si $A = \complement B$ et $B = \complement C$, alors $A = C$.

Dans tous les cas, on a bien $A\mathcal{R}C$. La relation $\mathcal{R}$ est symétrique, réflexive et transitive. Il s'agit bien d'une relation d'équivalence.

Exercice 19

On définit sur $\mathbb{Z}$ la relation $x\mathcal{R}y$ si et seulement si $x + y$ est pair.

1. Montrer qu'on définit ainsi une relation d'équivalence.
2. Quelles sont les classes d'équivalence de cette relation ?

Éléments de réponse 19

1. La relation est

- ◇ réflexive, car $x + x = 2x$ est pair ;
- ◇ symétrique, car $x + y = y + x$ et donc si $x + y$ est pair, $y + x$ est pair ;
- ◇ transitive, car si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x + y = 2k$ et $y + z = 2\ell$ pour des entiers k et ℓ. En effectuant la somme des ces deux égalités on trouve $x + 2y + z = 2k + 2\ell$, soit $x + z = 2(k + \ell - y)$, *i.e.* $x + z$ est pair.

2. Pour déterminer les classes d'équivalence de $\mathcal{R}$, il suffit de trouver une famille (E_i) d'ensembles tels que :
   - ◇ la réunion des E_i est $\mathbb{Z}$;
   - ◇ les E_i sont deux à deux disjoints ;
   - ◇ si x, y appartiennent au même E_i, alors $x\mathcal{R}y$; si x est dans E_i et y est dans E_j avec $i \neq j$, alors x n'est pas en relation avec y.

   Ici, on peut constater que tous les éléments en relation avec 0 sont les entiers pairs, tandis que tous les entiers en relation avec 1 sont les entiers impairs. Puisque l'ensemble des entiers pairs et des entiers impairs forme une partition de $\mathbb{Z}$, on en déduit que ces deux ensembles sont exactement les deux classes d'équivalence de la relation.

Exercice 20

Soient E un ensemble et $A \in \mathcal{P}(E)$. Deux parties B et C de E sont en relation, noté $B\mathcal{R}C$, si $B\Delta C \subset A$. Rappelons que

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = (A \cap \complement B) \cup (B \cap \complement A).$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence
2. Soit $B \in \mathcal{P}(E)$. Montrer que la classe de B est $\{(B \cap \complement A) \cup K \mid K \in \mathcal{P}(A)\}$.

Éléments de réponse 20

1. La relation $\mathcal{R}$ est
   - ◇ symétrique (car $B\Delta C = C\Delta B$) ;
   - ◇ réflexive, car $B\Delta B = \emptyset \subset A$;
   - ◇ transitive : si $B\Delta C \subset A$ et $C\Delta D \subset A$, alors $B\Delta D \subset A$. En effet, prenons $x \in B$ tel que $x \notin D$. Alors ou bien $x \notin C$ et dans ce cas $x \in A$ car $x \in B\Delta C$. Ou bien $x \in C$ et dans ce cas, $x \in A$ puisque $x \in C\Delta D$. On traite de façon symétrique l'inclusion $D \setminus B \subset A$.
2. Il y a deux choses à faire :

◇ Montrer que si C est de la forme $(B \cap \complement A) \cup K$, alors $B\mathcal{R}C$.

◇ Montrer que si $B\mathcal{R}C$, alors il existe K tel que $(B \cap \complement A) \cup K$.

D'abord, si $C = (B \cap \complement A) \cup K$, avec $K \subset A$, prouvons que $B\Delta C \subset A$. Prenons d'abord $x \in B$ tel que $x \notin C$. Alors $x \notin B \cap \complement A$, et donc $x \notin \complement A$, c'est-à-dire $x \in A$. Si maintenant $x \in C$ et $x \notin B$, alors $x \in K$ et donc $x \in A$. Réciproquement, considérons $C \in \mathcal{P}(E)$ tel que $B\Delta C \subset A$. Posons $K = C \cap A$ et prouvons que $C = (B \cap \complement A) \cup K$.

Prenons $x \in C$. Si $x \in A$, alors $x \in C \cap A \subset K$ et c'est bon. Si $x \notin A$, alors $x \in B$ puisque $C \setminus B \subset A$. En particulier, $x \in (B \cap \complement A)$ et c'est bon là aussi. Prenons $x \in (B \cap \complement A) \cup K$. Si $x \in K = C \cap A$, alors $x \in C$. Sinon, $x \in B \cap \complement A$, et donc $x \in C$, sinon $x \in B \setminus C$ et $x \in \complement A$, ce qui contredit que $B\Delta C \subset A$.

Exercice 21

Soit E un ensemble non vide. Soit $\Omega \subset \mathcal{P}(E)$ non vide vérifiant la propriété suivante : $\forall\, X, Y \in \Omega, \exists Z \in \Omega, Z \subset (X \cap Y)$. Considérons sur $\mathcal{P}(E)$ la relation $\mathcal{R}$ définie par

$$A\mathcal{R}B \iff \exists\, X \in \Omega,\ X \cap A = X \cap B.$$

1. Montrer que $\mathcal{R}$ définit une relation d'équivalence sur $\mathcal{P}(E)$.
2. Quelles sont les classes d'équivalence de $\emptyset$ et de E ?

Éléments de réponse 21

1. Vérifions les trois propriétés d'une relation d'équivalence :
   - ◇ $\mathcal{R}$ est symétrique : $A\mathcal{R}B \iff \exists\, X \in \Omega,\ X \cap A = X \cap B \iff \exists\, X \in \Omega,\ X \cap B = X \cap A \iff B\mathcal{R}A$.
   - ◇ $\mathcal{R}$ est réflexive : soit $A \in \mathcal{P}(E)$, soit $X \in \Omega$, alors nous avons bien $X \cap A = X \cap A$ et donc $A\mathcal{R}A$.
   - ◇ $\mathcal{R}$ est transitive : prenons A, B, $C \in \mathcal{P}(E)$ tels que $A\mathcal{R}B$ et $B\mathcal{R}C$. Alors d'une part
   $$A\mathcal{R}B \iff \exists\, X \in \Omega,\ X \cap A = X \cap B$$
   et d'autre part
   $$B\mathcal{R}C \iff \exists\, Y \in \Omega,\ Y \cap B = Y \cap C.$$
   Soit $Z \in \Omega$ tel que $Z \subset X \cap Y$. Alors on a $Z \cap X = Z$ et $Z \cap Y = Z$. De cela, nous tirons

$$Z \cap A = Z \cap X \cap A = Z \cap X \cap B = Z \cap B = Z \cap Y \cap B = Z \cap Y \cap C = Z \cap C.$$

   Ceci prouve bien que $A\mathcal{R}C$ et que $\mathcal{R}$ est une relation d'équivalence.
2. Cherchons ensuite la classe d'équivalence de $\emptyset$. Nous avons
$$A\mathcal{R}\emptyset \iff \exists\, X \in \Omega,\ A \cap X = \emptyset \cap X = \emptyset.$$
La classe d'équivalence de $\emptyset$ est donc constituée des parties A de E disjointes d'au moins un élément de Ω.

Cherchons enfin la classe d'équivalence de E. Nous avons

$$A\mathcal{R}E \iff \exists\, X \in \Omega,\ A \cap X = E \cap X = X.$$

La classe d'équivalence de E est donc constituée des parties A de E qui contiennent au moins un élément de Ω.

Exercice 22

On définit la relation $\mathcal{R}$ sur $\mathbb{N}^*$ par $p\mathcal{R}q \iff \exists\, k \in \mathbb{N}^*,\ q = pk$.

1. Montrer que $\mathcal{R}$ définit un ordre partiel sur $\mathbb{N}^*$.
2. Déterminer les majorants de $\{2, 3\}$ pour cet ordre.

Éléments de réponse 22

1. La relation est
   - ◇ réflexive : $p\mathcal{R}p$ puisque $p = p \times 1$ pour tout $p \in \mathbb{N}^*$;
   - ◇ antisymétrique : si $p\mathcal{R}q$ et $q\mathcal{R}p$, alors $p = qk$ et $q = pj$ avec $k, j \geq 1$ et donc $p = pjk$. Ceci n'est possible que si $p = 1$, mais alors $q = 1 = p$ ou si $jk = 1$, ce qui implique $j = k = 1$ et donc $p = q$.
   - ◇ transitive : si $p\mathcal{R}q$ et $q\mathcal{R}r$, alors $q = pk$ et $r = qj = pjk$, donc $p\mathcal{R}r$.
2. On définit donc ainsi un ordre sur $\mathbb{N}^*$ qui n'est pas total (par exemple, on ne peut pas comparer 2 et 3). Soit maintenant p un majorant de $\{2, 3\}$. Alors $2\mathcal{R}p$ et donc $p = 2k$, avec $k \geq 1$. De même, $p = 3j$ avec $j \geq 1$. Par unicité de la décomposition en produits de facteurs premiers, ceci est impossible. L'ensemble $\{2, 3\}$ n'a pas de majorant.

Exercice 23

Soient $A = (x_1, y_1)$ et $B = (x_2, y_2)$ deux points dans $E = \mathbb{R}^2$. Nous écrivons : $A\mathcal{R}B$ si $y_1 = y_2$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Décrire la classe d'équivalence de $A = (1, 2)$ que l'on notera $\overline{A}$ par :
   a) la description $\overline{A} = \{\ldots\}$,
   b) puis l'objet géométrique qu'il représente.

   (On rappelle qu'une classe d'équivalence est un sous-ensemble de E).
3. Plus généralement, décrire la classe d'équivalence de $A = (a, b) \in \mathbb{R}^2$ pour $(a, b) \in \mathbb{R}^2$ fixé (*i.e.* décrire $\overline{A} = \{\ldots\}$).
4. Pour cet exemple particulier $(E, \mathcal{R})$, montrer que pour toute classe d'équivalence $\overline{A} = \overline{(a, b)}$, on peut choisir un représentant spécifique de la forme $(0, y)$ (on précisera la valeur de y). On appellera cet élément *représentant canonique* (ce n'est pas toujours possible en général).

5. Montrer que $\{\overline{(0,y)}, y \in \mathbb{R}\}$ forme une partition de E correspondant aux classes d'équivalences de $\mathcal{R}$.
6. Interpréter géométriquement l'espace quotient $E/_{\mathcal{R}}$.
7. Même exercice avec la définition suivante : $A\mathcal{R}B$ si $x_1 = x_2$.
8. Même exercice avec la définition suivante : $A\mathcal{R}B$ si $\overrightarrow{AB} \in \mathcal{D}$, où $\mathcal{D}$ est une droite affine de $E = \mathbb{R}^2$.

Éléments de réponse 23

Exercice 24

Soient $\overrightarrow{u} = (x_1, y_1)$ et $\overrightarrow{v} = (x_2, y_2)$ deux vecteurs dans $E = \mathbb{R}^2$.
Nous écrivons $\overrightarrow{u}\mathcal{R}\overrightarrow{v}$ si $||\overrightarrow{u}|| = ||\overrightarrow{v}||$ (*i.e.* si $\overrightarrow{u}$ et $\overrightarrow{v}$ ont la même longueur).

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Décrire la classe d'équivalence de $A = (3, 4)$ que l'on notera $\overline{A}$ par :
   a) la description $\overline{A} = \{\ldots\}$,
   b) puis l'objet géométrique qu'il représente.
3. Décrire la classe d'équivalence de $0 = (0, 0)$.
4. Montrer que toute classe d'équivalence est de la forme $\overline{(0, R)}$ pour un $R \geq 0$ que l'on appellera *représentant canonique* de la classe considérée.
5. Quel est le *représentant canonique* de la classe de $A = (3, 4)$?
6. Montrer que $\{\overline{(0, R)} \,|\, R \geq 0\}$ forme une partition de E correspondant aux classes d'équivalences de $\mathcal{R}$.
7. Interpréter géométriquement l'espace quotient $E/_{\mathcal{R}}$.

Éléments de réponse 24

Exercice 25

Soient E et F deux ensembles. Soit f une application $f : E \to F$. Montrer que la relation binaire $\mathcal{R}$ définie sur E par

$$x\mathcal{R}y \iff f(x) = f(y)$$

est une relation d'équivalence sur E. Décrire la classe d'un élément $x \in E$.

Éléments de réponse 25

Exercice 26

Montrer que la relation binaire $\mathcal{R}$ définie sur $\mathbb{R}^+$ par

$$x\mathcal{R}y \iff \exists\, k, \ell \in \mathbb{N}^* \text{ tel que } kx = \ell y$$

est une relation d'équivalence sur $\mathbb{R}^+$. Décrire les classes d'équivalence $\overline{0}$ et $\overline{1}$.

Éléments de réponse 26

Exercice 27

Soit $f\colon \mathbb{R}^2 \to \mathbb{R}$ l'application définie par $f(x,y) = y - 2x$.

1. Montrer que chaque classe d'équivalence pour la relation $\mathcal{R}_f$ est une droite.
2. Montrer que ${}^{\mathbb{R}^2}\!/_{\mathcal{R}_f}$ est l'ensemble des droites parallèles à la droite d'équation $y = 2x$.
3. Montrer que f définit une bijection $\widetilde{f}\colon {}^{\mathbb{R}^2}\!/_{\mathcal{R}_f} \to \mathbb{R}$.

Éléments de réponse 27

1. Les classes d'équivalence pour $\mathcal{R}_f$ sont les parties $(\overline{m})_{m\in\mathbb{R}}$ de $\mathbb{R}^2$ telles que $\overline{m} = \{(x,y) \in \mathbb{R}^2 \,|\, y - 2x = m\}$.

   Pour $m \in \mathbb{R}$ la classe $\overline{m}$ est donc une droite de pente 2.
2. Toute droite de pente 2 a une équation de la forme $y - 2x = m$: l'ensemble des $\overline{m}$ est donc l'ensemble des droites de pente 2, autrement dit l'ensemble des droites parallèles à la droite d'équation $y = 2x$.
3. L'application f est surjective ; en effet, pour tout $m \in \mathbb{R}$, nous avons $f(0,m) = m$. Le Corollaire **??** assure alors que f définit une bijection $\widetilde{f}\colon {}^{\mathbb{R}^2}\!/_{\mathcal{R}_f} \to \mathbb{R}$.

Exercice 28

Soit $f\colon \mathbb{C}^* \to \mathbb{C}^*$ l'application définie par $f(z) = z^4$.

1. Soit $z \in \mathbb{C}^*$. Déterminer les éléments équivalents à z pour la relation $\mathcal{R}_f$.
2. Montrer que f définit une bijection $\widetilde{f}\colon {}^{\mathbb{C}^*}\!/_{\mathcal{R}_f} \to \mathbb{C}^*$.

Éléments de réponse 28

1. Pour tous z, $z' \in \mathbb{C}^*$ nous avons les équivalences

$$z'\mathcal{R}_f z \iff z'^4 = z^4 \iff \left(\frac{z'}{z}\right)^4 = 1 \iff \frac{z'}{z} \in \{1, \mathbf{i}, -1, -\mathbf{i}\} \iff z' \in \{z, -z, \mathbf{i}z, -\mathbf{i}z\}.$$

   Ainsi la classe de z est : $\overline{z} = \{z, -z, \mathbf{i}z, -\mathbf{i}z\}$.
2. L'application f est surjective ; en effet, tout nombre complexe non nul possède des racines quatrièmes non nulles. Le Corollaire **??** assure alors que f définit une bijection $\widetilde{f}\colon {}^{\mathbb{C}^*}\!/_{\mathcal{R}_f} \to \mathbb{C}^*$.

Exercice 29

Sur l'ensemble $E = \mathbb{N} \setminus \{0\}$ définissons une relation en posant :

$$\forall\, n,\, n' \in E,\ n\mathcal{R}n' \iff \text{il existe des entiers } u,\, v \text{ impairs tels que } \frac{n'}{n} = \frac{v}{u}.$$

Soit $f\colon E \to \mathbb{N}$ l'application qui à tout entier $n \geq 1$ associe l'exposant de 2 dans la décomposition de n en facteurs premiers. Par exemple $f(8) = f(40) = 3$ et $f(13) = 0$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Montrer que l'application f définit une bijection $\widetilde{f}\colon {}^{E}\!/_{\mathcal{R}} \to \mathbb{N}$.

Éléments de réponse 29

1. La relation $\mathcal{R}$ est réflexive. Soit $n \in E$, alors $\frac{n}{n} = \frac{1}{1}$ et $n\mathcal{R}n$.

   La relation $\mathcal{R}$ est symétrique. Soient n et n' dans E tels que $n\mathcal{R}n'$. Autrement dit il existe des entiers impairs u et v tels que $\frac{n'}{n} = \frac{u}{v}$. Nous en déduisons que $\frac{n}{n'} = \frac{v}{u}$ avec v, u entiers impairs. Ainsi $n'\mathcal{R}n$.

   La relation $\mathcal{R}$ est transitive. Soient n, n' et n'' dans E tels que $n\mathcal{R}n'$ et $n'\mathcal{R}n''$. Autrement dit il existe u, v, r et s des entiers impairs tels que $\frac{n'}{n} = \frac{v}{u}$ et $\frac{n''}{n'} = \frac{s}{r}$. Par conséquent
   $$\frac{n''}{n} = \frac{n''}{n'}\frac{n'}{n} = \frac{s}{r}\frac{v}{u} = \frac{sv}{ru}.$$
   Or d'une part s et v étant des entiers impairs sv est impair, d'autre part r et u étant des entiers impairs ru est impair. Il s'en suit que $n\mathcal{R}n''$.

2. Montrons que la relation $\mathcal{R}$ est égale à la relation $\mathcal{R}_f$ définie par f. Soient n, n' dans E. Si $n\mathcal{R}n'$, alors il existe des entiers impairs u et v tel que $nv = n'u$. L'exposant de 2 dans la décomposition de nv est le même que dans n, l'exposant de 2 dans la décomposition de $n'u$ est le même que dans n' ; par suite $f(n) = f(n')$ et $n\mathcal{R}_f n'$.

   Réciproquement, si 2 apparaît avec le même exposant dans la décomposition en facteurs premiers de n et n', alors $n = 2^k m$ et $n' = 2^k m'$ où m et m' sont impairs. Ainsi nous avons $\frac{n'}{n} = \frac{m'}{m}$, *i.e.* $n\mathcal{R}n'$. Par conséquent $\widetilde{f}$ existe et est injective. L'application f est surjective ; en effet, pour tout entier $k \geq 0$ $f(2^k) = k$. Il en résulte que $\widetilde{f}$ est surjective. Enfin, $\widetilde{f}$ réalise une bijection entre $\frac{E}{\mathcal{R}}$ et $\mathbb{N}$.

Exercice 30

Soit n un entier au moins égal à 1. Soit $E = \{1, 2, \ldots, 2n\}$. Nous souhaitons montrer que si l'on choisir $n + 1$ nombres de E, il y en a au moins qui est multiple d'un autre.

1. Soit $\mathcal{R}$ la relation définie sur E par
   $$\forall\, x,\, y \in E,\ x\mathcal{R}y \iff \exists\, k \in \mathbb{Z},\ y = 2^k x$$
   Montrer que $\mathcal{R}$ est une relation d'équivalence.

2. Montrer que toute classe d'équivalence a un unique représentant impair. En déduire qu'il y a n classes.
3. Soit $A \subset E$ une partie ayant $n+1$ éléments. Montrer qu'il existe a, $b \in A$ tels que $a \neq b$ et $a\mathcal{R}b$. Conclure.

Éléments de réponse 30

1. La relation $\mathcal{R}$ satisfait les trois propriétés suivantes :
   - ◇ pour tout x dans E, nous avons $x = 2^0 x$, *i.e.* $\mathcal{R}$ est réflexive ;
   - ◇ soient x et y dans E tels que $x\mathcal{R}y$, *i.e.* tels que $y = 2^k x$ pour un certain $k \in \mathbb{Z}$. Nous en déduisons que $x = 2^{-k} y$; remarquons que $-k$ appartient à $\mathbb{Z}$. Par suite $y\mathcal{R}x$. Ainsi $\mathcal{R}$ est symétrique.
   - ◇ soient x, y et z dans E tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $y = 2^k x$ et $z = 2^\ell y$ pour certains k, $\ell \in \mathbb{Z}$. Il en résulte que
   $$z = 2^\ell \underbrace{y}_{2^k x} = 2^\ell 2^k x = 2^{\ell+k} x;$$
   de plus, $\ell + k$ appartient à $\mathbb{Z}$. Ainsi $x\mathcal{R}z$ et $\mathcal{R}$ est transitive.
2. Soit $a \in E$. Soit k l'exposant de 2 dans la décomposition en facteurs premiers de a ; alors k appartient à $\mathbb{N}$ et a s'écrit $2^k b$ où b désigne un entier impair inférieur ou égal à a ; en particulier b appartient à E. Ainsi $a\mathcal{R}b$ et b est un représentant impair de $\overline{a}$. Supposons que $\overline{a}$ ait un représentant impair c distinct de b. Alors, en particulier, $b\mathcal{R}c$, *i.e.* il existe $m \in \mathbb{Z}$ tel que $b = 2^m c$. Étant donné que b et c sont impairs nous avons nécessairement $m = 0$ donc $b = c$.
3. Utilisons le principe des tiroirs

   > Si nous rangeons plus de n objets dans n tiroirs, alors l'un au moins des tiroirs contient au moins deux objets.

   Nous pouvons ranger chaque élément de la partie A dans sa classe d'équivalence. Puisque A possède plus de n éléments et qu'il y a n classes, au moins deux éléments de A sont dans la même classe d'après le principe des tiroirs. Ainsi il existe a, b dans A tels que $a \neq b$ et $a\mathcal{R}b$.

   Si par exemple $b > a$, alors $b = 2^k a$ avec $k > 0$ donc b est multiple de a.

Exercice 31

Notons $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers relatifs. Considérons sur $\mathbb{Z}[X]$ la relation $\sim$ définie par

$$\forall\, P, Q \in \mathbb{Z}[X],\ P\mathcal{R}Q \Longleftrightarrow P - Q \text{ est multiple de } X.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}[X]$.

2. Soit $P \in \mathbb{Z}[X]$. Montrer que P est équivalent au polynôme constant $P(0)$.
3. Soit $f\colon \mathbb{Z}[X] \to \mathbb{Z}$ l'application définie par $f(P) = P(0)$. Montrer que f définit une bijection entre $\mathbb{Z}[X]/\mathcal{R}$ et $\mathbb{Z}$.

Éléments de réponse 31

1. La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}[X]$; en effet,
   - ◇ la relation $\mathcal{R}$ est réflexive : pour tout polynôme $P \in \mathbb{Z}[X]$ nous avons d'une part $P - P = 0$, d'autre part 0 est multiple de X, donc $P - P$ est multiple de X, *i.e.* $P\mathcal{R}P$;
   - ◇ la relation $\mathcal{R}$ est symétrique : soient P et Q deux éléments de $\mathbb{Z}[X]$ tels que $P\mathcal{R}Q$, *i.e.* tels que $P - Q$ est multiple de X, alors $Q - P = -(P - Q)$ aussi, c'est-à-dire $Q\mathcal{R}P$;
   - ◇ la relation $\mathcal{R}$ est transitive : soient P, Q, R trois éléments de $\mathbb{Z}[X]$ tels que $P\mathcal{R}Q$ et $Q\mathcal{R}R$. Autrement dit $P - Q$ et $Q - R$ sont multiples de X, *i.e.* il existe U et V dans $\mathbb{Z}[X]$ tels que $P - Q = UX$ et $Q - R = VX$. Alors
   $$P - R = (P - Q) + (Q - R) = UX + VX = (U + V)X;$$
   en particulier $P - R$ est multiple de X, c'est-à-dire $P\mathcal{R}R$.
2. Le polynôme $P - P(0)$ s'annule en 0, *i.e.* le polynôme $P - P(0)$ a pour racine 0 ; il en résulte que $P - P(0)$ est multiple de X, c'est-à-dire $P\mathcal{R}P(0)$: P est en relation avec le polynôme constant $P(0)$.
3. Pour tous polynômes P, $Q \in \mathbb{Z}[X]$ nous avons $P\mathcal{R}P(0)$ et $Q\mathcal{R}Q(0)$. Ainsi $P\mathcal{R}Q$ si et seulement si $P(0)\mathcal{R}Q(0)$. Mais les polynômes constants $P(0)$ et $Q(0)$ ne sont équivalents que si leur différence $P(0) - Q(0)$ est multiple de X, c'est-à-dire si $P(0) - Q(0) = 0$. Finalement $P\mathcal{R}Q$ si et seulement si $P(0) = Q(0)$. Cela montre que les relations $\mathcal{R}$ et $\mathcal{R}_f$ sont les mêmes. La factorisation de f est donc une application injective $\widetilde{f}\colon \mathbb{Z}[X]/\mathcal{R} \to \mathbb{Z}$. De plus, l'application f est surjective ; en effet, pour tout $k \in \mathbb{Z}$, le polynôme constant $P = k$ vérifie $P(0) = k$, c'est-à-dire $f(P) = k$. Le Corollaire **??** assure alors que f définit une bijection $\widetilde{f}\colon \mathbb{C}^*/\mathcal{R}_f \to \mathbb{C}^*$.

Exercice 32

Considérons sur $\mathbb{R}^2$ la relation $\prec$ définie par

$$(x, y) \prec (x', y') \iff ((x < x') \text{ ou } (x = x' \text{ et } y \leq y'))$$

Montrer que ceci définit une relation d'ordre sur $\mathbb{R}^2$.

Éléments de réponse 32

La relation est

- ◇ réflexive : $x = x$ et $y \leq y$ impliquent $(x, y) \prec (x, y)$;
- ◇ antisymétrique : si $(x, y) \prec (x', y')$ et $(x', y') \prec (x, y)$, alors on a nécessairement que $x = x'$ (si $x < x'$ par exemple, on ne peut avoir $(x', y') \prec (x, y)$). Mais alors, on a à la fois $y \leq y'$ d'après la première relation, et aussi $y' \leq y$ d'après la seconde. Nous en déduisons que $x = x'$ et $y = y'$;
- ◇ transitive : si $(x, y) \prec (x', y')$ et $(x', y') \prec (x'', y'')$, alors :
  - ou bien $x = x'$ et $x' = x''$: dans ce cas, on a $y \leq y'$ et $y' \leq y''$ donc $y \leq y''$ et donc $(x, y) \prec (x'', y'')$;
  - ou bien $x = x'$ et $x' < x''$: dans ce cas, on a $x < x''$ et donc $(x, y) \prec (x'', y'')$;
  - ou bien $x < x'$ et $x' = x''$: dans ce cas, on a $x < x''$ donc $(x, y) \prec (x'', y'')$.

Remarque : ceci définit un ordre total sur $\mathbb{R}^2$; en effet, deux éléments sont toujours comparables.

Exercice 33

On munit $\mathbb{R}^2$ de la relation notée $\prec$ définie par $(x, y) \prec (x', y') \iff x \leq x'$ et $y \leq y'$.

1. Montrer que $\prec$ est une relation d'ordre sur $\mathbb{R}^2$.
2. L'ordre est-il total ?
3. Le disque fermé $\mathbb{D}$ de centre O et de rayon 1 a-t-il des majorants ? un plus grand élément ? une borne supérieure ?

Éléments de réponse 33

1. La relation $\prec$ est
   - ◇ réflexive : pour tout $(x, y) \in \mathbb{R}^2$, on a $x \leq x$ et $y \leq y$.
   - ◇ transitive : si $(x_1, y_1) \prec (x_2, y_2)$ et $(x_2, y_2) \prec (x_3, y_3)$, alors $x_1 \leq x_2 \leq x_3$ et $y_1 \leq y_2 \leq y_3$ donc $(x1, y1) \prec (x_3, y_3)$.
   - ◇ antisymétrique : si $(x, y) \prec (x', y')$ et $(x', y') \prec (x, y)$, alors on a à la fois $x \leq x'$ et $x' \leq x$ et donc $x = x'$ et de même $y = y'$.

   Elle définit donc bien une relation d'ordre sur $\mathbb{R}^2$.
2. L'ordre n'est pas total, car on ne peut pas comparer $(0, 1)$ et $(1, 0)$.
3. Soit (x, y) un majorant de $\mathbb{D}$. Alors $(1, 0) \prec (x, y)$ et donc $x \geq 1$. De même, $(0, 1) \prec (x, y)$ et donc $y \geq 1$. Ainsi, on a $x \geq 1$ et $y \geq 1$. Réciproquement, soit $(x, y) \in \mathbb{R}^2$ tel que $x \geq 1$ et $y \geq 1$. Alors (x, y) est clairement un majorant de $\mathbb{D}$, puisque tout élément (x_0, y_0) de $\mathbb{D}$ vérifie $x_0^2 + y_0^2 \leq 1$, et donc $x_0 \leq 1$ et $y_0 \leq 1$. On en déduit que l'ensemble des majorants de $\mathbb{D}$ est $\{(x, y) \in \mathbb{R}^2 \,|\, x \geq 1 et y \geq 1\}$. $\mathbb{D}$ n'admet donc pas de plus grand élément, puisque les majorants de $\mathbb{D}$ ne sont pas dans $\mathbb{D}$. En revanche, $\mathbb{D}$ admet une borne supérieure qui est $(1, 1)$, le plus petit des majorants de $\mathbb{D}$.

Exercice 34

Soit E un ensemble ordonné. Démontrer que toute partie de E admet un élément maximal si et seulement si toute suite croissante de E est stationnaire.

Éléments de réponse 34

◇ Démontrons que si toute partie de E admet un élément maximal, alors toute suite croissante de E est stationnaire.

Supposons d'abord que toute partie de E admet un élément maximal. Considérons $(u_n)_n$ une suite croissante de E, et posons $F = \{u_n \mid n \geq 0\}$. L'ensemble F possède donc un élément maximal u_{n_0}. Mais pour $n \geq n_0$, puisque $(u_n)_n$ est croissante, on a $u_n \geq u_{n_0}$. Mais comme u_{n_0} est un élément maximal de F et que u_n appartient à F, nous avons $u_n = u_{n_0}$. La suite est donc stationnaire.

◇ Démontrons que si toute suite croissante de E est stationnaire, alors toute partie de E admet un élément maximal. Raisonnons par contraposée.

Supposons donc qu'il existe dans E un ensemble F n'admettant pas d'élément maximal ; montrons qu'alors il existe une suite de E croissante et qui n'est pas stationnaire. Commençons par prendre n'importe quel élément $u_0 \in F$. Puisque u_0 n'est pas un élément maximal de F, il existe $u_1 \in F$ tel que $u_1 > u_0$. Puisque u_1 n'est pas un élément maximal de F, il existe $u_2 \in F$ tel que $u_2 > u_1$. Nous pouvons itérer ce procédé et construire ainsi une suite $(u_n)_n$ de F qui est strictement croissante, et donc qui n'est pas stationnaire.

Exercice 35

On dit qu'un ordre $\leq$ sur un ensemble E est bien fondé s'il n'existe pas de suite infinie strictement décroissante $(x_n)_n$ de E.

Démontrer que $\mathbb{N}^2$ muni de l'ordre lexicographique est bien fondé.

Éléments de réponse 35

Il suffit de démontrer par récurrence sur $p \geq 0$ la propriété suivante :

$\mathcal{P}_p$ il n'existe pas de suite $(x_n = (a_n, b_n))_n \subset \mathbb{N}^2$ strictement décroissante vérifiant $a_0 = p$.

- Initialisation. Supposons par l'absurde qu'une telle suite existe. Alors, pour tout entier $n \geq 1$, on sait que $a_n \leq a_0$ et donc $a_n = a_0$. Mais alors, la suite $(b_n)_n$ doit être strictement décroissante, et c'est une suite d'entiers positifs. C'est impossible !
- Hérédité. Supposons la propriété démontrée jusqu'au rang p et prouvons la au rang $p+1$. Comme précédemment, on raisonne par l'absurde et on suppose qu'il existe une suite $(x_n = (a_n, b_n))_n \subset \mathbb{N}^2$ strictement décroissante vérifiant $a_0 = p + 1$. Alors, pour tout entier $n \geq 1$, on sait que $a_n \leq a_0$. Si pour tout entier n, on avait $a_n = a_0$, alors on obtiendrait une contradiction en raisonnant exactement de la même façon que pour l'initialisation. Donc il existe un entier n_0 tel que $a_{n_0} \leq p$. Mais alors la suite $(x_n)_{n \geq 0}$ est une

suite strictement décroissante de $\mathbb{N}^2$ dont le premier terme est inférieur ou égal à p. Ceci contredit l'hypothèse de récurrence.

Remarquons qu'on utilise un raisonnement par l'absurde à l'intérieur d'une récurrence forte ! Plus généralement, l'ordre lexicographique défini sur le produit fini d'ensembles ayant un ordre bien fondé est lui-même un ordre bien fondé.

Exercice 36

Sur $\mathbb{C}$ on définit la relation $\mathcal{R}$ par : $z\mathcal{R}z' \iff |z| = |z'|$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Déterminer la classe d'équivalence de chaque $z \in \mathbb{C}$.

Éléments de réponse 36

1. Soient z, z', z'' des complexes quelconques.
   - ◇ $\mathcal{R}$ est réflexive : $z\mathcal{R}z$ car $|z| = |z|$.
   - ◇ $\mathcal{R}$ est symétrique : $z\mathcal{R}z' \Rightarrow z'\mathcal{R}z$ car $|z| = |z'|$ et donc $|z'| = |z|$.
   - ◇ $\mathcal{R}$ est transitive : si $z\mathcal{R}z'$ et $z'\mathcal{R}z''$ alors $|z| = |z'| = |z''|$ donc $z\mathcal{R}z''$.
2. La classe d'équivalence d'un point $z \in \mathbb{C}$ est l'ensemble des complexes qui sont en relation avec z, *i.e.* l'ensemble des complexes dont le module est égal à $|z|$. Géométriquement la classe d'équivalence de z est le cercle $\mathcal{C}$ de centre 0 et de rayon $|z|$:
$$\mathcal{C} = \left\{ |z| \mathrm{e}^{\mathbf{i}\vartheta} \,|\, \vartheta \in \mathbb{R} \right\}$$

Exercice 37

Montrer que la relation $\mathcal{R}$ définie sur $\mathbb{R}$ par : $x\mathcal{R}y \iff x \exp y = y \exp x$ est une relation d'équivalence. Préciser, pour x fixé dans $\mathbb{R}$, le nombre d'éléments de la classe de x modulo $\mathcal{R}$.

Éléments de réponse 37

1. La relation $\mathcal{R}$ est
   - ◇ réflexive : pour tout $x \in \mathbb{R}$, $x \exp x = x \exp x$ donc $x\mathcal{R}x$.
   - ◇ symétrique : pour x, $y \in \mathbb{R}$, si $x\mathcal{R}y$ alors $x \exp y = y \exp x$ donc $y \exp x = x \exp y$ donc $y\mathcal{R}x$.
   - ◇ transitive : soient x, y, $z \in \mathbb{R}$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x \exp y = y \exp x$ et $y \exp z = z \exp y$. Calculons $xy \exp z$:

     $xy \exp z = x(y \exp z) = x(z \exp y) = z(x \exp y) = z(y \exp x) = yz \exp x$.

     Ainsi $xy \exp z = yz \exp x$.

     - Si y est non nul, alors en divisant par y on vient de montrer que $x \exp z = z \exp x$ donc $x\mathcal{R}z$ et c'est fini.

- Si $y = 0$, alors $x = 0$ et $z = 0$ donc $x\mathcal{R}z$ également.

2. Soit $x \in \mathbb{R}$ fixé. Désignons par $\overline{x}$ la classe d'équivalence de x modulo $\mathcal{R}$:

$$\overline{x} = \{y \in \mathbb{R} \,|\, y\mathcal{R}x\}.$$

Ainsi

$$\overline{x} = \{y \in \mathbb{R} \,|\, x \exp y = y \exp x\}.$$

Considérons la fonction f définie par

$$f : \mathbb{R} \to \mathbb{R} \qquad\qquad t \mapsto \frac{t}{\exp t}.$$

Alors

$$\overline{x} = \{y \in \mathbb{R} \,|\, f(x) = f(y)\}.$$

Autrement dit, $\overline{x}$ est l'ensemble des $y \in \mathbb{R}$ qui par f prennent la même valeur que $f(x)$, *i.e.* $\overline{x} = f^{-1}(f(x))$.

Étudions maintenant la fonction f afin de déterminer le nombre d'antécédents : en calculant f' nous pouvons montrer que f est strictement croissante sur $]-\infty, 1]$ puis strictement décroissante sur $[1, +\infty[$. De plus, en $-\infty$ la limite de f est $-\infty$, $f(1) = \frac{1}{\mathrm{e}}$ et la limite en $+\infty$ est 0.

- ◇ si $x \leq 0$, alors $f(x)$ appartient à $]-\infty, 0]$ et $f(x)$ a un seul antécédent ;
- ◇ si $x > 0$ et $x \neq 1$, alors $f(x)$ appartient à $\left]0, \frac{1}{2}\right[$ et $f(x)$ a deux antécédents ;
- ◇ si $x = 1$, alors $f(x) = \frac{1}{\mathrm{e}}$ a un unique antécédent.

Finalement, si x appartient à $]0, 1[\cup]1, +\infty[$, alors $\#\overline{x} = \#f^{-1}(f(x)) = 2$ et si $x \leq 0$ ou $x = 1$, alors $\#\overline{x} = \#f^{-1}(f(x)) = 1$.

Exercice 38

Soit $(E, \leq)$ un ensemble ordonné. Considérons sur $\mathcal{P}(E) \setminus \{\emptyset\}$ la relation $\prec$ par

$$X \prec Y \iff (X = Y \text{ ou } \forall\, x \in X \ \forall\, y \in Y \ \ x \leq y).$$

Vérifier que c'est une relation d'ordre.

Éléments de réponse 38

La relation $\prec$ est :

- ◇ réflexive : pour tout $X \in \mathcal{P}(E)$ on a $X \prec X$ car $X = X$.
- ◇ anti-symétrique : pour X, $Y \in \mathcal{P}(E)$ tels que $X \prec Y$ et $Y \prec X$, alors par définition de $\prec$ on a $\forall\, x \in X \ \forall\, y \in Y \ \ x \leq y$ et $y \leq x$. Comme la relation $\leq$ est une relation d'ordre alors $x \leq y$ et $y \leq x$ implique $x = y$. Donc $\forall\, x \in X \ \forall\, y \in Y \ \ x = y$, ce qui implique que $X = Y$ (dans ce cas en fait X est vide ou un singleton).

◇ transitive : soient X ,Y, $Z \in \mathcal{P}(E)$ tels que $X \prec Y$ et $Y \prec Z$. Si $X = Y$ ou $Y = Z$ alors il est clair que $X \prec Z$. Supposons que $X \neq Y$ et $Y \neq Z$ alors $\forall\, x \in X \ \forall\, y \in Y \ x \leq y$ et $\forall\, y \in Y \ \forall\, z \in Z \ y \leq z$. Donc on a $\forall\, x \in X \ \forall\, y \in Y \ \forall\, z \in Z \ x \leq y$ et $y \leq z$, alors par transitivité de la relation $\leq$ on obtient : $\forall\, x \in X \ \forall\, z \in Z \ x \leq z$. Donc $X \prec Z$

1.2. Groupe $\mathbb{Z}$

1.2.1. Divisibilité dans $\mathbb{Z}$. —

Exercice 39

Étant donnés cinq nombres entiers consécutifs, on trouve toujours parmi eux (vrai ou faux et pourquoi) :

1. au moins deux multiples de 2 ;
2. au plus trois nombres pairs ;
3. au moins deux multiples de 3 ;
4. exactement un multiple de 5 ;
5. au moins un multiple de 6 ;
6. au moins un nombre premier.

Éléments de réponse 39

1. Si n est pair, alors $n+2$ et $n+4$ sont pairs alors que $n+1$ et $n+3$ sont impairs.

   Si n est impair, alors $n+2$ et $n+4$ sont impairs alors que $n+1$ et $n+3$ sont pairs.

   Il y a deux ou trois nombres pairs parmis ces cinq entiers, donc au moins deux nombres pairs.
2. D'apès 1. il y a deux ou trois nombres impairs donc au plus trois.
3. D'après 1. et 2. il y a au moins deux multiples de 3.
4. Parmi cinq nombres consécutifs il y a au moins un multiple de 5, notons le $n+k$, $k \in \{0, 1, 2, 3, 4\}$, multiple de 5 suivant est $n+k+5$ qui n'appartient pas à $\{n, n+1, n+2, n+3, n+4\}$, il y a donc exactement un multiple de 5.
5. C'est faux, par exemple dans $\{1, 2, 3, 4, 5\}$ il n'y a pas de multiple de 6.
6. C'est faux, par exemple dans $\{24, 25, 26, 27, 28\}$ il n'y a pas de nombre premier.

Exercice 40

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. 60 a plus de diviseurs (positifs) que 100.
2. 60 a moins de diviseurs (positifs) que 90.

3. 60 a moins de diviseurs (positifs) que 120.
4. si un entier divise 60, alors il divise 120.
5. si un entier strictement inférieur à 60 divise 60, alors il divise 90.
6. si un nombre premier divise 120, alors il divise 60.

Éléments de réponse 40

1. $60 = 2^2 \times 3^1 \times 5^1$; ainsi les diviseurs positifs de 60 sont de la forme $2^i \times 3^j \times 5^k$ avec $(i, j, k) \in \{0, 1, 2\} \times \{0, 1\} \times \{0, 1\}$. 60 a donc $3 \times 2 \times 2 = 12$ diviseurs.

   $100 = 2^2 \times 5^2$ donc les diviseurs positifs de 100 sont de la forme $2^i \times 5^j$ avec $(i, j) \in \{0, 1, 2\} \times \{0, 1, 2\}$. 100 a donc $3 \times 3 = 0$ diviseurs.

   60 a plus de diviseurs positifs que 100.
2. $90 = 2^1 \times 3^2 \times 5^1$ donc les diviseurs positifs de 90 sont de la forme $2^i \times 3^j \times 5^k$ avec $(i, jk) \in \{0, 1\} \times \{0, 1, 2\} \times \{0, 1\}$. 90 a donc $2 \times 3 \times 2 = 12$ diviseurs.

   60 a le même nombre de diviseurs positifs que 90, la réponse est donc vraie.
3. $120 = 2^3 \times 3^1 \times 5^1$ donc les diviseurs positifs de 120 sont de la forme $2^i \times 3^j \times 5^k$ avec $(i, j, k) \in \{0, 1, 2, 3\} \times \{0, 1\} \times \{0, 1\}$. 120 a donc $4 \times 2 \times 2 = 16$ diviseurs.

   Ainsi 60 a moins de diviseurs positifs que 120.

   Seconde méthode : $120 = 2 \times 60$, par conséquent les diviseurs de 60 sont aussi des diviseurs de 120 ; comme 120 est un diviseur de 120 mais pas de 60, 120 a plus de diviseurs que 60.
4. Si n est un diviseur de 60 il existe $k \in \mathbb{Z}$ tel que $60 = k \times n$ donc $120 = 2k \times n$. Il en résulte que n est un diviseur de 120.
5. C'est faux : 20 divise 60 et 20 ne divise pas 90.
6. Les diviseurs premiers de 120 sont 2, 3 et 5 ; ils divisent tous les trois 60.

   Seconde méthode : $120 = 2 \times 60$. 2 divise 60 ; soit $p > 2$ un diviseur premier de 120, il existe $k \in \mathbb{Z}$ tel que $120 = p \times k$, alors $p \times k = 2 \times 60$. D'après le théorème de Gauss p divise 2×60, p est premier avec 2, p divise donc 60.

Exercice 41

1. Calculer $\text{pgcd}(60, 84)$ par l'algorithme d'Euclide.
2. En déduire une identité de Bézout.
3. Calculer $\text{ppcm}(a, b)$.
4. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que : $au + bv = \text{pgcd}(a, b)$.
5. Donner la décomposition en facteurs premiers de a et b.
6. En déduire la décomposition en facteurs premiers de $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$, et retrouver les résultats des questions 1 et 3.

Éléments de réponse 41

1. Calcul du pgcd$(60, 84)$ par l'algorithme d'Euclide :

$$84 = 1 \times 60 + 24, \qquad 60 = 2 \times 24 + 12, \qquad 24 = 2 \times 12.$$

Puisque pgcd$(84, 60)$ est le dernier reste non nul, pgcd$(84, 60) = 12$.

2. Une identité de Bézout est donc

$$12 = 60 - 2 \times 24 = 60 - 2 \times (84 - 1 \times 60) = -2 \times 84 + 3 \times 60.$$

3. Calcul de ppcm$(84, 60)$:

$$\text{ppcm}(84, 60) = \frac{84 \times 60}{\text{pgcd}(84, 60)} = \frac{84 \times 60}{12} = 420.$$

4. Une solution particulière de $60u + 84v = 12$ est : $3 \times 60 + (-2) \times 84 = 12$ On fait la soustraction de $60u + 84v = 12$ avec $3 \times 60 + (-2) \times 84 = 12$, on obtient

$$60(u-3) + 84(v+2) = 0 \iff 60(u-3) = -84(v+2) \iff 5(u-3) = -7(v+2).$$

En particulier 5 divise $-7(v+2)$ et 5 est premier avec 7, donc d'après le théorème de Gauss 5 divise $-(v+2)$. Ainsi il existe un entier relatif k tel que $-(v+2) = 5k$ soit $v = -2 - 5k$; en substituant dans $5(u-3) = -7(v+2)$ nous obtenons $5(u-3) = 7 \times 5k$ soit $u - 3 = 7k$ ou encore $u = 3 + 7k$. Réciproquement

$$60(u-3) + 84(v+2) = 60(3 + 7k - 3) + 84(-2 - 5k + 2) = 60 \times 7k - 84 \times 5k = 0.$$

L'ensemble des couples (u, v) recherchés est : $\{(3 + 7k, -2 - 5k) \mid k \in \mathbb{Z}\}$.

5. La décomposition de 60 en facteurs premiers est $2^2 \times 3 \times 5$. La décomposition de 84 en facteurs premiers est $2^2 \times 3 \times 7$.

6. On retrouve :

$$\text{pgcd}(60, 84) = 2^2 \times 3 = 12, \qquad \text{ppcm}(60, 84) = 2^2 \times 3 \times 5 \times 7 = 420$$

Exercice 42

1. Calculer pgcd$(160, 171)$ par l'algorithme d'Euclide.
2. En déduire une identité de Bézout.
3. Calculer ppcm(a, b).
4. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que : $au + bv = \text{pgcd}(a, b)$.
5. Donner la décomposition en facteurs premiers de a et b.
6. En déduire la décomposition en facteurs premiers de pgcd(a, b) et ppcm(a, b), et retrouver les résultats des questions 1 et 3.

Éléments de réponse 42

1. Calcul du $\text{pgcd}(160, 171)$ par l'algorithme d'Euclide :

$$171 = 1 \times 160 + 11, \quad 160 = 14 \times 11 + 6, \quad 11 = 1 \times 6 + 5, \quad 6 = 1 \times 5 + 1, \quad 5 = 5 \times 1.$$

   Puisque $\text{pgcd}(171, 160)$ est le dernier reste non nul, nous avons : $\text{pgcd}(171, 160) = 1$.

2. Une identité de Bézout est $-29 \times 171 + 31 \times 160 = 1$. En effet

$$1 = 6-1\times5 = 6-1\times(11-1\times6) = -1\times11+2\times6 = -1\times11+2\times(160-14\times11) = 2\times160-29\times11 = 2\times160-29\times(17$$

3. Nous avons $\text{ppcm}(171, 160) = 171 \times 160 = 27360$.

4. Une solution particulière de $160u + 171v = 1$ est $31 \times 160 - 29 \times 171 = 1$. On fait la soustraction de $160u + 171v = 1$ par $31 \times 160 - 29 \times 171 = 1$ et nous obtenons $160(u - 31) + 171(v + 29) + 0$ c'est-à-dire $160(u - 31) = -171(v + 29)$. En particulier, 160 divise $-171(v + 29)$ et 160 est premier avec 171, d'après le théorème de Gauss 160 divise $-(v + 29)$. Autrement dit il existe un entier relatif k tel que $-(v + 29) = 160k$ ce qui se réécrit $v = -29 - 160k$; en substituant dans $160(u - 31) = -171(v + 29)$ nous obtenons $160(u - 31) = 171 \times 160k$ ou encore $u - 31 = 171k$ soit $u = 31 + 171k$. La réciproque étant toujours aussi évidente, l'ensemble des couples (u, v) recherchés est : $\{(31 + 171k, -29 - 160k) \mid k \in \mathbb{Z}\}$.

5. La décomposition de 171 en facteurs premiers est $171 = 32 \times 19$. La décomposition de 160 en facteurs premiers est $160 = 25 \times 5$.

6. On retrouve donc

$$\text{pgcd}(171, 160) = 1, \qquad \text{ppcm}(171, 160) = 2^5 \times 3^2 \times 5 \times 19 = 27360$$

Exercice 43

1. Calculer $\text{pgcd}(325, 520)$ par l'algorithme d'Euclide.
2. En déduire une identité de Bézout.
3. Calculer $\text{ppcm}(a, b)$.
4. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que : $au + bv = \text{pgcd}(a, b)$.
5. Donner la décomposition en facteurs premiers de a et b.
6. En déduire la décomposition en facteurs premiers de $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$, et retrouver les résultats des questions 1 et 3.

Éléments de réponse 43

1. Calcul du $\text{pgcd}(520, 325)$ par l'algorithme d'Euclide :

$$520 = 1 \times 325 + 195, \quad 325 = 1 \times 195 + 130, \quad 195 = 1 \times 130 + 65, \quad 130 = 2 \times 65$$

   Il en résulte que $\text{pgcd}(520, 325) = 65$.

2. Une identité de Bézout est :

$65 = 195-1\times130 = 195-1\times(325-1\times195) = -1\times325+2\times195 = -1\times325+2\times(520-1\text{Ö}325) = 2\times520-3\times325.$

3. Nous avons $\text{ppcm}(520, 325) = \frac{520\times325}{65} = 2600$.
4. Une solution particulière de $325u + 520v = 65$ est $-3 \times 325 + 2 \times 520 = 65$. On fait la soustraction de $325u + 520v = 65$ par $-3 \times 325 + 2 \times 520 = 65$; on obtient $325(u + 3) + 520(v-2) = 0$ ou encore $325(u+3) = -520(v-2)$, *i.e.* $5(u+3) = -8(v-2)$. En particulier 5 divise $-8(v - 2)$ et 5 est premier avec 8 ; d'après le théorème de Gauss 5 divise donc $-(v - 2)$. Autrement dit il existe un entier relatif k tel que $-(v - 2) = 5k$ ce qui se réécrit $v = 2 - 5k$. En substituant dans $5(u + 3) = -8(v - 2)$ nous obtenons $5(u + 3) = 8 \times 5k$ soit $u + 3 = 8k$ ou encore $u = -3 + 8k$. Les couples recherchés sont les $(-3 + 8k, 2 - 5k)$ avec $k \in \mathbb{Z}$.
5. La décomposition de 520 en facteurs premiers est : $520 = 2^3 \times 5 \times 13$;
   La décomposition de 325 en facteurs premiers est : $325 = 5^2 \times 13$.
6. On retrouve

$\text{pgcd}(325, 520) = 5\text{Ö}13 = 65, \quad \text{ppcm}(325, 520) = 2^3 \times 5^2 \times 13 = (2 \times 5) \times (2 \times 5) \times 2 \times 13 = 10 \times 10 \times 26 = 2$

Exercice 44

Soient a et b deux entiers positifs distincts et premiers entre eux. Calculer $\text{pgcd}(a + b, a - b)$ (discuter selon les parités de a et de b).

Éléments de réponse 44

Posons $\delta = \text{pgcd}(a + b, a - b)$. Alors δ divise $a + b$ et $a - b$. Par conséquent, δ divise la somme $(a + b) + (a - b) = 2a$ et la différence $(a + b) - (a - b) = 2b$. Il en résulte que δ divise $\text{pgcd}(2a, 2b) = 2\text{pgcd}(a, b) = 2$. Ainsi δ vaut 1 ou 2.

Notons que les entiers a et b étant premiers entre eux, ils ne sont pas tous les deux pairs.

- ◇ Premier cas : a et b sont impairs. Alors $a+b$ et $a-b$ sont pairs, donc leur pgcd est multiple de 2. Il s'en suit que $\text{pgcd}(a + b, a - b) = 2$.
- ◇ Second cas : a et b sont de parités différentes. Alors $a + b$ et $a - b$ sont impairs. Par suite $\delta \neq 2$. Nous en déduisons que $\text{pgcd}(a + b, a - b) = 1$.

Exercice 45

1. Trouver tous les entiers x, $y \in \mathbb{Z}$ tels que $15x - 22y = 1$.
2. Trouver tous les entiers x, $y \in \mathbb{Z}$ tels que $15x - 22y = 0$.
3. Trouver tous les entiers x, $y \in \mathbb{Z}$ tels que $15x + 24y = 5$.
4. Soit $c \in \mathbb{Z}$. Trouver tous les entiers x, $y \in \mathbb{Z}$ tels que $24x + 87y = c$.

Éléments de réponse 45

1. Les entiers 15 et 22 étant premiers entre eux, l'équation $15x - 22y = 1$ a des solutions dans $\mathbb{Z}$. Nous avons

$$22 = 15 \times 1 + 7 \iff \begin{pmatrix} 15 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 22 \\ 15 \end{pmatrix}$$
$$15 = 7 \times 2 + 1 \iff \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 15 \\ 7 \end{pmatrix}$$

   d'où

$$\begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 22 \\ 15 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 22 \\ 15 \end{pmatrix}$$

   En calculant la deuxième ligne du produit nous obtenons la relation de Bézout

$$-2 \times 22 + 3 \times 15 = 1.$$

   Ainsi le couple $(3, 2)$ est une solution de l'équation. Pour toute solution (x, y) nous avons $15x - 22y = 15 \times 3 - 22 \times 2$ ou encore $15(x-3) = 22(y-2)$. Par suite d'une part 22 divise le produit $15(x-3)$ et d'autre part 22 est premier à 15 ; il s'en suit que 22 divise $x - 3$, autrement dit il existe $k \in \mathbb{Z}$ tel que $x = 3 + 22k$. Il vient $22(y-2) = 15(x-3) = 15 \times 22k$, ou encore $y - 2 = 15k$, c'est-à-dire $y = 2 + 15k$. Finalement l'ensemble des solutions de l'équation $15x - 22y = 1$ dans $\mathbb{Z} \times \mathbb{Z}$ est

$$\{(3 + 22k, 2 + 15k) \,|\, k \in \mathbb{Z}\}$$

2. Le théorème de Gauss assure que si $15x = 22y$ alors y est multiple de 15, *i.e.* $y = 15k$, $k \in \mathbb{Z}$. Nous en déduisons que $x = 22k$. L'ensemble des solutions de l'équation $15x - 22y = 0$ dans $\mathbb{Z} \times \mathbb{Z}$ est

$$\{(22k, 15k) \,|\, k \in \mathbb{Z}\}$$

3. Notons que $\text{pgcd}(15, 24) = 3$ et 3 ne divise pas 5 ; l'équation n'a donc pas de solution.

4. Calculons $\text{pgcd}(24, 87)$:

$$\begin{aligned} 87 &= 3 \times 24 + 15 \\ 24 &= 1 \times 15 + 9 \\ 15 &= 1 \times 9 + 6 \\ 9 &= 1 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

   donc $\text{pgcd}(24, 87) = 3$. Si c n'est pas multiple de 3, alors l'équation n'a pas de solution.

   Supposons que c soit multiple de 3 ; écrivons c sous la forme $3c'$ avec $c' \in \mathbb{Z}$. L'équation $24x + 87y = c$ se réécrit $8x + 29y = c'$; à noter que 8 et 29 sont premiers entre eux. Nous

avons :

$$\begin{pmatrix} 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 29 \\ 8 \end{pmatrix} \qquad \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix}$$
$$\begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \qquad \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

et

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 29 \\ 8 \end{pmatrix} = () \begin{pmatrix} 29 \\ 8 \end{pmatrix}$$

Nous en déduisons la relation de Bézout : $8 \times 11 + 29 \times (-3) = 1$ et l'égalité

$$8 \times (11c') + 29 \times (-3c') = c'.$$

Ainsi le couple $(11c', -3c')$ est une solution de l'équation.

Si (x, y) est solution, alors $8(x - 11c') + 29(y + 3c') = 0$ et 29 divise $x - 11c'$. Autrement dit x s'écrit $11c' + 29k$ pour un certain k dans $\mathbb{Z}$.

Exercice 46

Posons

$$E = \left\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \,|\, \exists\, u \in \mathbb{Z},\, \exists\, v \in \mathbb{Z} \text{ tels que } \left\{ \begin{array}{c} x = u + v \\ y = 3u + 7v \end{array} \right.\right\}.$$

Montrer que pour tout $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ nous avons l'équivalence :

$$(x, y) \in E \Longleftrightarrow y - 3x \text{ est multiple de } 4$$

Éléments de réponse 46

Pour tous entiers x, y, u, v nous avons l'équivalence (méthode de Gauss)

$$\left\{ \begin{array}{l} u + v = x \\ 3u + 7v = y \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} 4v = y - 3x \\ 3u + 7v = y \end{array} \right.$$

La première équation du système dit que si $(x, y) \in E$, alors $y - 3x$ est multiple de 4.

Réciproquement, soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tel que $y - 3x = 4k$ avec $k \in \mathbb{Z}$. En posant $v = k$, $u = x - k$, nous avons $u + v = x$ et $3u + 7b = 3x - 3k + 7k = 3x + 4k = y$; par suite (x, y) appartient à E.

Exercice 47

Soient a_1, a_2, …, a_n des entiers non nuls. Si $\text{pgcd}(a_1, a_2, \ldots, a_n) = 1$, on dit que a_1, a_2, …, a_n sont premiers entre eux dans leur ensemble.

1. Montrer que si parmi les entiers a_1, a_2, …, a_n il y a en a deux qui sont premiers entre eux, alors a_1, a_2, …, a_n sont premiers entre eux dans leur ensemble.

   Trouver trois entiers positifs a, b et c tels que $\text{pgcd}(a,b,c) = 1$, $\text{pgcd}(a,b) \neq 1$, $\text{pgcd}(b,c) \neq 1$ et $\text{pgcd}(a,c) \neq 1$.
2. Montrer que $\text{pgcd}(a_1,a_2,a_3) = \text{pgcd}(a_1, \text{pgcd}(a_2,a_3))$.
3. Montrer qu'il existe des entiers relatifs u_1, u_2, …, u_n tels que
$$a_1u_1 + a_2u_2 + \ldots + a_nu_n = \text{pgcd}(a_1,a_2,\ldots,a_n).$$

Éléments de réponse 47

1. Quitte à réindicer les a_i supposons que a_1 et a_2 sont premiers entre eux. Le seul diviseur commun à a_1 et a_2 est 1 ; a fortiori le seul diviseur positif commun à tous les a_i est 1.

   Nous avons

   $\text{pgcd}(6,10) = 2$, $\text{pgcd}(6,15) = 3$, $\text{pgcd}(10,15) = 5$, $\text{pgcd}(6,10,15)1 =$
2. Posons $\delta = \text{pgcd}(a_1,a_2,a_3)$. Par définition δ divise a_2 et a_3 ; il en résulte que δ divise $\text{pgcd}(a_2,a_3)$. Puisque δ divise a_1, nous en déduisons que δ divise $\text{pgcd}(a_1, \text{pgcd}(a_2,a_3)$.

   Réciproquement, $\text{pgcd}(a_1, \text{pgcd}(a_2,a_3))$ divise a_1 et $\text{pgcd}(a_2,a_3)$ donc divise a_1, a_2 et a_3. Ainsi $\text{pgcd}(a_1, \text{pgcd}(a_2,a_3))$ divise $\delta = \text{pgcd}(a_1,a_2,a_3)$.

   Finalement $\delta = \text{pgcd}(a_1, \text{pgcd}(a_2,a_3))$.
3. Nous obtenons par récurrence à partir de la question 2. l'égalité

(1.2.1) $$\text{pgcd}(a_1,a_2,\ldots,a_n) = \text{pgcd}(\text{pgcd}(a_1,a_2,\ldots,a_{n-1}),a_n).$$

   Raisonnons encore par récurrence.

   - $n = 2$: le théorème de Bézout assure l'existence de deux entiers u_1 et u_2 tels que $a_1u_1 + a_2u_2 = \text{pgcd}(a_1,a_2)$.
   - Soit $n \geq 3$. Supposons (hypothèse de récurrence) qu'il existe des entiers relatifs u_1, u_2, …, u_{n-1} tels que $a_1u_1 + a_2u_2 + \ldots + a_{n-1}u_{n-1} = \text{pgcd}(a_1,a_2,\ldots,a_{n-1})$. Le théorème de Bézout assure l'existence de deux entiers relatifs v et u_n tels que
   $$\text{pgcd}(a_1,a_2,\ldots,a_{n-1})v + a_nu_n = \text{pgcd}(\text{pgcd}(a_1,a_2,\ldots,a_{n-1}),a_n).$$
   L'hypothèse de récurrence assure que
   $$(a_1u_1 + a_2u_2 + \ldots + a_{n-1}u_{n-1})v + a_nu_n = \text{pgcd}(\text{pgcd}(a_1,a_2,\ldots,a_{n-1}),a_n).$$
   soit
   $$a_1(u_1v) + a_2(u_2v) + \ldots + a_{n-1}(u_{n-1}v) + a_nu_n = \text{pgcd}(\text{pgcd}(a_1,a_2,\ldots,a_{n-1}),a_n).$$
   Finalement (1.2.1) conduit à
   $$a_1(u_1v) + a_2(u_2v) + \ldots + a_{n-1}(u_{n-1}v) + a_nu_n = \text{pgcd}(a_1,a_2,\ldots,a_n).$$

Exercice 48

Soient a et b des entiers strictement positifs tels que $a < b$. Déterminer le plus petit entier $k \geq 1$ tel que ka soit multiple de b.

Éléments de réponse 48

Pour tout $k \in \mathbb{Z}$ nous avons : b divise ak si et seulement si ak est multiple de b et de a si et seulement si ak est multiple de $\text{ppcm}(a, b)$ si et seulement si ak est multiple de $\frac{ab}{\text{pgcd}(a,b)}$ si et seulement si k est multiple de $\frac{b}{\text{pgcd}(a,b)}$.

Ainsi le plus petit entier positif k tel que ak soit multiple de a est donc $\frac{b}{\text{pgcd}(a,b)}$.

Exercice 49

Rappelons le résultat suivant que nous allons utiliser : soit n un entier au moins égal à 2. L'entier $\nu_p(a)$ désigne l'exposant de p dans la décomposition de a en facteurs premiers. Pour tout nombre premier p, nous avons

$$\nu_p(n!) = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \ldots + E\left(\frac{n}{p^k}\right) + \ldots$$

(où la somme n'a qu'un nombre fini de termes).

Rappelons que nous notons $\binom{n}{k}$ les coefficients binomiaux où $n \in \mathbb{N}$, $k \in \mathbb{N}$ et $0 \leq k \leq n$.
Soit p un nombre premier.

1. Supposons p impair. Soit k un enier tel que $0 < k < 2p$. Montrer que si $k \neq p$, alors $\binom{2p}{k}$ est multiple de p mais pas de p^2. Montrer que $\binom{2p}{p}$ n'est pas multiple de p.
2. Soit k un entier tel que $0 < k < p$. Soit r un entier positif. Montrer que $\binom{kp^r}{p^r}$ n'est pas multiple de p.

Éléments de réponse 49

Rappelons la formule $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ pour tous entiers n et k tels que $0 \leq k \leq n$.

1. Nous avons $\nu_p\left(\binom{2p}{k}\right) = \nu((2p)!) - \nu_k(p!) - \nu_p((2p-k)!)$. L'inégalité $2 < p$ conduit à $2p < p^2$ donc $E\left(\frac{2p}{p^2}\right) = 0$ et $\nu_p((2p)!) = E\left(\frac{2p}{p}\right) = 2$.
   - ◇ Supposons $0 < k < p$. Puisque $p > k$, p ne divise pas $k!$ donc $\nu_p(k!) = 0$. À partir de $p < 2p - k < 2p$ et $2p < p^2$ nous obtenons $2p - k < p^2$ d'où $E\left(\frac{2p-k}{p^2}\right) = 0$ et $\nu_p((2p-k)!) = E\left(\frac{2p-k}{p}\right) = 1$. Nous en déduisons que $\nu_p\left(\binom{2p}{k}\right) = 2 - 0 - 1 = 1$, donc $\binom{2p}{k}$ est multiple de p mais pas de p^2.
   - ◇ Supposons $p < k < 2p$. Nous avons $\binom{2p}{k} = \binom{2p}{2p-k}$ et $0 < 2p - k < p$. D'après le résultat ci-dessus $\binom{2p}{p}$ n'est pas multiple de p.
   - ◇ Nous avons $\binom{2p}{p} = \frac{(2p)!}{(p!)^2}$ donc $\nu_p\left(\binom{2p}{p}\right) = \nu_p((2p)!) - 2\nu_p(p!) = 2 - 2 \times 1 = 0$. Ainsi $\binom{2p}{p}$ n'est pas multiple de p.

2. L'inégalité $0 < k < p$ conduit à $kp^r < p^{r+1}$ d'où

$$\begin{aligned}\nu_p((kp^r)!) &= E\left(\frac{kp^r}{p}\right) + E\left(\frac{kp^r}{p^2}\right) + \ldots + E\left(\frac{kp^r}{p^r}\right)\\ &= k(1 + p + \ldots + p^{r-1})\\ &= ka\end{aligned}$$

où l'on a posé $a = 1 + p + \ldots + p^{r-1}$.

De même,

$$\nu_p((p^r)!) = 1 + p + \ldots + p^{r-1} = a \qquad \text{et} \qquad \nu_p() = (k-1)a$$

la deuxième égalité étant évidemment vraie aussi pour $k = 1$. Par suite

$$\nu_p\left(\binom{kp^r}{p^r}\right) = \nu_p((kp^r)!) - \nu_p((p^r)!) - \nu_p((kp^r - p^r)!) = ka - a - (k-1)a = 0.$$

Cela signifie que $\binom{kp^r}{p^r}$ n'est pas multiple de p.

Exercice 50

On définit la suite de Fibonacci $(F_n)_n$ en posant

$$F_0 = 0, \qquad F_1 = 1, \qquad \forall\, n \geq 1,\ F_{n+1} = F_n + F_{n-1}.$$

1. Montrer que pour tout entier $n \geq 1$ nous avons

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \tag{1.2.2}$$

2. En déduire que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
3. En utilisant (1.2.2) pour des entiers $n \geq 0$ et $p \geq 1$ montrer que

$$F_{n+p} = F_{n+1}F_p + F_nF_{p-1}.$$

4. Soient a et b des entiers tels que $0 \leq b < a$.

4.a) En utilisant 3. montrer que $\text{pgcd}(F_a, F_b) = \text{pgcd}(F_{a-b}, F_b)$.

4.b) En déduire que si r est le reste de la division de a par b, alors $\text{pgcd}(F_a, F_b) = \text{pgcd}(F_b, F_r)$.

4.c) Montrer que $\text{pgcd}(F_a, F_b) = F_{\text{pgcd}(a,b)}$.

Éléments de réponse 50

Remarquons que, d'après la relation de récurrence, tous les F_n sont des entiers positifs ou nuls car F_0 et F_1 le sont.

1. La relation de récurrence assure que $\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$ pour tout entier $n \geq 1$. Nous en déduisons que

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Nous avons $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ d'où

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}$$

Les colonnes d'une matrice s'obtenant en multipliant à droite par les vecteurs canoniques, les colonnes de $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$ sont (dans l'ordre) $\left(\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} \right)$ et $\left(\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \right)$ d'où l'égalité (1.2.2).

2. En prenant le déterminant de chaque membre de (1.2.2) nous obtenons :

$$\det \left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \right) = \det \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

soit

$$\left(\det \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right)^n = F_{n+1}F_{n-1} - F_n^2$$

ou encore $(-1)^n = F_{n+1}F_{n-1} - F_n^2$.

3. Si $n = 0$, l'égalité est visiblement vraie.

Supposons $n \geq 1$ et multiplions les égalités (1.2.2) pour n et p

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \begin{pmatrix} F_{p+1} & F_p \\ F_p & F_{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+p} = \begin{pmatrix} F_{n+p+1} & F_{n+p} \\ F_{n+p} & F_{n+p-1} \end{pmatrix}$$

Nous obtenons l'égalité cherchée en calculant, dans le produit de gauche, le coefficient situé sur la première ligne et la deuxième colonne.

4.a) D'après la relation de la question 3. les diviseurs communs à F_n et F_p sont les mêmes que les diviseurs communs à F_{n+p} et F_p : nous avons donc $\text{pgcd}(F_{n+p}, F_p) = \text{pgcd}(F_n, F_p)$. Appliquons ce résultat à $p = b$ et $n = a - b$, alors $n + p = a$ et

$$\text{pgcd}(F_a, F_b) = \text{pgcd}(F_{n+p}, F_p) = \text{pgcd}(F_n, F_p) = \text{pgcd}(F_{a-b}, F_b).$$

4.b) Soient q et r le quotient et le reste de la division de a par b : $a = bq + r$ et $0 \leq r < b$. Nous avons

$$\text{pgcd}(F_a, F_b) = \text{pgcd}(F_{a-b}, F_b) = \text{pgcd}(F_{a-2b}, F_b) = \ldots = \text{pgcd}(F_{a-qb}, F_b) = \text{pgcd}(F_r, F_b).$$

4.c) Soient $r_1 = r$, r_2, …, r_n les restes successifs non nuls dans l'algorithme d'Euclide pour a et b. Nous avons $r_{n+1} = 0$ et d'après 4.b)

$$\text{pgcd}(F_a, F_b) = \text{pgcd}(F_b, F_{r_1}) = \text{pgcd}(F_{r_1}, F_{r_2}) = \ldots = \text{pgcd}(F_{r_n}, F_{r_{n+1}}) = \text{pgcd}(F_{r_n}, F_0) = \text{pgcd}(F_{r_n}, 0) = F_{r_n}.$$

Puisque $r_n = \text{pgcd}(a, b)$ il vient $\text{pgcd}(F_a, F_b) = F_{\text{pgcd}(a,b)}$.

1.2.2. Congruences et $\mathbb{Z}/n\mathbb{Z}$. —

Exercice 51

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si un entier est congru à 0 modulo 6, alors il est divisible par 6.
2. Si le produit de deux entiers est congru à 0 modulo 6, alors l'un des deux est multiple de 6.
3. Si un entier est congru à 5 modulo 6 alors toutes ses puissances paires sont congrues à 1 modulo 6.
4. Si deux entiers sont congrus à 4 modulo 6, alors leur somme est congrue à 2 modulo 6.
5. Si deux entiers sont congrus à 4 modulo 6, alors leur produit est congru à 2 modulo 6.
6. Si un entier est congru à 4 modulo 6, alors toutes ses puissances sont aussi congrues à 4 modulo 6.

Éléments de réponse 51

1. Soit n un entier congru à 0 modulo 6. Il existe $k \in \mathbb{Z}$ tel que $n = 0 + 6k$ ce qui montre que 6 divise n. L'affirmation est vraie.
2. $2 \times 3 = 6 \equiv 0 \mod 6$ et pourtant ni 2, ni 3 ne sont congrus à 0 modulo 6. L'affirmation est fausse.
3. Soit n un entier congru à 5 modulo 6, il existe $k \in \mathbb{Z}$ tel que $n = 5 + 6k$; alors
$$n = -1 + 6 + 6k = -1 + 6(k + 1)$$
ce qui montre que n est congru à -1 modulo 6. Or si $n \equiv -1 \mod 6$, alors $n^{2p} \equiv (-1)^{2p} \mod 6$. Puisque $(-1)^{2p} = 1$, nous obtenons $n^{2p} \equiv 1 \mod 6$. Autrement dit les puissances paires de n sont congrues à 1 modulo 6. L'affirmation est vraie.
4. Si $a \equiv 4 \mod 6$ et $b \equiv 4 \mod 6$, alors $a + b \equiv 4 + 4 \mod 6$. Puisque $4 + 4 = 8 \equiv 2 \mod 6$, nous obtenons $a + b \equiv 2 \mod 6$. L'affirmation est vraie.
5. Si $a \equiv 4 \mod 6$ et $b \equiv 4 \mod 6$, alors $ab \equiv 4 \times 4 \mod 6$. Puisque $4 \times 4 = 16 \equiv 4 \mod 6$, nous obtenons $ab \equiv 4 \mod 6$. L'affirmation est fausse.
6. D'après le 5. $a^2 \equiv 4 \mod 6$. Par une récurrence très simple nous obtenons $a^n \equiv 4 \mod 6$. L'affirmation est vraie.

Exercice 52

Soit $n \in \mathbb{N}$ un entier.

1. Montrer que si n n'est divisible par aucun entier inférieur ou égal à $\sqrt{n}$, alors n est premier.
2. Montrer que les nombres $n!+2$, $n!+3$, …, $n!+n$ ne sont pas premiers.
3. En déduire que pour tout n il existe n entiers consécutifs non premiers.

Éléments de réponse 52

1. La contraposée de cette proposition est : si n n'est pas premier, alors n est divisible par au moins un nombre inférieur ou égal à $\sqrt{n}$. Démontrons cette assertion : n n'est pas premier, il existe donc $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $n = ab$ et $a \geq b$. Il en résulte que $n \geq b^2$; par suite $\sqrt{n} \geq b$.
2. $n!+2$ est divisible par 2, $n!+3$ est divisible par 3, $n!+n$ est divisible par n ; ces nombres ne sont pas premiers.
3. $n!+2$, $n!+3$, …, $n!+n$ sont $n-1$ entiers consécutifs non premiers : $\big((n+1)!+2$, $(n+1)!+3$, …, $(n+1)!+(n+1)\big)$.

Exercice 53

1. Trouver les entiers $x \in \mathbb{Z}$ tels que $261x+2$ soit multiple de 305.
2. Soient a, $b \in \mathbb{Z}$. Trouver les entiers $x \in \mathbb{Z}$ tels que $\begin{cases} x \equiv a \bmod 12 \\ x \equiv b \bmod 19 \end{cases}$

Éléments de réponse 53

1. Nous avons

$$305 = 261 \times 1 + 44, \quad 261 = 44 \times 5 + 41, \quad 44 = 41 \times 1 + 3, \quad 41 = 3 \times 13 + 2, \quad 3 = 2 \times 1 + 1$$

d'où

$$1 = 3-2\times1 = 3-(41-3\times13)\times1 = -41+3\times14 = -41+(44-41)\times14 = 44\times14+41\times(-15) = 44\times14+(261-44\times5$$

De manière équivalente on a

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -13 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 305 \\ 261 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -83 & 97 \\ 89 & -104 \end{pmatrix} \begin{pmatrix} 305 \\ 261 \end{pmatrix}$$

d'où la relation de Bézout en calculant la seconde ligne :

$$1 = 305 \times 89 - 104 \times 261.$$

Nous avons donc $-104\times261 \equiv 1 \bmod 305$. Pour tout $x \in \mathbb{Z}$ nous avons donc $261x+2$ est multiple de 305 si et seulement si $261x \equiv -2 \bmod 305$ si et seulement si $x \equiv (-104)\times(-2) \bmod 305$. Il en résulte que les solutions sont les entiers x congrus à 208 modulo 305.

2. Afin de trouver une solution particulière nous écrivons la relation de Bézout $12\times8-19\times5 = 1$ d'où

$$-19\times5 = -95 \equiv \begin{cases} 1 \bmod 12 \\ 0 \bmod 19 \end{cases} \qquad \text{et} \qquad 12\times8 = 96 \equiv \begin{cases} 0 \bmod 12 \\ 1 \bmod 19 \end{cases}$$

Nous en déduisons que l'entier $x_0 = -95a + 96b$ est congru à a modulo 12 et à b modulo 10. Donc x_0 est une solution particulière du système.

Les solutions sont les entiers congrus à x_0 modulo $19\times12 = 229$ c'est-à-dire les entiers de la forme $-95a + 96b + 228k$ où $k \in \mathbb{Z}$.

Exercice 54

Trouver les entiers $x \in \mathbb{Z}$ tels que $\begin{cases} x \equiv 1 \bmod 7 \\ x \equiv 4 \bmod 9 \\ x \equiv 3 \bmod 5 \end{cases}$

Éléments de réponse 54

Notons que $7\times13 + (9\times5)\times(-2) = 1$ est une relation de Bézout entre 7 et 9×5. Remarquons que $9\times4 + (7\times5)\times(-1) = 1$ est une relation de Bézout entre 9 et 7×5. De même $5\times(-25) + (7\times9)\times2 = 1$ est une relation de Bézout entre 5 et 7×9.

Nous en déduisons les congruences

$$(9\times5)\times(-2) = -90 \equiv \begin{cases} 1 \bmod 7 \\ 0 \bmod 9 \\ 0 \bmod 5 \end{cases}, \quad (7\times5)\times(-1) = -35 \equiv \begin{cases} 0 \bmod 7 \\ 1 \bmod 9 \\ 0 \bmod 5 \end{cases}, \quad (7\times9)\times(2) = 126 \equiv \begin{cases} 0 \mo \\ 0 \mo \\ 1 \mo \end{cases}$$

Par suite l'entier $x_0 = 1\times(-90) + 4\times(-35) + 3\times126 = 148$ est une solution particulière du système. Les solutions sont les entiers x tels que $x - x_0$ est congru à 0 modulo 7, 9 et 5, *i.e.* tels que $x - x_0$ est multiple de $\text{ppcm}(7,9,5) = 7\times9\times5 = 315$. Finalement les solutions sont les entiers de la forme $148 + 315k$ où k désigne un entier relatif.

Exercice 55

Soient a, $b \in \mathbb{Z}$. Considérons le système $\begin{cases} x \equiv a \bmod 21 \\ x \equiv b \bmod 24 \end{cases}$

À quelle condition existe-t-il au moins une solution ? En supposant vérifiée cette condition résoudre le système.

Éléments de réponse 55

Remarquons que $\text{pgcd}(21,24) = 3$. Soit x une solution du système : alors d'une part $x \equiv a \bmod 3$, d'autre part $x \equiv b \bmod 3$. Par suite $a \equiv b \bmod 3$. Pour que le système ait au moins une

solution il faut donc que a et b vérifient la condition $a \equiv b \bmod 3$, *i.e.* que $b-a$ soit multiple de 3.

Réciproquement supposons que $a \equiv b \bmod 3$. En appelant q le quotient de $b-a$ par 3, nous avons $b = a+3q$ et le système s'écrit

$$\begin{cases} x \equiv a \bmod 21 \\ x \equiv a+3q \bmod 24 \end{cases}$$

Si x est solution du système, alors $x-a$ est multiple de 21 donc de 3. Écrivons $x-a$ sous la forme $3y$. La première équation du système devient $x-a = 3y \equiv 0 \bmod 21$. Or $3y \equiv 0 \bmod 21$ si et seulement si $3y$ est multiple de 21 si et seulement si y est multiple de 7. La seconde équation du système devient $x-a = 3y \equiv 3q \bmod 24$. Or $3y \equiv 3q \bmod 24$ si et seulement si $3y-3q$ est multiple de 24 si et seulement si $y-q$ est multiple de 8. Puisque $-7 \equiv 1 \bmod 8$, l'entier $y_0 = -7q$ est solution. Les autres solutions sont les entiers $y = -7q+56k$ avec $k \in \mathbb{Z}$. Si x est solution du système initial, il existe donc un entier relatif k tel que

$$x = a+3(-7q+56k) = a-7(b-a)+3\times 56k = 8a-7b+168k.$$

On vérifie que ces entiers x sont effectivement solutions. Finalement les solutions sont les entiers de la forme $8a-7b+168k$, $k \in \mathbb{Z}$.

Exercice 56

1. Soit $a \in \mathbb{Z}$. Trouver les entiers relatifs x et y tels que $\begin{cases} 9x+2y \equiv a \\ 3x+4y \equiv 0 \end{cases} \bmod 10$.
2. Trouver les entiers relatifs x et y tels que $\begin{cases} 2x+6y \equiv 1 \\ 3x+14y \equiv 9 \end{cases} \bmod 35$

Éléments de réponse 56

1. En remarquant que $9 \equiv -1 \bmod 10$, nous avons les équivalences

$$\begin{cases} 9x+2y \equiv a \bmod 10 \\ 3x+4y \equiv 0 \bmod 10 \end{cases} \iff \begin{cases} -x+2y \equiv a \bmod 10 \\ 3x+4y \equiv 0 \bmod 10 \end{cases} \iff \begin{cases} x \equiv 2y-a \bmod 10 \\ 3(2y-a)+4y \bmod 10 \end{cases} \iff \begin{cases} x \equiv 2y-a \bmod \\ 3a \equiv 0 \bmod 1 \end{cases}$$

car $6y+4y = 10y \equiv 0 \bmod 10$. La condition $3a \equiv 0 \bmod 10$ est équivalente à a est multiple de 10 : c'est une condition nécessaire pour que le système ait au moins une solution.

Supposons que a soit multiple de 10. On peut choisir $y \in \mathbb{Z}$ quelconque et en posant $x = 2y-a$ on obtient un couple $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ solution. Le système a donc dans ce cas une infinité de solutions.

2. En soustrayant la première équation de la seconde, nous obtenons $x+8y \equiv 8 \bmod 35$, ce qui permet d'éliminer x dans la seconde équation :

$$\begin{cases} 2x+6y \equiv 1 \bmod 35 \\ 3x+14y \equiv 9 \bmod 35 \end{cases} \iff \begin{cases} x+8y \equiv 8 \bmod 35 \\ 3x+14y \equiv 9 \bmod 35 \end{cases} \iff \begin{cases} x+8y \equiv 8 \bmod 35 \\ 3(8-8y)+14y \equiv 9 \bmod 35 \end{cases} \iff \begin{cases} x+8y \equiv \\ 10y \equiv 15 \end{cases}$$

Dans le dernier système la seconde équation équivaut à $2y \equiv 3 \bmod 7$. Comme $2\times(-3) \equiv 1 \bmod 7$, cela équivaut, en multipliant par -3, à $y \equiv -9 \equiv 5 \bmod 7$. Si (x, y) est solution, il existe donc un entier $k \in \mathbb{Z}$ tel que :

$$y = 5 + 7k \text{ et } x \equiv 8 - 8y \equiv 8 - 40 - 56k \equiv -32 - 56k \equiv 3 + 14k \bmod 35$$

On vérifie que ces couples sont bien solutions : les solutions du système sont les couples $(3 + 14k + 35\ell, 5 + 7k)$ où k, $\ell \in \mathbb{Z}$.

Exercice 57

Soient a, b, m des entiers strictement positifs. Montrer que l'équation $ax \equiv b \bmod m$ a au moins une solution si et seulement si $\text{pgcd}(a, m)$ divise b.

Éléments de réponse 57

Posons $\delta = \text{pgcd}(a, m)$.

- ◇ Supposons qu'il existe $x \in \mathbb{Z}$ tel que $ax \equiv b \bmod m$. Il existe donc un entier relatif k tel que $ax = b + km$. Puisque δ divise a et m, δ divise $b = ax - km$.
- ◇ Réciproquement, supposons que δ divise b. Posons $a = \delta a'$, $m = \delta m'$ et $b = \delta b'$. Puisque a' et m' sont premiers entre eux, il existe x et y dans $\mathbb{Z}$ tels que $a'x - m'y = b'$ (en effet si α, β sont des entiers non nuls et γ un entier, alors les nombres de la forme $\alpha u + \beta v$, u, $v \in \mathbb{Z}$, sont les multiples de $\text{pgcd}(\alpha, \beta)$. Il en résulte que l'équation $\alpha x + \beta y = \gamma$ a des solutions si et seulement si γ est multiple de $\text{pgcd}(\alpha, \beta)$.). Ainsi $ax = da'x = dm'y + db' = my + b$; par suite $ax \equiv b \bmod m$.

Exercice 58

Soit $n \in \mathbb{N}$. Montrer que $5^n - 1$ est multiple de 12 si et seulement si n est pair.

Éléments de réponse 58

Remarquons que $5^n - 1$ est toujours multiple de 4 car $5^n \equiv 1^n = 1 \bmod 4$. Puisque $5 \equiv -1 \bmod 3$, nous avons $5^n \equiv (-1)^n \bmod 3$; nous en déduisons les équivalences

$$5^n - 1 \text{ est multiple de } 3 \iff 5^n \equiv 1 \bmod 3 \iff (-1)^n \equiv 1 \bmod 3 \iff n \text{ est pair.}$$

Aini $5^n - 1$ est multiple de 12 si et seulement si n est pair.

Exercice 59

1. Soit p un nombre premier et soit a un entier non multiple de p. Rappelons que, par convention, $a^0 = 1$. Montrer que la suite $(a^n \bmod p)_{n\in\mathbb{N}}$ est périodique.
2. Pour tout entier $n \in \mathbb{N}$ calculer $2^n \bmod 7$. Quelle est la période de la suite $(2^n \bmod 7)$?
3. Pour tout entier $n \in \mathbb{N}$ calculer $3^n \bmod 7$. Quelle est la période de la suite $(3^n \bmod 7)$?

Éléments de réponse 59

1. D'après le Corollaire du Théorème de Fermat (Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$ non multiple de p, nous avons $a^{p-1} \equiv 1 \bmod p$) on a $a^{p-1} \equiv 1 \bmod p$. Ainsi $a^0 \equiv a^{p-1} \bmod p$, et par conséquent $a^{(p-1)+k} = a^{p-1}a^k \equiv a^k$ quel que soit $k \in \mathbb{N}$: la suite $(a^n \bmod p)_{n\in\mathbb{N}}$ a donc pour période $p-1$. Ce n'est peut-être pas la plus petite période, comme le montre la question suivante.
2. Nous avons $2^3 \equiv 1 \bmod 7$, donc $2^{3+k} = 2^3 2^k \equiv 2^k \bmod 7$: la suite a pour période 3. C'est la plus petite période car $2^2 \not\equiv 2^0$ mpd 7. Soit $n \in \mathbb{N}$. Désignons par r le reste de la division de n par 3. Il existe $k \in \mathbb{N}$ tel que $n = 3k + r$ et nous avons
$$2^n = 2^{3k+r} = (2^3)^k\, 2^r \equiv 2^r \bmod 7.$$
3. De même nous avons $3^6 \equiv 1 \bmod 7$ d'où $3^{6+k} = 3^k 3^6 \equiv 3^k \bmod 7$. Ainsi la suite a pour période 6. Elle n'a pas de période plus petite car pour tout entier i tel que $1 \leq i \leq 5$, 3^k n'est pas congru à 1 modulo 7.

   Soit $n \in \mathbb{N}$. Désignons par r le reste de la division de n par 6. Il existe $k \in \mathbb{N}$ tel que $n = 6k + r$ et
$$3^n = 3^{6k+r} = (3^6)^k\, 3^r \equiv 3^r \bmod 7.$$
   Nous en déduisons le tableau des valeurs de $3^n \bmod 7$:

n	$6k$	$6k+1$	$6k+2$	$6k+3$	$6k+4$	$6k+5$
$3^n \bmod 7$	1	3	2	6	4	5

Exercice 60

Calculer $2^{500} \bmod 13$ et $26^{1000} \bmod 17$.

Éléments de réponse 60

◇ Puisque 13 est premier et que 2 n'est pas multiple de 13, nous avons $2^{12} \equiv 1 \bmod 13$ d'après le Corollaire du Théorème de Fermat (Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$ non multiple de p, nous avons $a^{p-1} \equiv 1 \bmod p$). Écrivons la division euclidienne de 500 par 12 : $500 = 12 \times 41 + 8$. Par suite
$$2^{500} = 2^{12\times 41+8} = 2^{12\times 41}\, 2^8 = (2^{12})^{41}\, 2^8 \equiv 1^{41} 2^8 \equiv 2^8 \bmod 13.$$
Or $2^4 = 16 \equiv 3 \bmod 13$ donc $2^8 = (2^4)^2 \equiv 3^2 \equiv 9 \bmod 13$. Par conséquent $2^{500} \equiv 9 \bmod 13$.

◇ Comme $26 \equiv 9 \bmod 17$ nous avons $26^{1000} \equiv 9^{1000} \bmod 17$. Étant donné que 17 est premier et que 9 n'est pas multiple de 17, nous avons $9^{16} \equiv 1 \bmod 17$ d'après le Corollaire du Théorème de Fermat (Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$ non multiple de p, nous avons $a^{p-1} \equiv 1 \bmod p$). Écrivons la division euclidienne de 1000 par 16 : $1000 = 16 \times 62 + 8$, d'où
$$9^{1000} = 9^{16\times 62+8} = (9^{16})^{62}\, 9^8 = 1^{62}\, 9^8 \equiv 9^8 \bmod 17.$$

Calculons 9^8 mod 17 : nous avons $9^2 \equiv 13 \equiv -4 \bmod 17$ d'où

$$9^4 = (9^2)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \bmod 17$$

et finalement $9^8 = (9^4)^2 \equiv (-1)^2 \equiv 1 \bmod 17$. Il en résulte que $26^{1000} \equiv 1 \bmod 17$.

Exercice 61

Soit p un nombre premier impair et soit $t \in \mathbb{N}$. Montrer que pour tout entier $k \geq 0$ nous avons $(1+tp)^{p^k} \equiv 1 + tp^{k+1} \bmod p^{k+2}$.

Éléments de réponse 61

Raisonnons par récurrence sur k.

Si $k = 0$, la formule est vraie car $p^0 = 1$ donc les deux membres sont égaux à $1 + tp$.

Soit k un entier positif ou nul tel que la formule est vraie. Nous avons

$$(1+tp)^{p^{k+1}} = (1+tp)^{p^k \times p} = \left((1+tp)^{p^k}\right)^p$$

Par hypothèse $(1+tp)^{p^k} \equiv 1 + tp^{k+1} \bmod p^{k+2}$; il existe donc un entier $a \in \mathbb{Z}$ tel que

$$(1+tp)^{p^k} = 1 + tp^{k+1} + ap^{k+2} = 1 + p^{k+1}(t+ap).$$

Il vient

$$\begin{aligned}
(1+tp)^{p^{k+1}} &= \left((1+tp)^{p^k}\right)^p \\
&= \left(1 + p^{k+1}(t+ap)\right)^p \\
&= 1 + p\,p^{k+1}(t+ap) + \sum_{j=2}^{p-1} \binom{p}{j} p^{(k+1)j}(t+ap)^j + p^{(k+1)p}(t+ap)^p/
\end{aligned}$$

La somme des deux premiers termes est

$$1 + p^{k+2}(t+ap) = 1 + tp^{k+2} + ap^{k+3} \equiv 1 + tp^{k+2} \bmod p^{k+3}.$$

Par conséquent il suffit de montrer que chacun des autres termes est multiple de p^{k+3}.

- ◇ Sous le signe de sommation chaque coefficient $\binom{p}{j}$ est multiple de p (en effet rappelons que si p est un nombre premier, pour tout entier k tel que $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est un multiple de p). Par suite pour $2 \leq j \leq p-1$, $\binom{p}{j} p^{(k+1)j}(t+ap)^j$ est multiple de $pp^{(k+1)\times 2} = p^{1+2k+2} = p^{2k+3}$ donc de p^{k+3} car $2k+3 \geq k+3$.
- ◇ Concentrons-nous sur le dernier terme : comme p est un nombre impair, nous avons $p \geq 3$ d'où $(k+1)p = pk + p \geq 3k + 3 \geq k + 3$. Ce dernier terme est donc aussi multiple de p^{k+3}.

Nous avons montré que $(1+tp)p^{k+1} \equiv 1 + tp^{k+2} \bmod p^{k+3}$: d'après le principe de récurrence l'égalité demandée est vraie quel que soit $k \geq 0$.

1.3. En construction

Exercice 62

1. L'assertion suivante est-elle vraie ? fausse ? pourquoi ?
   La soustraction est une loi de composition interne dans $\mathbb{Z}$.
2. L'assertion suivante est-elle vraie ? fausse ? pourquoi ?
   0 est élément neutre de la soustraction dans $\mathbb{Z}$.
3. L'assertion suivante est-elle vraie ? fausse ? pourquoi ?
   La soustraction dans $\mathbb{Z}$ est associative.
4. L'assertion suivante est-elle vraie ? fausse ? pourquoi ?
   0 est élément neutre pour l'addition dans $\mathbb{N}$.
5. L'assertion suivante est-elle vraie ? fausse ? pourquoi ?
   L'addition est associative dans $\mathbb{N}$.

Éléments de réponse 62

Exercice 63

On définit une loi de composition interne $\star$ sur $\mathbb{R}$ par :

$$\forall\, a, b \in \mathbb{R}\,, \quad a \star b \;=\; \ln(e^a + e^b)\,.$$

1. Cette loi est-elle associative ?
2. Cette loi est-elle commutative ?
3. Possède-t-elle un élément neutre ?

Éléments de réponse 63

1. Soient x, y et z trois réels. Alors
   - ◇ d'une part
   $$\begin{aligned}(x * y) * z &= (\ln(\exp(x) + \exp(y))) * z \\ &= \ln\big(\exp(\ln(\exp(x) + \exp(y))) + \exp(z)\big) \\ &= \ln\big(\exp(x) + \exp(y) + \exp(z)\big)\end{aligned}$$
   - ◇ et d'autre part
   $$\begin{aligned}x * (y * z) &= x * \big(\ln(\exp(y)) + \ln(\exp(z))\big) \\ &= \ln\big(\exp(x) + \exp(\ln(\exp(y)) + \ln(\exp(z)))\big) \\ &= \ln\big(\exp(x) + \exp(y) + \exp(z)\big).\end{aligned}$$
   En particulier $(x * y) * z = x * (y * z)$: la loi $*$ est associative.
2. Soient x et y deux réels. Alors

- ◇ d'une part $x * y = \ln(\exp(x) + \exp(y))$,
- ◇ d'autre part $y * x = \ln(\exp(y) + \exp(x)) = \ln(\exp(x) + \exp(y))$.

En partiulier, $x * y = y * x$! la loi $*$ est commutative.

3. Supposons qu'il existe un élément neutre r, *i.e.* un réel r tel que pour tout $x \in \mathbb{R}$ nous ayons $x * r = r * x = x$. En particulier $r * x = x$, *i.e.* $\ln(\exp(x) + \exp(r)) = x$. Or si $\ln(\exp(x) + \exp(r)) = x$, alors $\exp\big(\ln(\exp(x) + \exp(r))\big) = \exp(x)$ qui se réecrit $\exp(x) + \exp(r) = \exp(x)$, soit $\exp(r) = 0$: contradition avec $\exp(u) > 0$ pour tout $u \in \mathbb{R}$. La loi de composition $*$ n'admet donc pas d'élément neutre.

Exercice 64

Pour x, $y \in [0, 1]$, on définit $\star$ par $x \star y = x + y - xy$.

1. Montrer que $\star$ définit une loi de composition interne sur $[0, 1]$.
2. Cette loi est-elle associative ? Commutative ?
3. Cette loi est-elle commutative ?
4. Possède-t-elle un élément neutre ?
5. Quels sont les éléments inversibles ?
6. Soit $\alpha \in [0, 1]$. Montrer que $[\alpha, 1]$ est stable par $\star$ (soit : $\forall x, y \in [\alpha, 1]$, $x \star y \in [\alpha, 1]$).

Éléments de réponse 64

1. Montrons que $\star$ définit une loi de composition interne sur $[0, 1]$. Il s'agit de vérifier que si x, y appartiennent à $[0, 1]$, alors $x \star y$ appartient à $[0, 1]$. Soient x, y dans $[0, 1]$.
   - ◇ Montrons que $x \star y = x + y - xy \geq 0$: comme $x \geq 0$ et $0 \leq y \leq 1$ nous avons $xy \leq x$ et $-xy \geq -x$. Par suite $x \star y = x + y - xy \geq x + y - x = y \geq 0$.
   - ◇ Montrons qe $x \star y = x + y - xy \leq 1$: nous avons $(x - 1)(1 - y) \leq 0$, c'est-à-dire $x - xy - 1 + y \leq 0$, *i.e.* $x + y - xy \leq 1$.
2. Soient x, y et z trois réels dans $[0, 1]$. Alors
   - ◇ d'une part
   $$\begin{aligned} x \star (y \star z) &= x \star (y + z - yz) \\ &= x + y + z - yz - x(y + z - yz) \\ &= x + y + z - xy - xz - yz + xyz, \end{aligned}$$
   - ◇ d'autre part
   $$\begin{aligned} (x \star y) \star z &= (x + y - xy) \star z \\ &= x + y - xy + z - (x + y - xy)z \\ &= x + y + z - xy - xz - yz + xyz. \end{aligned}$$

   En particulier $x \star (y \star z) = (x \star y) \star z$: la loi $\star$ est associative.

3. Soient x et y deux réels dans $[0,1]$. Alors
   - ◇ d'une part $x \star y = x + y - xy$,
   - ◇ d'autre part $y \star x = y + x - yx = x + y - xy$.

   En particulier $x \star y = y \star x$ et cette loi est commutative.
4. Supposons que cette loi possère un élément neutre e. Alors pour tout $x \in [0,1]$ nous avons $x \star e = e \star x = x$. Mais $x \star e = x$ se réecrit $x + e - x \cdot e = x$, *i.e.* $e(1-x) = 0$. Nous avons $e(1-x) = 0$ pour tout $x \in [0,1]$ si et seulement si $e = 0$. Ainsi 0 est l'élément neutre de la loi $\star$; vérifions : soit $x \in [0,1]$, alors
$$\begin{cases} x \star 0 = x + 0 - x \cdot 0 = x \\ 0 \star x = 0 + x - 0 \cdot x = x \end{cases}$$
5. Déterminons les éléments inversibles. L'élément $x \in [0,1]$ est inversible s'il existe $x' \in [0,1]$ tel que $x \star x' = x' \star x = 0$ ce qui se réecrit $x + x' - xx' = 0$ ou encore $x = x'(x-1)$. Si $x \neq 1$, alors nous obtenons $x' = \frac{x}{x-1}$. Si $0 < x < 1$, alors $-1 < x - 1 < 0$ et $x' = \frac{x}{x-1} < 0$; en particulier x' n'appartient pas à $[0,1]$. Ainsi si $0 < x < 1$, alors x n'est pas inversible. Si $x = 0$, alors $x' = \frac{x}{x-1} = 0$ et x est un élément inversible. Si $x = 1$, alors $x = x'(x-1)$ équivaut à $1 = x' \cdot 0$ soit $1 = 0$. Par suite 1 n'est pas inversible.
6. Soient $\alpha \in [0,1]$ et x, y dans $[\alpha, 1]$.
   - ◇ Montrons que $x \star y \leq 1$. Nous avons $(x-1)(1-y) \leq 0$, *i.e.* $x - xy - 1 + y \leq 0$, soit $\underbrace{x + y - xy}_{x \star y} \leq 1$.
   - ◇ Montrons que $x \star y \geq \alpha$. D'une part $x \geq \alpha \geq 0$, d'autre part $\alpha \leq y \leq 1$; par suite $xy \leq x$ et $-xy \geq -x$. Il en résulte que
$$x * y = x + y - xy \geq x + y - x = y \geq \alpha.$$
   Finalement $x * y$ appartient à $[\alpha, 1]$.

Exercice 65

Dans cet exercice, on souhaite vérifier, lorsque $n = 4$, la propriété suivante : si E est un ensemble muni d'une loi associative $\star$ et $x_1, \ldots, x_n \in E$, alors $x_1 \star \ldots \star x_n$ est défini sans ambiguité (tous les parenthésages possibles conduisant au même résultat). Pour cela, montrer que si a, b, c, $d \in E$, alors
$$a \star ((b \star c) \star d) = ((a \star b) \star c) \star d,$$
et
$$(a \star b) \star (c \star d) = ((a \star b) \star c) \star d,$$
puis conclure.

Éléments de réponse 65

Soient a, b, c et d dans E ; alors

- ◇ d'une part $a \star \big((b \star c) \star d\big) = \big(a \star (b \star c)\big) \star d = \big((a \star b) \star c\big) \star d = (a \star b) \star (c \star d)$,
- ◇ d'autre part $\big((a \star b) \star c\big) \star d = (a \star b) \star (c \star d)$

d'où $a \star \big((b \star c) \star d\big) = (a \star b) \star (c \star d) = \big((a \star b) \star c\big) \star d$. Finalement $a \star b \star c \star d$ est défini sans ambiguïté.

Exercice 66

Considérons la loi de composition interne suivante : $f\colon \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*,\ (a,b) \mapsto f(a,b) = a^b$.

1. La loi f est-elle commutative ?
2. La loi f est-elle associative ?
3. La loi f possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 66

1. Cette loi n'est pas commutative ; en effet $f(1,2) = 1^2 = 1 \neq f(2,1) = 2^1 = 2$.
2. Cette loi n'est pas associative ; en effet d'une part
$$f\big(f(2,1),2\big) = f(2^1,2) = f(2,2) = 2^2 = 4$$
et d'autre part
$$f\big(2,f(1,2)\big) = f(2,1^2) = f(2,1) = 2^1 = 2;$$
en particulier $f\big(f(2,1),2\big) \neq f\big(2,f(1,2)\big)$.
3. Supposons que cette loi possède un élément neutre ; alors pour tout x dans $\mathbb{N}^*$ nous avons $f(r,x) = f(x,r) = x$. L'égalité $f(x,r) = x$ se réecrit $x^r = x$ ou encore $x^{r-1} = 1$. Or $x^{r-1} = 1$ pour tout $x \in \mathbb{N}^*$ conduit à $r-1 = 0$ soit $r = 1$. Réecrivons alors $f(r,x) = x$:
$$f(r,x) = x \iff r^x = x \iff 1^x = x \iff 1 = x :$$
contradiction. Cette loi n'admet donc pas d'élément neutre et par conséquent pas d'élément inversible.

Exercice 67

Considérons la loi de composition interne : $\mathrm{pgcd}\colon \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*,\ (a,b) \mapsto \mathrm{pgcd}(a,b)$.

1. Cette loi est-elle commutative ?
2. Cette loi est-elle associative ?
3. Cette loi possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 67

1. Soient a et b deux entiers naturels non nuls. Soient D_a l'ensemble des diviseurs de a et D_b l'ensemble des diviseurs de b ; l'ensemble $D_a \cap D_b$ est l'ensemble des diviseurs communs de a et b. Ce sous-ensemble non vide de $\mathbb{N}$ (en effet 1 appartient à $D_a \cap D_b$) et majoré admet donc un plus grand élément appelé plus grand diviseur commun de a et b et noté $\text{pgcd}(a, b)$. La commutativité de la loi résulte du fait que $D_a \cap D_b = D_b \cap D_a$.
2. En reprenant les notations précédentes nous avons $(D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c)$ d'où l'associativité.
3. Cette loi n'admet pas d'élément neutre et par suite pas d'élément inversible.

Exercice 68

Considérons la loi de composition interne : $\text{ppcm} : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*,\ (a, b) \mapsto \text{ppcm}(a, b)$.

1. Cette loi est-elle commutative ?
2. Cette loi est-elle associative ?
3. Possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 68

1. Soient a et b deux entiers naturels non nuls, M_a l'ensemble des multiples de a et M_b l'ensemble des multiples de b. L'ensemble $M_a \cap M_b$ est l'ensemble des multiples communs de a et de b. Le sous-ensemble $M_a \cap M_b$ est un ensemble non vide de $\mathbb{N}^*$ (en effet ab appartient à $M_a \cap M_b$) et minoré. Il en résulte que $M_a \cap M_b$ admet un plus petit élément appelé plus petit commun multiple de a et b et noté $\text{ppcm}(a, b)$. La commutativité de la loi résulte de l'égalité $M_a \cap M_b = M_b \cap M_a$.
2. Cette loi est associative. Reprenons les notations précédentes ; l'égalité $M_a \cap (M_b \cap M_c) = (M_a \cap M_b) \cap M_c$ entraîne l'associativité de la loi.
3. Cette loi admet pour élément neutre 1 ; en effet pour tout $a \in \mathbb{N}^*$ nous avons en reprenant les notations précédentes
$$M_a \cap M_1 = M_a \cap \mathbb{N}^* = M_a$$
d'où $\text{ppcm}(a, 1) = a$ pour tout $a \in \mathbb{N}^*$.

   L'élément $a \in \mathbb{N}^*$ est inversible s'il existe $b \in \mathbb{N}^*$ tel que le plus petit élément de $M_a \cap M_b = 1$, *i.e.* tel que $\text{ppcm}(a, b) = \text{ppcm}(b, a) = 1$. Il en résulte que l'unique élément inversible est 1 qui admet pour inverse 1.

Exercice 69

Considérons la loi de composition interne suivante. Soit $\mathcal{P}$ le plan cartésien et A, $B \in \mathcal{P}$. On pose $m(A, B) = I$, le milieu de $[A, B]$.

1. Étudier si cette loi est commutative.
2. Étudier si cette loi est associative.

3. Possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 69

Soit $(O, \overrightarrow{u}, \overrightarrow{v})$ un repère orthonormé de $\mathcal{P}$; soit (x_A, y_A) (resp. (x_B, y_B)) les coordonnées de A (resp. B dans ce repère. Alors $A * B = M$ se réecrit $(x_A, y_A) * (x_B, y_B) = \left(\frac{x_A+y_A}{2}, \frac{x_B+y_B}{2}\right) = (x_M, y_M)$.

1. Cette loi est commutative : soient A, B dans $\mathcal{P}$ alors
$$\begin{aligned}(x_A, y_A) * (x_B, y_B) &= \left(\frac{x_A + y_A}{2}, \frac{x_B + y_B}{2}\right)\\ &= \left(\frac{x_B + y_B}{2}, \frac{x_A + y_A}{2}\right)\\ &= (x_B, y_B) * (x_A, y_A).\end{aligned}$$

2. Remarquons que d'une part
$$\begin{aligned}(2,2) * \big((0,1) * (1,0)\big) &= (2,2) * \left(\frac{0+1}{2}, \frac{1+0}{2}\right)\\ &= (2,2) * \left(\frac{1}{2}, \frac{1}{2}\right)\\ &= \left(\frac{2+\frac{1}{2}}{2}, \frac{2+\frac{1}{2}}{2}\right)\\ &= \left(\frac{5}{4}, \frac{5}{4}\right)\end{aligned}$$
et d'autre part
$$\begin{aligned}\big((2,2) * (0,1)\big) * (1,0) &= \left(\frac{2+0}{2}, \frac{2+1}{2}\right) * (1,0)\\ &= \left(1, \frac{3}{2}\right) * (1,0)\\ &= \left(\frac{1+1}{2}, \frac{\frac{3}{2}+0}{2}\right)\\ &= \left(1, \frac{3}{4}\right).\end{aligned}$$
En particulier $(2,2)*\big((0,1)*(1,0)\big) \neq \big((2,2)*(0,1)\big)*(1,0)$: cette loi n'est pas associative.

3. Supposons qu'il existe un élément neutre (x_E, y_E). Alors pour tout (x_A, y_A) nous avons
$$(x_A, y_A) * (x_E, y_E) = (x_E, y_E) * (x_A, y_A) = (x_A, y_A).$$
Mais $(x_A, y_A) * (x_E, y_E) = (x_A, y_A)$ se réécrit $\left(\frac{x_A+x_E}{2}, \frac{y_A+y_E}{2}\right) = (x_A, y_A)$ soit $(x_E, y_E) = (x_A, y_A)$ pour tout (x_A, y_A) : contradiction. Ainsi la loi $*$ n'admet pas d'élément neutre et donc pas d'élément inversible.

Exercice 70

Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes ses parties. Considérons la loi de composition interne : $f\colon \mathcal{P}(E)\times\mathcal{P}(E)\to\mathcal{P}(E),\ (A,B)\mapsto f(A,B)=A\cap B$.

1. Cette loi est-elle commutative ?
2. Cette loi est-elle associative ?
3. Possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 70

1. Cette loi est commutative : soient A et B deux éléments de $\mathcal{P}(E)$, alors
$$f(A,B)=A\cap B=B\cap A=f(B,A).$$
2. Cette loi est associative : soient A, B et C trois éléments de $\mathcal{P}(E)$, alors
$$A*(B*C)=f(A,f(B,C))=f(A,B\cap C)=A\cap(B\cap C)=A\cap B\cap C$$
et
$$(A*B)*C=f(f(A,B),C)=f(A\cap B,C)=(A\cap B)\cap C=A\cap B\cap C.$$
En particulier, $A*(B*C)=(A*B)*C$.
3. Notons que pour tout A dans $\mathcal{P}(E)$ nous avons d'une part $A*E=f(A,E)=A\cap E=A$ et d'autre part $E*A=f(E,A)=E\cap A=A$; de plus E appartient à $\mathcal{P}(E)$. Il s'en suit que E est l'élément neutre de la loi f.

   L'unique élément inversible est E et son inverse est E. En effet rappelons que $A\in\mathcal{P}(E)$ est inversible s'il existe $B\in\mathcal{P}(E)$ tel que $f(A,B)=f(B,A)=E$. Or $f(A,B)=f(B,A)=E$ se réecrit $A\cap B=E$. Mais $A\cap B\subseteq A$ d'où $E\subseteq A$ et $A=E$ (car $A\subseteq E$). Alors $A\cap E=E$ se réecrit $E\cap B=E$ ce qui implique $B=E$.

Exercice 71

Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes ses parties. Considérons la loi de composition interne : $f\colon \mathcal{P}(E)\times\mathcal{P}(E)\to\mathcal{P}(E),\ (A,B)\mapsto f(A,B)=A\cup B$.

1. Cette loi est-elle commutative ?
2. Cette loi est-elle associative ?
3. Cette loi possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 71

1. Cette loi est commutative : soient A, B dans $\mathcal{P}(E)$ alors d'une part $f(A,B)=A\cup B$, d'autre part $f(B,A)=B\cup A=A\cup B$ d'où $f(A,B)=f(B,A)$.
2. Cette loi est associative : soient A, B et C dans $\mathcal{P}(E)$, alors

◇ d'une part $A*(B*C) = f(A, f(B,C)) = f(A, B\cup C) = A\cup(B\cup C) = A\cup B\cup C$,

◇ d'autre part $(A*B)*C = f(f(A,B),C) = f(A\cup B, C) = (A\cup B)\cup C = A\cup B\cup C$

d'où $A*(B*C) = (A*B)*C$

3. Cette loi admet un élément neutre : pour tout $A\in\mathcal{P}(E)$ nous avons $f(A,\emptyset) = f(\emptyset, A) = A\cup\emptyset = A$.

   Il y a un unique élément inversible $\emptyset$ d'inverse $\emptyset$. En effet un élément A est inversible s'il existe B dans $\mathcal{P}(E)$ tel que $f(A,B) = f(B,A) = \emptyset$, *i.e.* tel que $A\cup B = \emptyset$. Or $A\cup B \supseteq A$ donc si $A\cap B = \emptyset$, alors $\emptyset\subseteq A$ et $A = \emptyset$. Alors $A\cup B = \emptyset$ se réecrit $\emptyset\cup B = \emptyset$ d'où $B = \emptyset$.

Exercice 72

Soit E un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes ses parties. Considérons la loi de composition interne : $f\colon \mathcal{P}(E)\times\mathcal{P}(E)\to\mathcal{P}(E),\ (A,B)\mapsto f(A,B) = A\smallsetminus B := A\cap B^c$.

1. Cette loi est-elle commutative ?
2. Cette loi est-elle associative ?
3. Possède-t-elle un élément neutre et quels sont les éléments inversibles le cas échéant ?

Éléments de réponse 72

1. Cette loi n'est pas commutative : en effet $f(E,\emptyset) = E\cap\emptyset^c = E\cap E = E$ et $f(\emptyset, E) = \emptyset\cap E^c = \emptyset\cap\emptyset = \emptyset$. En particulier $f(E,\emptyset)\neq f(\emptyset, E)$.
2. Cette loi n'est pas associative : soit $A\in\mathcal{P}(E)\smallsetminus\{E,\emptyset\}$, alors

   ◇ d'une part

   $$f(E, f(A,A)) = f(E, A\cap A^c) = f(E,\emptyset) = E\cap\emptyset^c = E\cap E = E,$$

   ◇ d'autre part

   $$f(f(E,A),A) = f(E\cap A^c, A) = f(A^c, A) = A^c\cap A^c = A^c.$$

   Puisque A appartient à $\mathcal{P}(E)\smallsetminus\{E,\emptyset\}$, nous avons $A^c\neq E$, c'est-à-dire $f(E, f(A,A))\neq f(f(E,A),A)$.
3. Cette loi admet un élément neutre s'il existe $N\in\mathcal{P}(E)$ tel que pour tout $A\in\mathcal{P}(E)$ on ait $f(A,N) = f(N,A) = A$, *i.e.* $A\cap N^c = N\cap A^c = A$. L'égalité $A\cap N^c = A$ implique $N^c\subseteq A$ d'où $A^c\subseteq N$. À partir de $A^c\subseteq N$ nous obtenons $A^c\cap N = A^c$ mais par ailleurs nous savons que $A^c\cap N = A$. Il en résulte que $A^c = A$: absurde. Ainsi cette loi n'admet ni élément neutre, ni inversible.

Exercice 73

1. L'ensemble $\left\{\frac{a}{5^n}\,|\,a\in\mathbb{Z},\ n\in\mathbb{N}\right\}$ muni de l'addition des réels est-il un groupe ?
2. L'ensemble $\left\{\frac{a}{3^n}\,|\,a\in\mathbb{Z},\ n\in\mathbb{N}\right\}$ muni de l'addition des réels est-il un groupe ?

3. L'ensemble $\{a\sqrt{5} \,|\, a \in \mathbb{Z}\}$ muni de l'addition des réels est-il un groupe ?
4. L'ensemble $\{a\sqrt{5} \,|\, a \in \mathbb{N}\}$ muni de l'addition des réels est-il un groupe ?
5. L'ensemble $\{a\sqrt{2} + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$ muni de l'addition des réels est-il un groupe ?
6. L'ensemble $\{a\sqrt{2} + b\sqrt{5} \,|\, a \in \mathbb{Z}, b \in \mathbb{N}\}$ muni de l'addition des réels est-il un groupe ?

à compléter

Éléments de réponse 73

1. L'ensemble $\{\frac{a}{5^n} \,|\, a \in \mathbb{Z}, n \in \mathbb{N}\}$ muni de l'addition des réels est un groupe.
2. L'ensemble $\{\frac{a}{3^n} \,|\, a \in \mathbb{Z}, n \in \mathbb{N}\}$ muni de l'addition des réels est un groupe.
3. L'ensemble $\{a\sqrt{5} \,|\, a \in \mathbb{Z}\}$ muni de l'addition des réels est un groupe.
4. L'ensemble $\{a\sqrt{5} \,|\, a \in \mathbb{N}\}$ muni de l'addition des réels n'est pas un groupe.
5. L'ensemble $\{a\sqrt{2} + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$ muni de l'addition des réels est un groupe.
6. L'ensemble $\{a\sqrt{2} + b\sqrt{5} \,|\, a \in \mathbb{Z}, b \in \mathbb{N}\}$ muni de l'addition des réels n'est pas un groupe.

Exercice 74

1. L'ensemble $\{1, -1\}$ muni de la multiplication des réels est-il un groupe ?
2. L'ensemble $\{1, -1, \frac{1}{2}, 2\}$ muni de la multiplication des réels est-il un groupe ?
3. L'ensemble $\{3^n \,|\, n \in \mathbb{Z}\}$ muni de la multiplication des réels est-il un groupe ?
4. L'ensemble $\{a3^n \,|\, a = \pm 1, n \in \mathbb{Z}\}$ muni de la multiplication des réels est-il un groupe ?
5. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}^*\}$ muni de la multiplication des réels est-il un groupe ?
6. L'ensemble $\{a+b\sqrt{3} \,|\, a, b \in \mathbb{Q}^*\} \setminus \{0\}$ muni de la multiplication des réels est-il un groupe ?

à compléter

Éléments de réponse 74

1. L'ensemble $\{1, -1\}$ muni de la multiplication des réels est un groupe.
2. L'ensemble $\{1, -1, \frac{1}{2}, 2\}$ muni de la multiplication des réels n'est pas un groupe.
3. L'ensemble $\{3^n \,|\, n \in \mathbb{Z}\}$ muni de la multiplication des réels est un groupe.
4. L'ensemble $\{a3^n \,|\, a = \pm 1, n \in \mathbb{Z}\}$ muni de la multiplication des réels est un groupe.
5. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}^*\}$ muni de la multiplication des réels n'est pas un groupe.
6. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}^*\} \setminus \{0\}$ muni de la multiplication des réels est un groupe.

Exercice 75

Définissons pour (x, y) et (x', y') dans $\mathbb{R}^* \times \mathbb{R}$

$$(x, y) \star (x', y') = (xx', xy' + y).$$

1. Montrer que $(\mathbb{R}^* \times \mathbb{R}, \star)$ est un groupe.

2. Est-il abélien ?
3. Est-ce que $]0,+\infty[\times\mathbb{R},\star)$ est un sous-groupe de $(\mathrm{G},\star)$?

Éléments de réponse 75

1. Si $x\neq 0$ et $x'\neq 0$, alors $xx'\neq 0$, donc $(x,y)\star(x',y')=(xx',xy'+y)\in\mathbb{R}^*\times\mathbb{R}$. La loi $*$ est une loi interne.

   Soient x, x', x'' dans $\mathbb{R}^*$ et soient y, y', y'' dans $\mathbb{R}$. Alors d'une part

$$(x,y)\star\Big((x',y')\star(x'',y'')\Big)=(x,y)\star\Big(x'x'',x'y''+y'\Big)=\Big(xx'x'',x(x'y''+y')+y\Big)=(xx'x'',xx'y''+xy'+y)$$

   et d'autre part

$$\Big((x,y)\star(x',y')\Big)\star(x'',y'')=\Big(xx',xy'+y\Big)\star(x'',y'')=(xx'x'',xx'y''+xy'+y)$$

   Par suite la loi $\star$ est associative.

   Soit (a,b) tel que pour tout $(x,y)\in\mathrm{G}$ nous ayons

$$(a,b)\star(x,y)=(x,y)\star(a,b)=(x,y).$$

   Ces égalités équivalent à

$$(ax,ay+b)=(xa,xb+y)=(x,y)\Longleftrightarrow\left\{\begin{array}{l}ax=xa=x\\ay+b=xb+y=y\end{array}\right.\Longleftrightarrow\left\{\begin{array}{l}a=1\\b=0\end{array}\right.$$

   De plus $(1,0)$ appartient à G. Il en résulte que $(1,0)$ est l'élément neutre.

   Soit $(x,y)\in\mathrm{G}$; on cherche (x',y') tel que $(x,y)\star(x',y')=(x',y')\star(x,y)=(1,0)$. Ces égalités se réécrivent comme suit

$$\begin{array}{rcl}(xx',xy'+y)=(x'x,x'y+y')=(1,0) & \Longleftrightarrow & \left\{\begin{array}{l}xx'=x'x=1\\xy'+y=x'y+y'=0\end{array}\right.\\ & \Longleftrightarrow & \left\{\begin{array}{l}x'=\frac{1}{x}\\xy'+y=\frac{1}{x}y+y'=0\end{array}\right.\\ & \Longleftrightarrow & \left\{\begin{array}{l}x'=\frac{1}{x}\neq 0\\y'=-\frac{y}{x}\end{array}\right.\end{array}$$

   Ainsi le symétrique de (x,y) est $\left(\frac{1}{x},-\frac{y}{x}\right)$.

   Finalement $(\mathrm{G},\star)$ est un groupe.

2. Puisque d'une part $(1,2)\star(2,0)=(2,2)$ et d'autre part $(2,0)\star(1,2)=(2,4)$ ce groupe n'est pas abélien.

3. Remarquons que l'élément neutre $(1,0)$ de $(\mathrm{G},\star)$ appartient à $]0,+\infty[\times\mathbb{R}$.

   Soient (x,y) et (x',y') deux éléments de $]0,+\infty[\times\mathbb{R}$. Alors

$$(x,y)\star\left(\frac{1}{x'},-\frac{y'}{x'}\right)=\left(\frac{x}{x'},x\left(-\frac{y'}{x'}\right)+y\right)=\left(\frac{x}{x'},\frac{-xy'+x'y}{x'}\right).$$

Comme $\frac{x}{x'} > 0$, nous obtenons que $\left(\frac{x}{x'}, \frac{-xy'+x'y}{x'}\right)$ appartient à $]0, +\infty[\times\mathbb{R}$.

Il s'en suit que $(]0, +\infty[\times\mathbb{R}, \star)$ est un sous-groupe de $(\mathrm{G}, \star)$.

Exercice 76

Le but de l'exercice est d'étudier les groupes à 1, 2, 3 ou 4 éléments.

1. Écrire la table de composition d'un groupe à 1 élément.
2. Écrire la table de composition d'un groupe à 2 éléments. Vérifier qu'il est isomorphe aux groupes suivants

$$\mathbb{Z}/2\mathbb{Z}, \qquad \left(\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right\}, \times\right)$$
$$\mathcal{S}_2, \qquad \left(\left\{x \mapsto x,\, x \mapsto \frac{1}{x}\right\}, \circ\right)$$
$$\Big(\{1, -1\}, \times\Big).$$

3. Écrire la table de composition d'un groupe à 3 éléments. Vérifier qu'il est isomorphe aux groupes suivants

$$\mathbb{Z}/3\mathbb{Z}, \qquad \left(\{1, \mathrm{e}^{2\mathbf{i}\pi/3}, \mathrm{e}^{4\mathbf{i}\pi/3}\}, \times\right)$$
$$\Big(\{(1\ 2\ 3), (2\ 3\ 1), (3\ 1\ 2)\}, \circ\Big) \qquad \left(\left\{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\right\}, \times\right)$$

4. Soit $\Big(\{e, a, b, c\}, \star\Big)$ un groupe à 4 éléments, d'élément neutre e.
5. a) Montrer qu'il existe au moins un élément, autre que l'élément neutre, qui est son propre symétrique.

   Nous supposons désormais que b est son propre symétrique.

   b) Supposons que $a\star c = c\star a = e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants

$$\left(\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right\}, \times\right), \qquad \mathbb{Z}/4\mathbb{Z}$$
$$\Big(\{(1\ 2\ 3\ 4), (2\ 3\ 4\ 1), (3\ 4\ 1\ 2), (4\ 1\ 2\ 3), \}, \circ\Big), \qquad \Big(\{1, \mathbf{i}, -1, -\mathbf{i}\}, \times\Big)$$

c) Supposons que $a\star a = c\star c = e$. Remplir la table de composition du groupe. Montrer qu'il est isomorphe aux groupes suivants

$$\left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}0&-1\\-1&0\end{pmatrix}\right\},\times\right), \qquad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

$$\Big(\{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (2\ 1\ 3\ 4),\ (2\ 1\ 4\ 3),\ \},\circ\Big),, \qquad \Big(\mathcal{P}(\{x,\,y\}),\Delta\Big).$$

d) Vérifier que nous sommes toujours dans le cas de la question 4.b) ou dans le cas de la question 4.c).

6. Vérifier que tous les groupes de cet exercice sont abéliens.

Éléments de réponse 76

Exercice 77

1.a) Montrer que $\mathbb{U} := \{z \in \mathbb{C} \,|\, |z| = 1\}$ est un groupe abélien pour la multiplication de $\mathbb{C}$.

1.b) Expliciter l'élément neutre ainsi que l'inverse d'un élément quelconque de $\mathbb{U}$.

2. Considérons maintenant $p \in \mathbb{N}^*$ et $\mathbb{U}_p := \{z \in \mathbb{C} \,|\, z^p = 1\}$.

2.a) Montrer que $\mathbb{U}_p$ est un groupe abélien fini inclus dans $\mathbb{U}$.

2.b) Décrire les éléments de $\mathbb{U}_p$ sous forme exponentielle.

2.c) Représenter graphiquement $\mathbb{U}_p$ dans le plan pour $p = 2,\ 3,\ 4,\ 6$.

Éléments de réponse 77

1.a) Soient z, w dans $\mathbb{U}$. Alors $|zw| = |z|\,|w| = 1\times 1 = 1$; autrement dit, si z et w appartiennent à $\mathbb{U}$, alors zw aussi et

$$*\colon \mathbb{U}\times\mathbb{U}\to\mathbb{U}, \qquad (z,w)\mapsto z*w = zw$$

est bien une loi de composition interne.

- ◇ Cette loi est associative : soient x, y et z dans $\mathbb{U}$ alors d'une part $x*(y*z) = x*(yz) = xyz$ et $(x*y)*z = (xy)*z = (xy)z = xyz$. En particulier $(x*y)*z = x*(y*z)$.
- ◇ Cette loi possède un élément neutre que est $1 \in \mathbb{U}$. En effet, pour tout $z \in \mathbb{U}$ nous avons

$$1*z = 1\,z = z \qquad\qquad z*1 = z\,1 = z.$$

- ◇ Tout élément de $\mathbb{U}$ est inversible ; en effet si z appartient à $\mathbb{U}$, alors $\left|\frac{1}{z}\right| = \frac{|1|}{|z|} = \frac{1}{1} = 1$, *i.e.* $\frac{1}{z}$ appartient à $\mathbb{U}$.
- ◇ Cette loi est commutative. En effet soient x et y dans $\mathbb{U}$; alors d'une part $x*y = xy$ et d'autre part $y*x = yx = xy$. En particulier $x*y = y*x$.

Il en résulte que $\mathbb{U}$ est un groupe abélien pour la multiplication de $\mathbb{C}$.

1.b)

2.a) Commençons par montrer que $\mathbb{U}_p$ est un sous-groupe de $\mathbb{U}$.

- ◇ Notons que $\mathbb{U}_p \neq \emptyset$: $1 \in \mathbb{U}_p$.
- ◇ Montrons que $\mathbb{U}_p$ est stable pour $*$: soient x et y dans $\mathbb{U}_p$, alors $(xy)^p = x^p y^p = 1 \times 1 = 1$ d'où xy appartient à $\mathbb{U}_p$.
- ◇ Montrons que $\mathbb{U}_p$ est stable par inversion : soit $z \in \mathbb{U}_p$, alors $\left(\frac{1}{z}\right)^{1/p} = \frac{1}{z^p} = \frac{1}{1} = 1$ et $\frac{1}{z}$ appartient à $\mathbb{U}_p$.

Puisque $(\mathbb{U}, \cdot)$ est abélien, $(\mathbb{U}_p, \cdot)$ aussi.

L'équation $z^p = 1$ admet exactement p solutions dans $\mathbb{C}$, c'est-à-dire $|\mathbb{U}_p| = p$; en particulier $\mathbb{U}_p$ est fini.

2.b) Décrions les éléments de $\mathbb{U}_p$ sous forme exponentielle. Rappelons que $\mathbb{U}_p = \{z \in \mathbb{C} \,|\, z^p = 1\}$ autrement dit $\mathbb{U}_p$ est l'ensemble des racines pième de l'unité. Ainsi les éléments de $\mathbb{U}_p$ sont les $\exp\left(\frac{2\mathbf{i}\pi k}{p}\right)$ avec $0 \leq k \leq p-1$.

représentation graphique

2.c)

Exercice 78

1. Munissons $\mathbb{R}$ de la loi de composition interne $*$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x * y = xy + (x^2 - 1)(y^2 - 1).$$
   a) Montrer que $*$ est commutative.
   b) Montrer que $*$ n'est pas associative.
   c) Montrer que 1 est élément neutre.
2. Munissons $\mathbb{R}^{+*}$ de la loi de composition interne $*$ définie par
$$\forall\, x,\, y \in \mathbb{R}^{+*} \quad x * y = \sqrt{x^2 + y^2}.$$
   a) Montrer que $*$ est commutative.
   b) Montrer que $*$ est associative.
   c) Montrer que 0 est élément neutre.
3. Munissons $\mathbb{R}$ de la loi de composition interne $*$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x * y = \sqrt[3]{x^3 + y^3}$$
   a) Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}, *)$ vers $(\mathbb{R}, +)$.
   b) En déduire que $(\mathbb{R}, *)$ est un groupe abélien.

Éléments de réponse 78

Exercice 79

Soit $\mathrm{G} =]-1,1[$. Pour x, $y \in \mathrm{G}$, on définit $x \star y := \frac{x+y}{1+xy}$. Montrer que $(\mathrm{G}, \star)$ est un groupe abélien.

Éléments de réponse 79

◇ Commençons par montrer que $*$ est une loi de composition interne.

i) Soient x et y dans G alors $x < 1$ et $1 - y > 0$ d'où $x(1-y) < 1 \cdot (1-y)$, soit $x(1-y) < 1-y$, *i.e.* $x - xy < 1 - y$ ou encore $x + y < 1 + xy$. Comme x et y appartiennent à G nous avons $1 + xy > 0$; cette dernière inégalité combinée à $x + y < 1 + xy$ entraîne $\frac{x+y}{1+xy} < 1$.

ii) Soient x et y dans G alors d'une part $1 + x > 0$, d'autre part $1 + y > 0$. Il en résulte que $(1 + x)(1 + y) > 0$, *i.e.* $1 + x + y + xy > 0$, soit $x + y > -(1 + xy)$. Par ailleurs comme x et y appartiennent à G nous avons $1 + xy > 0$; cette dernière inégalité combinée à $x + y > -(1 + xy)$ implique $\frac{x+y}{1+xy} > -1$.

Finalement i) et ii) entraînent l'assertion suivante : si x et y appartiennent à G, alors $x * y$ appartient à G. Autrement dit $*$ est une loi de composition interne.

◇ Montrons que $*$ est associative : soient x, y et z dans G, alors d'une part

$$x * (y * z) = x * \left(\frac{y+z}{1+yz}\right) = \frac{x + \frac{y+z}{1+yz}}{1 + x - \frac{y+z}{1+yz}} = \frac{x+y+z+xyz}{1+xy+xz+yz}$$

et d'autre part

$$(x * y) * z = \left(\frac{x+y}{1+xy}\right) * z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} = \frac{x+y+z+xyz}{1+xy+xz+yz}.$$

En particulier, $x * (y * z) = (x * y) * z$ et $*$ est commutative.

◇ Montrons que $*$ possède pour élément neutre 0. Commençons par remarquer que 0 appartient à G. De plus, pour tout $x \in \mathrm{G}$, nous avons

$$x * 0 = \frac{x+0}{1+x\cdot 0} = x, \qquad 0 * x = \frac{0+x}{1+0\cdot x} = x.$$

◇ Montrons que tout élément de G est inversible : soit $x \in \mathrm{G} =]-1,1[$, alors $-x$ appartient à G et

$$x * (-x) = \frac{x + (-x)}{1 - x^2} = \frac{0}{1-x^2} = 0, \qquad (-x) * x = \frac{-x + x}{1 - x^2} = \frac{0}{1-x^2} = 0.$$

◇ Montrons que $*$ est commutative : soient x et y dans G, alors

$$x * y = \frac{x+y}{1+xy}, \qquad y * x = \frac{y+x}{1+yx} = \frac{x+y}{1+xy}$$

d'où $x * y = y * x$: $*$ est commutative.

Exercice 80

Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble de toutes ses parties. Montrer que E muni l'application « différence symétrique »

$$\Delta : \mathcal{P}(E) \times \mathcal{P}(E) \ \to \ \mathcal{P}(E), \ (A, B) \ \mapsto \ A\Delta B \ := \ (A \setminus B) \cup (B \setminus A)$$

est un groupe abélien. Expliciter l'élément neutre ainsi que l'inverse d'un élément quelconque.

Éléments de réponse 80

Exercice 81

Soit $(E_1, \star_1)$ et $(E_2, \star_2)$ deux groupes. Sur le produit cartésien $E_1 \times E_2$, on définit la loi interne $\star$ par : $(h, k) \star (h', k') = (h \star_1 h', k \star_2 k')$.
Montrer que $(E_1 \times E_2, \star)$ est un groupe et qu'il est abélien si E_1 et E_2 le sont. Généraliser au produit cartésien de $n \in \mathbb{N}^*$ groupes, $(E_1, \star_1)$, ..., $(E_n, \star_n)$.

Éléments de réponse 81

Exercice 82

1. Soit $(\mathrm{G}, \star)$ un groupe et $x \in \mathrm{G}$. Montrer que les applications de G dans G définies par $\tau_{d,x} : y \in \mathrm{G} \mapsto y \star x \in \mathrm{G}$ et $\tau_{g,x} : y \in \mathrm{G} \mapsto x \star y \in \mathrm{G}$ (respectivement appelées translations à droite et à gauche définies par x) sont des bijections.
2. Construire toutes les tables de multiplication des groupes à 2 éléments. Sont-ils abéliens ?
3. Construire toute les tables de multiplications des groupes à 3 éléments. Sont-ils abéliens ?

Éléments de réponse 82

Exercice 83

Considérons l'ensemble des matrices

$$\mathcal{H}_3(\mathbb{R}) \ := \ \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, a, \, b, \, c \in \mathbb{R} \right\}$$

muni de la loi produit des matrices ; il est appelé groupe de Heisenberg continu.

1. Montrer que $\mathcal{H}_3(\mathbb{R})$ est un groupe non-abélien.
2. Décrire l'élément neutre de $\mathcal{H}_3(\mathbb{R})$.
3. Décrire l'inverse d'un élément quelconque de $\mathcal{H}_3(\mathbb{R})$.

Éléments de réponse 83

1. Montrons que $\mathcal{H}_3(\mathbb{R})$ est un groupe.

◇ La loi produit des matrices est une loi de composition interne : soient $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & u & v \\ 0 & 1 & w \\ 0 & 0 & 1 \end{pmatrix}$ dans $\mathcal{H}_3(\mathbb{R})$; alors

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & u & v \\ 0 & 1 & w \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u+a & v+aw+c \\ 0 & 1 & w+b \\ 0 & 0 & 1 \end{pmatrix}$$

est de la forme $\begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}$ avec α, β et γ dans $\mathbb{R}$ donc appartient à $\mathcal{H}_3(\mathbb{R})$.

◇ La loi produit des matrices est associative.

◇ La matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est l'élément neutre pour la loi produit des matrices ; en effet soit $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ dans $\mathcal{H}_3(\mathbb{R})$, alors

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

◇ Tout élément $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{H}_3(\mathbb{R})$ admet pour inverse l'élément de $\mathcal{H}_3(\mathbb{R})$ donné par $\begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$. En effet

$$\begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Le groupe $\mathcal{H}_3(\mathbb{R})$ n'est pas abélien : les matrices $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ appartiennent à $\mathcal{H}_3(\mathbb{R})$ et

$$\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}} \neq \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}$$

2.

3.

Exercice 84

Montrer que $\mathbb{R}$ muni de la loi

$$\star\colon \mathbb{R}\times\mathbb{R}\to\mathbb{R}, \qquad (x,y)\mapsto x\star y=(x^3+y^3)^{1/3}$$

est un groupe abélien.

Éléments de réponse 84

Exercice 85

Soit $f_{a,b}\colon \mathbb{R}\mapsto\mathbb{R}$ la fonction définie par $f_{a,b}(x)=ax+b$. Montrer que l'ensemble

$$\mathcal{A} \;:=\; \{f_{a,b}\ ;\ a\in\mathbb{R}^*, b\in\mathbb{R}\}$$

muni de la composition des fonctions « $\circ$ » est un groupe non-abélien. On décrira l'élément neutre et l'inverse de chaque élément de $\mathcal{A}$ ($\mathcal{A}$ est appelé le groupe affine de la droite réelle $\mathbb{R}$).

Éléments de réponse 85

Exercice 86 Groupe d'exposant 2.

On dit qu'un groupe $(\mathbb{R},\star)$ est d'exposant 2 si $\mathrm{G}\neq\{e\}$ (i.e. G est "non trivial") et si, pour tout $x\in\mathrm{G}$, $x\star x=e$.

1. Donner un exemple de groupe d'exposant 2 de cardinal 2. Montrer que les groupes de cardinal 3 ne sont pas d'exposant 2. Donner un exemple de groupe d'exposant 2 de cardinal 4.
2. Montrer que tout groupe d'exposant 2 est abélien.

Éléments de réponse 86

Exercice 87

Soient z_1, $z_2 \in \mathbb{C}^*$. On pose $z_1 \sim z_2$ s'il existe $\lambda > 0$ tel que $z_1 = \lambda z_2$.

1. Montrer que $\sim$ est une relation d'équivalence sur $\mathbb{C}^*$.
2. Soit $z \in \mathbb{C}^*$ fixé. Décrire géométriquement dans la classe $\overline{z} = \{\gamma \in \mathbb{C}^* \,|\, \gamma \sim z\}$ pour la relation d'équivalence $\sim$. (On rappelle qu'une classe $\overline{z}$ est en particulier un sous-ensemble de $\mathbb{C}^*$.)

3. Montrer que la relation d'équivalence $\sim$ est compatible avec la loi du groupe $(\mathbb{C}^*, \times)$ au sens suivant : si $z_1 \sim z_2$ et $z_3 \sim z_4$ alors $z_1 z_3 \sim z_2 z_4$.

   On note $Y = (\mathrm{G}/\sim) = \{\overline{z}, z \in \mathbb{C}^*\}$ *l'ensemble dont les éléments sont les classes d'équivalences* $\overline{z}$ *pour* z *parcourant* $\mathbb{C}^*$. (Y *est appelé espace quotient de* G *par* $\sim$.)

4. Montrer que pour $0 \leq \theta_1 < \theta_2 < 2\pi$, les classes $\overline{(e^{i\theta_1})}$ et $\overline{(e^{i\theta_2})}$ sont deux à deux disjointes. De plus, montrer que l'on a
$$Y = (\mathrm{G}/\sim) = \{\overline{(e^{\mathbf{i}\theta})}, \theta \in [0, 2\pi[\} \quad \text{et} \quad \mathrm{G} = \bigcup_{\theta \in [0,2\pi[} \overline{(e^{\mathbf{i}\theta})}.$$
5. On pose $\psi \colon (\mathrm{G}/\sim) \to \mathbb{T} = \{z \in \mathbb{C} \,|\, |z| = 1\}$ l'application définie par $\psi(\overline{z}) = \frac{z}{|z|}$. Montrer que l'on peut *identifier* $(\mathrm{G}/\sim)$ et $\mathbb{T}$, i.e. ψ est une application bijective.

6. Soient z_1, $z_2 \in \mathbb{C}^*$. On pose $\overline{z_1} \star \overline{z_2} = \overbrace{\overline{(z_1 z_2)}}$. Montrer que $(X, \star)$ est un groupe.

7. Montrer que l'application $\varphi \colon (X, \star) \to (]0, +\infty[, \times)$ est un isomorphisme de groupes. (Ici $(]0, +\infty[, \times)$ est le groupe multiplicatif sur $]0, +\infty[$.)

8. Quel est le lien entre la classe d'équivalence $\overline{z}$ de $z \in \mathbb{C}^*$ et la décomposition polaire de z ?

Éléments de réponse 87

Exercice 88

Soit $f_{a,b} \colon \mathbb{R} \mapsto \mathbb{R}$ la fonction définie par $f_{a,b}(x) = ax + b$.

1. Montrer que l'ensemble
$$\mathcal{A} \;:=\; \{f_{a,b} \;;\; a \in \mathbb{R}^*, b \in \mathbb{R}\}$$
muni de la composition des fonctions "$\circ$" est un groupe non-abélien ; $\mathcal{A}$ est appelé le groupe affine de la droite réelle $\mathbb{R}$.

2. Décrire l'élément neutre de $\mathcal{A}$.
3. Décrire l'inverse de chaque élément de $\mathcal{A}$.

Éléments de réponse 88

Exercice 89

Soit $\mathrm{GL}(n,\mathbb{R})$ l'ensemble des matrices carrées inversibles de taille n à coefficients réels.

1. Vérifier que $\mathrm{GL}(n,\mathbb{R})$ muni de la multiplication matricielle est un groupe.
2. L'ensemble des matrices diagonales à coefficients diagonaux tous non nuls est-il un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$?
3. On suppose maintenant que $n = 2$. Les ensembles suivants sont-ils des sous-groupes de $\mathrm{GL}(2,\mathbb{R})$:

a) $\mathrm{H}_1 := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a > 0,\ b \in \mathbb{R} \right\}$? b) $\mathrm{H}_2 := \left\{ \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \mid a > 0,\ b \in \mathbb{R} \right\}$?

Éléments de réponse 89

Exercice 90 Sous-groupes usuels

Soit $(\mathrm{G},\cdot)$ un groupe noté multiplicativement. Montrer que les parties suivantes de G sont des sous-groupes de G :

a) Le centre $Z(\mathrm{G})$ de G défini par
$$Z(\mathrm{G}) = \{a \in \mathrm{G} \mid \forall\, x \in \mathrm{G}\ xa = ax\}.$$
b) $x\mathrm{H}x^{-1} = \{xax^{-1} \mid a \in \mathrm{H}\}$, où $x \in \mathrm{G}$ et H est un sous-groupe de G.
c) Rappelons qu'un élément $x \in \mathrm{G}$ est dit de *torsion* s'il existe $n \in \mathbb{N}$ tel que $x^n = 1_{\mathrm{G}}$. Montrer que si G est abélien, l'ensemble des éléments de torsion est un sous-groupe de G.

Éléments de réponse 90

Exercice 91

Soient $A = (x_1, y_1)$ et $B = (x_2, y_2)$ deux points dans $E = \mathbb{R}^2$. On écrit $A \sim B$ si $y_1 = y_2$.

1. Montrer que $\sim$ est une relation d'équivalence.
2. Décrire la classe d'équivalence de $A = (1, 2)$ que l'on notera $\overline{A}$ par :
   1) la description $\overline{A} = \{\ldots\}$,
   2) puis l'objet géométrique qu'il représente.
   (On rappelle qu'une classe d'équivalence est un sous-ensemble de E).
3. Plus généralement, décrire la classe d'équivalence de $A = (a, b) \in \mathbb{R}^2$ pour $(a, b) \in \mathbb{R}^2$ fixé (*i.e.* décrire $\overline{A} = \{\ldots\}$.)

4. Pour cet exemple particulier $(E, \sim)$, montrer que pour toute classe d'équivalence $\overline{A} = \overline{(a,b)}$, on peut choisir un représentant spécifique de la forme $(0, y)$ (on précisera la valeur de y). On appellera cet élément *représentant canonique* (Ce n'est pas toujours possible en général).
5. Montrer que $\{\overline{(0,y)}, y \in \mathbb{R}\}$ forme une partition de E correspondant aux classes d'équivalences de $\sim$.
6. Interpréter géométriquement l'espace quotient $E/\sim$.
7. Même exercice avec la définition suivante : on écrit $A \sim B$ si $x_1 = x_2$.
8. Même exercice avec la définition suivante : on écrit $A \sim B$ si $\overrightarrow{AB} \in \mathcal{D}$, où $\mathcal{D}$ est une droite affine de $E = \mathbb{R}^2$..

Éléments de réponse 91

Exercice 92

Soient $\overrightarrow{u} = (x_1, y_1)$ et $\overrightarrow{v} = (x_2, y_2)$ deux vecteurs dans $E = \mathbb{R}^2$.
Nous écrivons écrit $\overrightarrow{u} \sim \overrightarrow{v}$ si $||\overrightarrow{u}|| = ||\overrightarrow{v}||$, ($\overrightarrow{u}$ et $\overrightarrow{v}$ ont la même longueur).

1. Montrer que $\sim$ est une relation d'équivalence.
2. Décrire la classe d'équivalence de $A = (3, 4)$ que l'on notera $\overline{A}$ par :
   1) la description $\overline{A} = \{\ldots\}$,
   2) puis l'objet géométrique qu'il représente.
3. Décrire la classe d'équivalence de $0 = (0, 0)$.
4. Montrer que toute classe d'équivalence est de la forme $\overline{(0,R)}$ pour un $R \geq 0$ que l'on appellera *représentant canonique* de la classe considérée.
5. Quel est le *représentant canonique* de la classe de $A = (3, 4)$?
6. Montrer que $\{\overline{(0,R)} \,|\, R \geq 0\}$ forme une partition de E correspondant aux classes d'équivalences de $\sim$.
7. Interpréter géométriquement l'espace quotient $E/\sim$.

Éléments de réponse 92

Exercice 93

Soient E et F deux ensembles et une application $f : E \to F$. Montrer que la relation binaire $\mathcal{R}$ définie sur E par

$$x \mathcal{R} y \iff f(x) = f(y)$$

est une relation d'équivalence sur E. Décrire la classe d'un élément $x \in E$.

Éléments de réponse 93

Exercice 94

Démontrer que la relation binaire $\mathcal{R}$ définie sur $\mathbb{R}^+$ par

$$x\mathcal{R}y \iff \exists\, k, \ell \in \mathbb{N}^* \text{ tel que } kx = \ell y$$

est une relation d'équivalence sur $\mathbb{R}^+$. Décrire les classes d'équivalence $\overline{0}$ et $\overline{1}$.

Éléments de réponse 94

Exercice 95

Soit $(\mathrm{G}, \star)$ un groupe fini de cardinal pair.

1. Démontrer que la relation binaire $\mathcal{R}$ définie sur G par
$$x\mathcal{R}y \iff y \in \{x, x^{-1}\}$$
est une relation d'équivalence sur G.
2. Discuter, pour $x \in \mathrm{G}$, la valeur du cardinal de $\overline{x}$.
3. En déduire l'existence d'un élément $x \in \mathrm{G} \setminus \{e\}$ tel que $x \star x = e$.
4. Réciproquement, montrer que tout groupe fini $(\mathrm{G}, \star)$ admettant un élément $x \neq e$ vérifiant $x \star x = e$ est d'ordre pair.

Éléments de réponse 95

Exercice 96

1. Munissons $\mathbb{R}$ de la loi de composition interne $\star$ définie par
$$\forall\, x,\, y \in \mathbb{R} \quad x \star y = xy + (x^2 - 1)(y^2 - 1).$$
   a) Montrer que $\star$ est commutative.
   b) Montrer que $\star$ n'est pas associative.
   c) Montrer que 1 est élément neutre.
2. Munissons $\mathbb{R}^{+*}$ de la loi de composition interne $\star$ définie par
$$\forall\, x,\, y \in \mathbb{R}^{+*} \quad x \star y = \sqrt{x^2 + y^2}.$$
   a) Montrer que $\star$ est commutative.
   b) Montrer que $\star$ est associative.
   c) Montrer que 0 est élément neutre.
   d) Montrer qu'aucun élément de $\mathbb{R}^{+*}$ n'a de symétrique pour $\star$.
3. Munissons $\mathbb{R}$ de la loi de composition interne $\star$ définie par :
$$\forall\, x,\, y \in \mathbb{R} \quad x \star y = \sqrt[3]{x^3 + y^3}.$$
   a) Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}, \star)$ vers $(\mathbb{R}, +)$.

b) En déduire que $(\mathbb{R}, \star)$ est un groupe abélien.

Éléments de réponse 96

Exercice 97

Soit E l'ensemble des parties d'un ensemble à deux éléments, par exemple $E = \mathcal{P}(\{0, 1\})$ donc

$$E = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Considérons les lois de composition $\star$ suivantes sur l'ensemble E :

- ◇ réunion : $A \star B = A \cup B$;
- ◇ intersection : $A \star B = A \cap B$;
- ◇ différence symétrique : $A \star B = A \Delta B = (A \setminus B) \cup (B \setminus A)$;
- ◇ réunion des complémentaires : $A \star B = \complement A \cup \complement B$;
- ◇ intersection des complémentaires : $A \star B = \complement A \cap \complement B$.

Pour chacune d'entre elles :

1. Écrire la table de composition de la loi $\star$.
2. L'ensemble E possède-t-il un élément neutre pour la loi $\star$?
3. La loi $\star$ est-elle associative ?
4. La loi $\star$ est-elle commutative ?
5. L'ensemble E muni de la loi $\star$ est-il un groupe ?
6. Répondre aux questions 2 à 5 en remplaçant E par l'ensemble des parties d'un ensemble quelconques.

Éléments de réponse 97

Exercice 98

Soient $(G, \star)$ un groupe et H, K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.

Éléments de réponse 98

Exercice 99

1. Soient n, $m \in \mathbb{N}^*$. Déterminer $n\mathbb{Z} \cap m\mathbb{Z}$.
2. Dans $(\mathbb{Z}, +)$, quel est le sous-groupe engendré par :

   a) $E_1 = \{3\}$? b) $E_2 = \{8, 12\}$? c) $E_3 = \{n, m\}$ pour $n, m \in \mathbb{N}^*$?

Éléments de réponse 99

Exercice 100

Soient G un groupe noté multiplicativement et H un sous-ensemble fini non vide de G stable pour la loi de G.

1. Soit $x \in \mathrm{H}$. Montrer que l'application $\varphi : \mathbb{N} \to \mathrm{G},\ n \mapsto x^n$ n'est pas injective.
2. En déduire que $e \in \mathrm{H}$ et que si $x \in \mathrm{H}$, alors $x^{-1} \in \mathrm{H}$.
3. Montrer que H est un sous-groupe de G.
4. Est-ce encore vrai si H est infini ?

Éléments de réponse 100

Exercice 101

Soient G un groupe d'élément neutre e et H, K deux sous-groupes de G d'ordres des entiers premiers. Montrer que $\mathrm{H} = \mathrm{K}$ ou que $\mathrm{H} \cap \mathrm{K} = \{e\}$.
Indication : Quels sont les générateurs d'un groupe fini d'ordre premier ?

Éléments de réponse 101

Exercice 102

Soient $(\mathrm{G}, \cdot)$ un groupe noté multiplicativement et H un sous-groupe de G. On dit que H est distingué dans G si, pour tout $a \in \mathrm{G}$:

$$a\mathrm{H}a^{-1} = \left\{aha^{-1} \,|\, h \in \mathrm{H}\right\} \subset \mathrm{H}\,.$$

1. Montrer que $\{e_\mathrm{G}\}$ et G sont distingués dans G.
2. Quels sont les sous-groupes distingués de G lorsque G est abélien ?
3. Montrer que H est distingué ssi pour tout $a \in \mathrm{G}$, $a\mathrm{H} = \mathrm{H}a$ (où $a\mathrm{H} = \left\{ah \,|\, h \in \mathrm{H}\right\}$ et $\mathrm{H}a = \left\{ha \,|\, h \in \mathrm{H}\right\}$).
4. On suppose que H est distingué dans G. Soit K un sous-groupe de G. Montrer que $\mathrm{KH} = \left\{kh \,|\, (k,h) \in \mathrm{K} \times \mathrm{H}\right\}$ est un sous-groupe de G. En déduire le groupe engendré par $\mathrm{K} \cup \mathrm{H}$.
5. Montrer que le centre $Z(\mathrm{G})$ de G est distingué dans G.

Éléments de réponse 102

Exercice 103

Considérons l'application f de $(\mathbb{C}^*, \cdot)$ dans $(\mathbb{U}, \cdot)$ définie par $f(z) = \frac{z}{|z|}$. L'ensemble $\mathbb{U}$ désigne ici l'ensemble des nombres complexes de module 1.

1. Montrer que f est un morphisme de groupes.

2. Décrire le noyau $\ker f$ de f.
3. Décrire l'image $\operatorname{im} f$ de f.

Éléments de réponse 103

Exercice 104

Considérons l'application exp de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \cdot)$.

1. Montrer que f est un morphisme de groupes.
2. Décrire le noyau $\ker f$ de f.
3. Décrire l'image $\operatorname{im} f$ de f.

Éléments de réponse 104

Exercice 105

Considérons l'application f de $(\mathbb{U}, \cdot)$ dans $(\mathbb{U}, \cdot)$ définie par $f(z) = z^2$. L'ensemble $\mathbb{U}$ désigne ici l'ensemble des nombres complexes de module 1.

1. Montrer que f est un morphisme de groupes.
2. Décrire le noyau $\ker f$ de f.
3. Décrire l'image $\operatorname{im} f$ de f.

Éléments de réponse 105

Exercice 106

Soit $(\mathrm{G}, \cdot)$ un groupe (noté multiplicativement). Pour $a \in \mathrm{G}$, on définit l'application $\tau_a \colon \mathrm{G} \to \mathrm{G}$ par $\tau_a(x) = axa^{-1}$ pour tout $x \in \mathrm{G}$.

1. Montrer que, pour tout $a \in \mathrm{G}$, τ_a est un automorphisme de G. Quelle est la bijection réciproque de τ_a ?
2. Montrer que $\mathcal{T} = \{\tau_a \mid a \in \mathrm{G}\}$ muni du produit de composition est un groupe.

Éléments de réponse 106

Exercice 107

1. Soient deux groupes G, G′ notés multiplicativement et $f \colon \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Montrer que le sous-groupe $\ker f$ de G est distingué dans G, *i.e.* que, pour tout $a \in \mathrm{G}$: $a \ker f \, a^{-1} \subset \ker f$.
2. Soit $\mathrm{GL}(n, \mathbb{R})$ le groupe des matrices carrées réelles inversibles de taille $n \in \mathbb{N}^*$. Déduire de ce qui précède que le sous-ensemble $\mathrm{SL}(n, \mathbb{R})$ des matrices de déterminant 1 est un sous-groupe distingué de $\mathrm{GL}(n, \mathbb{R})$.

Éléments de réponse 107

Exercice 108

Soient G et G′ deux groupes d'ordre $p \in \mathbb{N}^*$ premier. Montrer que G et G′ sont isomorphes.

Éléments de réponse 108

Exercice 109

1. Montrer que
$$\mathrm{G} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\}$$
est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.
2. On pose
$$\mathrm{H} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}.$$
Montrer que H est un sous-groupe de G. Quelle est l'interprétation graphique de H ?
3. On définit $f \colon \mathbb{R}_+^* \times \mathrm{H} \to \mathrm{G}$ par $f(r, A) = rA$. Montrer que f est un isomorphisme du groupe produit $\mathbb{R}_+^* \times \mathrm{H}$ vers le groupe G.
Rappel : $\mathbb{R}_+^* = \{x \in \mathbb{R} \,|\, x > 0\}$ *est un sous-groupe de* $(\mathbb{R}^*, \cdot)$.

Éléments de réponse 109

On dit que G est le groupe des matrices de rotation.

Exercice 110

Soit $(\mathrm{G}, \cdot)$ un groupe admettant deux sous-groupes H et K tels que :

1. $\mathrm{G} = \mathrm{HK} = \{hk \,|\, h \in \mathrm{H},\, k \in \mathrm{K}\}$,
2. $\mathrm{H} \cap \mathrm{K} = \{e\}$,
3. les éléments de H et de K commutent : pour tout $(h, k) \in \mathrm{H} \times \mathrm{K}$, on a $hk = kh$.

Montrer que G est isomorphe au groupe produit $\mathrm{H} \times \mathrm{K}$ (muni de la loi produit).
Rappel : cette loi est définie par $(h, k).(h', k') = (hh', kk')$ *pour tous* h, $h' \in \mathrm{H}$ *et* k, $k' \in \mathrm{K}$.

Éléments de réponse 110

Exercice 111

Soient F un ensemble, $(\mathrm{G}, \cdot)$ un groupe, et φ une application bijective de F sur G. Pour x, $y \in \mathrm{F}$, on définit la loi de composition interne $\star$ par :
$$x \star y := \varphi^{-1}(\varphi(x).\varphi(y)).$$

1. Montrer que $(\mathrm{F}, \star)$ est un groupe isomorphe à $(\mathrm{G}, \cdot)$.

2. Considérons le groupe

$$\mathrm{G} \;:=\; \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a,\, b \in \mathbb{R}, a^2+b^2 \neq 0 \right\}$$

Définissons φ par :

$$\forall\, (a,b) \in \mathbb{R}^2 \smallsetminus \{(0,0)\}\,, \quad \varphi(a,b) \;:=\; \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Montrer que φ réalise une bijection de $\mathbb{R}^2 \smallsetminus \{(0,0)\}$ sur G et expliciter la loi de composition interne $\star$ obtenue sur $\mathbb{R}^2 \smallsetminus \{(0,0)\}$. En identifiant l'élément $(a,b) \in \mathbb{R}^2 \smallsetminus \{(0,0)\}$ avec $a + \mathbf{i}b \in \mathbb{C}^*$, quelle loi de composition interne retrouve-t-on sur $\mathbb{C}^*$?

Éléments de réponse 111

Exercice 112

Dans $(\mathbb{C}^*, \cdot)$, quel est l'ordre de -1 ? De $\mathbf{i}$? De 2 ? De $\frac{1}{2} + \frac{\sqrt{3}}{2}\mathbf{i}$?
Plus généralement, quels sont les éléments d'ordre fini ?

Éléments de réponse 112

Exercice 113

Soit $(\mathrm{G}, \cdot)$ un groupe fini d'ordre $n \in \mathbb{N}^*$. Soit x un élément de G. Que vaut x^n ?

Éléments de réponse 113

Exercice 114

Déterminer tous les sous-groupes finis de $(\mathbb{R}^*, \cdot)$ et de $(\mathbb{C}^*, \cdot)$.

Éléments de réponse 114

Exercice 115

Soit $p \in \mathbb{N}^*$ et $\mathbb{U}_p = \{z \in \mathbb{C} \,|\, z^p = 1\}$ le groupe des racines p-ièmes de l'unité.

1. Montrer que
$$\mathbb{U}_p \;:=\; \{z_{p,k} = e^{\frac{2k\pi\mathbf{i}}{p}} = z_{1,p}^k \,|\, k = 0,\, \ldots,\, p-1\}.$$
2. Déterminer tous les sous-groupes de $\mathbb{U}_p$ pour $p = 3,\, 4,\, 6$.
3. Décrire les générateurs de $\mathbb{U}_p$ pour $p = 3,\, 4,\, 6$.
4. Décrire les générateurs de $\mathbb{U}_p$ pour $p \in \mathbb{N}^*$ quelconque.

Éléments de réponse 115

Exercice 116

Soient a et b deux éléments d'un groupe $(\mathrm{G}, \cdot)$.

1. Montrer que si a et b sont conjugués, i.e. s'il existe $g \in \mathrm{G}$ tel que $b = gag^{-1}$, alors ils ont le même ordre (éventuellement infini).
2. La réciproque est-elle vraie ?
3. Montrer que ab et ba ont le même ordre (éventuellement infini).
4. Supposons a d'ordre $n \in \mathbb{N}^*$. Quel est l'ordre de a^2 ? Et celui de a^k, où $k \in \mathbb{Z}$?

Éléments de réponse 116

Exercice 117

Soient G et H deux groupes. Soit $\mathrm{G} \times \mathrm{H}$ le groupe produit.

1. Montrer que si $g \in \mathrm{G}$ est d'ordre p et $h \in \mathrm{H}$ est d'ordre q, alors $(g, h) \in \mathrm{G} \times \mathrm{H}$ est d'ordre $\mathrm{ppcm}(p, q)$.
2. On suppose que G et H sont cycliques. Montrer que $\mathrm{G} \times \mathrm{H}$ l'est aussi si et seulement si les ordres de G et de H sont premiers entre eux.

Éléments de réponse 117

Exercice 118

On considère $\mathfrak{S}_3$ le groupe des permutations de $\{1, 2, 3\}$.

1. Rappeler le nombre d'éléments de $\mathfrak{S}_3$.
2. Quels sont les éléments de $\mathfrak{S}_3$?
3. Dresser la table de la loi de $\mathfrak{S}_3$.

Éléments de réponse 118

Exercice 119

Soient p cycles $\sigma_1, \ldots, \sigma_p$ deux à deux disjoints de longueurs respectives $n_1, \ldots, n_p$. Que vaut l'ordre de $\sigma_1 \circ \cdots \circ \sigma_p$ en fonction de $n_1, \ldots, n_p$?

Éléments de réponse 119

Exercice 120

Pour les permutations σ_ℓ suivantes : décomposer σ_ℓ en produit de cycles disjoints, en produit de transpositions, calculer σ_ℓ^{100} et σ_ℓ^{2020}, ainsi que l'ordre de σ_ℓ :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{pmatrix}$$

$$\text{et} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}.$$

Éléments de réponse 120

Exercice 121

Soient $p \in \mathbb{N}^*$, $n \in \{1, \ldots, p\}$ et n éléments a_1, …, a_n de $\{1, \ldots, p\}$ distincts deux à deux.

1. Montrer que $(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_2) \circ \cdots \circ (a_{n-1}\ a_n)$.
2. Soit $\sigma \in \mathfrak{S}_p$. Montrer que : $\sigma \circ (a_1\ a_2\ \cdots\ a_n) \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_n))$.
3. Simplifier le produit de 3-cycles $(1\ 2\ 3) \circ (2\ 3\ 4) \circ (1\ 3\ 2)$.

Éléments de réponse 121

Exercice 122

Pour $n \in \mathbb{N}^*$, montrer que les ensembles suivants engendrent $\mathfrak{S}_n$:

$$S_1 := \{(1\,2),\ (2\,3), \ldots, (n-1\,n)\}, \quad S_2 := \{(1\,2),\ (1\,3), \ldots, (1\,n)\}, \quad S_3 := \{(1\,2),\ (1\,2\,\ldots\,n)\}.$$

Éléments de réponse 122

Exercice 123 Signature d'une permutation.

Soit $n \in \mathbb{N}^*$. Dans la suite, on admettra le résultat suivant : si s_1, …, s_p sont $p \geq 0$ transpositions dans $\mathfrak{S}_n$ telles que $s_1 \circ \ldots \circ s_p = \mathrm{Id}$, alors p est pair. On rappelle par ailleurs que tout $\sigma \in \mathfrak{S}_n$ s'écrit comme un produit de transpositions (d'après le cours, ou d'après l'exercice précédent).

1. On définit l'application signature $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ de la façon suivante : pour tout $\sigma \in \mathfrak{S}_n$ de la forme $\sigma = s_1 \circ \ldots \circ s_p$, où s_1, …, s_p sont $p \geq 0$ transpositions, $\varepsilon(\sigma) := (-1)^p$. Montrer que cela définit bien une application de $\mathfrak{S}_n$ dans $\{-1, 1\}$.
2. Que vaut la signature d'une transposition ?
3. Soit σ un p-cycle. Montrer que $\varepsilon(\sigma) = (-1)^{p-1}$.
4. Calculer la signature des permutations suivantes

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{bmatrix}, \qquad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{bmatrix}$$

$$\text{et} \quad \sigma_3 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{bmatrix}.$$

5. On dit qu'une permutation $\sigma \in \mathfrak{S}_n$ est paire si $\varepsilon(\sigma) = 1$. Montrer que l'ensemble des permutations paires est un sous-groupe de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$.
6. Soit $A = (a_{ij})_{1 \leq i,j \leq n} \in M(n, \mathbb{C})$ une matrice carrée de taille n. Montrer que :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, a_{\sigma(1)\,1} \cdots a_{\sigma(n)\,n}\,.$$

Éléments de réponse 123

Exercice 124 Preuve par 9.

1. Soit $x \in \mathbb{N}$; soit $s(x) \in \mathbb{N}$ la somme des chiffres apparaissant dans l'écriture décimale de x. Montrer que $\overline{x} = \overline{s(x)}$ dans $\mathbb{Z}/9\mathbb{Z}$.
2. En déduire que l'égalité $1263 \times 551 = 696\,913$ est fausse.

Éléments de réponse 124

Exercice 125

On veut démontrer que le nombre (de Fermat) $F_5 := 2^{2^5} + 1$ n'est pas premier.

1. Écrire la division euclidienne de 641 par 5.
2. Écrire la division euclidienne de 641 par 5^4.
3. En déduire que $\overline{5}.\overline{2^7} = \overline{-1}$ et que $\overline{5^4} = \overline{-2^4}$ dans $\mathbb{Z}/641\mathbb{Z}$.
4. En exprimant $\overline{5^4}$ de deux façons différentes, en déduire que 641 divise F_5.

Éléments de réponse 125

Exercice 126

Soit $(A, +, \cdot)$ un anneau. Montrer que, pour tous x, $y \in A$ et $n \in \mathbb{Z}$:

1. $0_A \cdot x \;=\; x \cdot 0_A \;=\; 0_A$,
2. $(-x) \cdot y \;=\; -(x \cdot y) \;=\; x \cdot (-y)$ et $(nx) \cdot y \;=\; n(x \cdot y) \;=\; x \cdot (ny)$,
3. $(n1_A) \cdot x \;=\; nx \;=\; x \cdot (n1_A)$, et en déduire que $0_A = 1_A$ si et seulement si $A = \{0_A\}$.

Éléments de réponse 126

Exercice 127

Soit $p \geq 2$ un entier.

1. Montrer que l'anneau $\left(\mathbb{Z}/p\mathbb{Z}, +, \cdot\right)$ est intègre si, et seulement si, p est premier.
2. **Corps.** On dit qu'un anneau (unitaire) $(A, +, \cdot)$ est un corps lorsque $0_A \neq 1_A$ (ce qui équivaut à $A \neq \{0_A\}$) et tout $x \in A^* := A \setminus \{0_A\}$ est inversible (pour la multiplication).
   (a) Montrer qu'un corps est un anneau intègre.
   (b) Montrer que l'anneau $\left(\mathbb{Z}/p\mathbb{Z}, +, \cdot\right)$ est un corps si, et seulement si, p est premier.

Éléments de réponse 127

Exercice 128

1. Soit $(A, +, \times)$ un anneau (unitaire). Montrer que l'ensemble
$$A^\times := \{a \in A \,|\, , a \text{ est inversible pour la multiplication } \times\}$$
muni de la multiplication est un groupe. Qu'en déduit-on lorsque A est un corps ?
2. Soit $n \in \mathbb{N}^*$ un entier. Montrer que pour tout $k \in \mathbb{Z}$, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.
3. **Fonction indicatrice d'Euler**. On définit la fonction indicatrice d'Euler φ par :
$$\forall n \in \mathbb{N}^*, \quad \varphi(n) := \text{Card}(\{k \in \{1, \dots, n\} \ ; \ k \text{ est premier avec } n\}) \in \mathbb{N}.$$
   (a) Que vaut $\varphi(i)$ pour $i \in \{1, \dots, 6\}$? Que vaut $\varphi(n)$ lorsque n est premier ?
   (b) Démontrer le théorème d'Euler et le petit théorème de Fermat :
$$\forall n \in \mathbb{N}^*, \ \forall a \in \mathbb{Z}, \quad \text{pgcd}(a, n) = 1 \Longrightarrow a^{\varphi(n)} = 1 \ [n]$$
   et
$$\forall n \in \mathbb{N}^* \text{ premier}, \ \forall a \in \mathbb{Z} \quad a^n = a \ [n].$$

Éléments de réponse 128

Exercice 129

(*On rappelle en particulier que* $+$ *et* $\times$ *sont des lois internes associatives et commutatives dans* $\mathbb{Q}$.)

On note $E = \mathbb{Q} \setminus \{-1\} = \{a \in \mathbb{Q} \,|\, a \neq -1\}$. Pour tous $a, b \in E$, on pose
$$a \star b = a + b + ab.$$

1. Vérifier que $\star$ est une loi de composition interne dans E. (On pourra commencer par déterminer une factorisation en produit de deux éléments de $\mathbb{Q}$ de l'expression : $1 + a + b + ab$).
2. Montrer que $(E, \star)$ est un groupe abélien. On précisera la valeur de l'élément neutre e, ainsi que l'expression de l'inverse a^{-1} pour tout $a \in E$.
3. Soient a, $b \in E$ fixés. Résoudre l'équation $a \star x = b$ dans E. (On donnera la formule explicite de x en fonction de a, b.)
4. Donner la valeur explicite de $x \in E$ vérifiant $2 \star x = 3$.

Éléments de réponse 129

1. Soient $a \in E$ alors a, $b \in \mathbb{Q}$ et donc $a + b + ab$ car $\mathbb{Q}$ est stable par la loi somme et la loi produit. Montrons que si $a \neq -1$ et $b \neq -1$ alors $a + b + ab \neq -1$. On fait une démonstration par l'absurde. Supposons qu'il existe a, $b \in \mathbb{Q}$ tels que : $a \neq -1$ et $b \neq -1$ ainsi que $a + b + ab = -1$, i.e $1 + a + b + ab = 0$. On a la factorisation : $(1 + a)(1 + b) = 1 + a + b + ab$, terme qui est donc nul. Or le produit de deux nombres vaut 0 si et seulement si l'un des deux est nul. Donc, soit $a + 1 = 0$ et il s'ensuit $a = -1$

(Contradiction), soit $b+1=0$ et il s'ensuit $b=-1$ (Contradiction). Ainsi $a+b+ab=-1$ n'est pas possible si $a\neq -1$ et $b\neq -1$ donc $a+b+ab\neq -1$ comme affirmé. Ainsi pour tous $a,b\in\mathbb{Q}\setminus\{-1\}$, $a\star b\in\mathbb{Q}\setminus\{-1\}$: la loi $\star$ est une loi de composition interne.

2. Montrons que $(E,\star)$ est un groupe abélien.

(1) La commutativité est évidente puisque la somme et le produit commutent dans $\mathbb{Q}$.

(2) L'associativité : soient a, b, $c\in E$, calculons les deux termes $(a\star b)\star c$ et $a\star(b\star c)$ séparément en utilisant le fait que $+$ et $\times$ sont des lois internes associatives et commutatives dans $\mathbb{Q}$. On doit montrer que ces quantités sont égales. On a

$$\begin{aligned}(a\star b)\star c &= (a\star b)+c+(a\star b).c\\ &= (a+b+ab)+c+(a+b+ab)c\\ &= a+b+c+ab+ac+bc+abc.\end{aligned}$$

Par ailleurs, on a

$$\begin{aligned}a\star(b\star c) &= a+(b\star c)+a.(b\star c)\\ &= a+(b+c+bc)+a(b+c+bc)\\ &= a+b+c+ab+ac+bc+abc.\end{aligned}$$

D'où l'on déduit l'égalité $(a\star b)\star c=a\star(b\star c)$ cherchée.

Élément neutre : On cherche $e\in\mathbb{Q}\setminus\{-1\}$ tel que, pour tout $a\in\mathbb{Q}\setminus\{-1\}$, $a\star e=e\star a=a$ (Si e existe alors il est unique).

Méthode 1 : On propose une valeur pour e puis on vérifie $a\star e=e\star a=a$ pour tout $a\in E$. On voit que $e=0$ convient. Mais il faut aussi vérifier que $e\in\mathbb{Q}\setminus\{-1\}$! Ce qui est le cas.

Méthode 2 : La méthode 1 ne marche que si on a un candidat à proposer pour e. Ce qui n'est pas toujours possible à "deviner". Il est alors préférable de trouver e en résolvant les équations $a\star e=e\star a=a$ (ou simplement $a\star e=a$ dans le cas où $\star$ est commutative). Il est important de noter que e doit être indépendant de tous les $a\in E$. On cherche donc $e\in E$ tel que $a+e+ae=a$. Ceci équivaut à $e(1+a)=0$. Puisque $a+1\neq 0$ ($a\in E$), on peut diviser cette relation par $1+a$ pour obtenir $e=0$. Le nombre $e=0$ est donc pour l'instant un candidat pour le neutre. Il faut ensuite bien vérifier $a\star e=e\star a=a$ pour tout $a\in E$. Ce qui est le cas.

(4) Inverses : Pour tout $a\in\mathbb{Q}\setminus\{-1\}$, on cherche $b\in\mathbb{Q}\setminus\{-1\}$ (unique) tel que $a\star b=b\star a=e=0$. Puisque la loi $\star$ est commutative, il suffit de résoudre l'équation $a\star b=0$, c'est-à-dire

$$a+b+ab=0\Longleftrightarrow b(1+a)=-a\Longleftrightarrow b=\frac{-a}{1+a},$$

puisque $a+1\neq 0$.

Il faut vérifier que $b\in\mathbb{Q}\setminus\{-1\}$ **!** Puisque $a\in\mathbb{Q}\setminus\{-1\}$, il est clair que $b\in\mathbb{Q}$ comme quotient de deux nombres rationnels. On va montrer que $b\neq -1$ par un raisonnement

par l'absurde. Supposons donc que $b = -1$, i.e $\frac{-a}{1+a} = -1$ ou encore $-a = -1 - a$, ce qui donnerait $0 = -1$. Ceci est impossible. Donc, on a montré que $b \neq -1$ et finalement $b \in \mathbb{Q} \setminus \{-1\}$.

Ainsi tout élément $a \in \mathbb{Q} \setminus \{-1\}$ est inversible pour la loi $\star$ et l'inverse est donné par la formule $a^{-1} = \frac{-a}{1+a}$. (Attention a^{-1} désigne ici l'inverse pour la loi $\star$, et non pas pour la loi $\times$!)

Conclusion : $(E, \star)$ est un groupe abélien.

3. Puisque tout $a \in E$ est inversible d'inverse a^{-1}, on a les équivalences suivantes :

$$\begin{aligned} a \star x = b &\iff a^{-1} \star (a \star x) = a^{-1} \star b \\ &\iff (a^{-1} \star a) \star x = a^{-1} \star b \\ &\iff e \star x = a^{-1} \star b \\ &\iff x = a^{-1} \star b. \end{aligned}$$

La solution x existe et elle est unique. Elle est donnée par cette dernière formule $x = a^{-1} \star b$. (Ceci a été vu en cours). Cette formule est générale pour les groupes. Sur l'exemple présent, ceci donne :

$$x = a^{-1} \star b = \left(\frac{-a}{1+a}\right) + b + \left(\frac{-a}{1+a}\right) b = \frac{b-a}{1+a}.$$

(Ceci revient à résoudre $a + x + ax = b$ pour $a, b \in E$ donnés.)

4. On pose $a = 2$ et $b = 3$ et on applique le résultat de la question 3. On calcule d'abord

$$a^{-1} = \frac{-a}{1+a} = -\frac{2}{3}.$$

Ainsi l'unique solution x de l'équation est donnée par

$$x = \left(-\frac{2}{3}\right) \star 3 = \left(-\frac{2}{3}\right) + 3 + \left(-\frac{2}{3}\right).3 = \frac{1}{3} \in E.$$

On peut aussi appliquer directement la formule $x = \frac{b-a}{1+a} = \frac{1}{3}$.

Exercice 130

Dans cet exercice, on considère le groupe abélien $(\mathbb{C}^*, \times)$ dont l'élément neutre est 1.

Soient z_1, $z_2 \in \mathbb{C}^*$. On pose $z_1 \mathcal{R} z_2$ si et seulement si $|z_1| = |z_2|$ (égalité des modules).

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{C}^*$.
2. Pour tout $z \in \mathbb{C}^*$, on pose

$$\overline{z} = \{\gamma \in \mathbb{C}^* : \gamma \mathcal{R} z\}.$$

Montrer que pour tous z_1, $z_2 \in \mathbb{C}^*$: $\quad z_1 \mathcal{R} z_2 \quad \iff \quad \overline{z_1} = \overline{z_2}$.

3. Soit $z \in \mathbb{C}^*$ fixé. Décrire géométriquement la classe
$$\overline{z} = \{\gamma \in \mathbb{C}^* \,|\, \gamma \,\mathcal{R}\, z\}$$
comme sous-ensemble de $\mathbb{C}^*$ (On identifiera $\mathbb{C}^*$ avec une partie du plan usuel). On appelle $\overline{z}$ la classe d'équivalence de z pour la relation d'équivalence $\mathcal{R}$. Pour tout $\gamma \in \overline{z}$, on dit que γ est un représentant de la classe $\overline{z}$.
4. Montrer que pour tout $z \in \mathbb{C}^*$, il existe un unique $0 < R < +\infty$ tel que $\overline{R} = \overline{z}$. (On dira que R est un représentant canonique de la classe $\overline{z}$). Dessiner la classe $\overline{z}$ et le R correspondant dans $\mathbb{C}^*$.
5. Montrer que pour tous $0 < R_1, R_2 < +\infty$ avec $R_1 \neq R_2$, les classes $\overline{R_1}$ et $\overline{R_2}$ sont disjointes.

   Dans la suite, on note $X = (\mathbb{C}^*/\mathcal{R}) := \{\overline{z}, z \in \mathbb{C}^*\}$, l'ensemble constitué des classes d'équivalences $\overline{z}$ pour z parcourant $\mathbb{C}^*$ (X est appelé *espace quotient de* $\mathbb{C}^*$ *par la relation* $\mathcal{R}$). Comme d'habitude, tout nombre $R \in \mathbb{R}$ est identifié au nombre complexe $\alpha = R + \mathbf{i}.0$. On note $\alpha = R$ pour simplifier.
6. En déduire que l'on a
$$(i) \quad X = (\mathbb{C}^*/\mathcal{R}) = \{\overline{R}, R > 0\} \quad \text{et} \quad (ii) \quad \mathbb{C}^* = \biguplus_{R>0} \overline{R}.$$
($\biguplus_{i\in J} A_i$ signifie que c'est l'union disjointe des ensembles A_i.)
7. En une phrase dire ce qu'est l'ensemble X. Puis interpréter graphiquement dans $\mathbb{C}^*$ l'égalité (ii) de la question précédente.
8. (a) Montrer que pour tous z_1, z_2, z_3, $z_4 \in \mathbb{C}^*$, tels que $\overline{z_1} = \overline{z_3}$ et $\overline{z_2} = \overline{z_4}$ alors $\overline{\widehat{(z_1 z_2)}} = \overline{\widehat{(z_3 z_4)}}$. (Le terme $\overline{\widehat{(z_1 z_2)}}$ désigne la classe du produit $(z_1 z_2)$ dans $\mathbb{C}^*$).

   En conséquence, on pose $\overline{z_1} \star \overline{z_2} = \overline{\widehat{(z_1 z_2)}}$ pour $z_1, z_2 \in \mathbb{C}^*$ alors $\star$ définit bien une loi de composition interne sur X puisque le produit ne dépend pas des représentants des classes $\overline{z_1}$ et $\overline{z_2}$.

   (b) Montrer que $(X, \star)$ est un groupe. Décrire l'élément neutre ainsi que l'inverse de toute classe $\overline{z}$ où $z \in \mathbb{C}^*$ (On donnera un représentant de la classe de l'inverse $(\overline{z})^{-1}$).
9. Montrer que l'application $\varphi\colon (X, \star) \to (]0, +\infty[, \times)$ définie par $\varphi(\overline{z}) = |z|$ est un isomorphisme de groupe, i.e

   (a) Pour tous $z_1, z_2 \in \mathbb{C}^*$,
$$\varphi(\overline{z_1} \star \overline{z_2}) = \varphi(\overline{z_1}).\varphi(\overline{z_2}) \qquad (h).$$
   Indication. Pour montrer que l'application φ est bien définie, on commencera par montrer que si γ est un représentant quelconque de la classe $\overline{z}$ alors $\varphi(\overline{\gamma}) = \varphi(\overline{z})$. Puis on montrera (a) et (b). (Rappel : $(]0, +\infty[, \times)$ est le groupe multiplicatif sur $]0, +\infty[$.)

(b) L'application φ est bijective de X dans $]0,\infty[$. Décrire puis interpréter φ^{-1}.

Dernière remarque : pour $z_1,\ z_2 \in \mathbb{C}^*$,

$$|z_1| = |z_2| \Longleftrightarrow |z_1 \times z_2^{-1}| = 1.$$

D'où l'on peut déduire aussi que $z_1 \mathcal{R}\, z_2$ si et seulement s'il existe $\gamma \in \mathbb{C}^*$ vérifiant $|\gamma| = 1$ et $z_1 = \gamma z_2$.

Éléments de réponse 130

1. Montrons que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{C}^*$:
   (a) Réflexivité. Soit $z \in \mathbb{C}^*$, alors $z \mathcal{R}\, z \Longleftrightarrow |z| = |z|$. Ceci est vrai.
   (b) Symétrie. Soient $z_1,\ z_2 \in \mathbb{C}^*$ tel que $z_1 \mathcal{R}\, z_2$ alors $|z_1| = |z_2|$ ou encore $|z_2| = |z_1|$, i.e $z_2 \mathcal{R}\, z_1$.
   (c) Transitivité. Soient $z_1, z_2, z_3 \in \mathbb{C}^*$ tels que $z_1 \mathcal{R}\, z_2$ et $z_2 \mathcal{R}\, z_3$, *i.e.* $|z_1| = |z_2|$ et $|z_2| = |z_3|$. On en déduit $|z_1| = |z_3|$, c'est-à-dire $z_1 \mathcal{R}\, z_3$.
2. Montrons que pour tous $z_1,\ z_2 \in \mathbb{C}^*$: $\quad z_1 \mathcal{R}\, z_2 \quad \Longleftrightarrow \quad \overline{z_1} = \overline{z_2}$.
   a) Montrons que si $z_1 \mathcal{R}\, z_2$, alors $\overline{z_1} = \overline{z_2}$.
   Soient $z_1,\ z_2 \in \mathbb{C}^*$ fixés. On suppose que $z_1 \mathcal{R}\, z_2$. Il faut montrer $\overline{z_1} = \overline{z_2}$.
      ◇ Montrons une première inclusion $\overline{z_1} \subset \overline{z_2}$.
      Soit $\gamma \in \overline{z_1}$. Alors on a $\gamma \mathcal{R} z_1$ et $z_1 \mathcal{R} z_2$. Par transitivité, on en déduit $\gamma \mathcal{R} z_2$, *i.e.* $\gamma \in \overline{z_2}$. Ainsi, on obtient : si $\gamma \in \overline{z_1}$, alors $\gamma \in \overline{z_2}$, *i.e.* $\overline{z_1} \subset \overline{z_2}$.
      ◇ Montrons la seconde inclusion $\overline{z_2} \subset \overline{z_1}$. La démonstration est similaire à la précédente et se fait simplement en échangeant les rôles de z_1 et z_2.
   b) Montrons désormais que si $\overline{z_1} = \overline{z_2}$, alors $z_1 \mathcal{R} z_2$.
   Soient $z_1,\ z_2 \in \mathbb{C}^*$ fixés. On suppose que $\overline{z_1} = \overline{z_2}$. Il faut montrer $z_1 \mathcal{R}\, z_2$. Par réflexivité $z_1 \mathcal{R}\, z_1$ donc $z_1 \in \overline{z_1}$. Puisque $\overline{z_1} = \overline{z_2}$, on en déduit $z_1 \in \overline{z_2}$ donc $z_1 \mathcal{R} z_2$. Ceci conclut l'assertion.
   Commentaire. Pour tout $z \in \mathbb{C}^*$ fixé, l'ensemble $\overline{z}$ est un sous-ensemble de $\mathbb{C}^*$ contenant exactement les éléments de $\mathbb{C}^*$ équivalent à z. En particulier, cet ensemble contient z lui-même. (Ceci est un fait général : la classe d'un élément contient toujours l'élément à cause de la réflexivité de $\mathcal{R}$).
3. Soit $z \in \mathbb{C}^*$ fixé. Décrivons géométriquement la classe

$$\overline{z} = \{\gamma \in \mathbb{C}^* : \gamma \mathcal{R}\, z\}$$

comme sous-ensemble de $\mathbb{C}^*$

Fixons $z \in \mathbb{C}^*$. Nous avons $\gamma \in \overline{z} \iff \gamma \mathcal{R} z \iff |\gamma| = |z|$: γ et z ont même module. Ainsi γ est sur le cercle de centre 0, origine du plan, et de rayon $\rho = |z|$ fixé. (Faire un dessin !).

La classe d'équivalence $\overline{z} = \{\gamma \in \mathbb{C}^* : \gamma \mathcal{R} z\}$ s'identifie donc à ce cercle de centre 0 et de rayon $|z|$ dans le plan. Ce résultat permet de se représenter géométriquement toutes les classes d'équivalence pour cette relation $\mathcal{R}$. (Attention : une interprétation géométrique n'est pas toujours possible pour les classes d'équivalence en général. Cette situation est particulière.)

Nous pouvons aussi interpréter la relation d'équivalence par : « deux nombres complexes non nuls sont équivalents au sens de la relation $\mathcal{R}$ si et seulement s'ils sont sur le même cercle de centre 0 ».

4. Montrons que pour tout $z \in \mathbb{C}^*$, il existe un unique $0 < R < +\infty$ tel que $\overline{R} = \overline{z}$. (Nous dirons que R est un représentant canonique de la classe $\overline{z}$).

   Soit $z \in \mathbb{C}^*$.

   Cherchons $R > 0$ tel que $\overline{R} = \overline{z}$. Puisque $\overline{R} = \overline{z} \iff R \mathcal{R} z \iff R = |R| = |z|$, l'unique candidat pour R est donc $R = |z|$. On a bien $R > 0$ car $z \neq 0$. Réciproquement, si on pose $R = |z| > 0$ alors $\overline{R} = \overline{z}$.

   On dessine la classe $\overline{z}$: c'est le cercle de rayon R et de centre l'origine du plan.

   Le représentant canonique de la classe $\overline{z}$ correspond ainsi au point $R + \mathbf{i}.0 = |z| + \mathbf{i}.0$ dans $\mathbb{C}^*$. Ce point est obtenu comme intersection du cercle de rayon R de centre l'origine du plan avec le demi-axe

$$D^+ = \{\gamma = x + \mathbf{i}y \in \mathbb{C}, x > 0, y = 0\}.$$

5. Montrons que pour tous $0 < R_1, R_2 < +\infty$ avec $R_1 \neq R_2$, les classes $\overline{R_1}$ et $\overline{R_2}$ sont disjointes.

   Nous raisonnons par l'absurde. Soit $0 < R_1, R_2 < +\infty$ avec $R_1 \neq R_2$. Supposons $\overline{R_1} \cap \overline{R_2} \neq \emptyset$. Il existe $\gamma \in \overline{R_1} \cap \overline{R_2}$ puisque cet ensemble est supposé non vide. Ainsi, nous avons $\gamma \mathcal{R} R_1$ et $\gamma \mathcal{R} R_2$, c'est-à-dire $|\gamma| = R_1$ et $|\gamma| = R_2$. D'où, il s'ensuit que $R_1 = R_2$. C'est impossible d'après l'hypothèse $R_1 \neq R_2$.

   Dans la suite, nous notons $X = (\mathbb{C}^*/\mathcal{R}) := \{\overline{z}, z \in \mathbb{C}^*\}$, l'ensemble constitué des classes d'équivalences $\overline{z}$ pour z parcourant $\mathbb{C}^*$ (X est appelé *espace quotient de* $\mathbb{C}^*$ *par la relation* $\mathcal{R}$). Comme d'habitude, tout nombre $R \in \mathbb{R}$ est identifié au nombre complexe $\alpha = R + \mathbf{i}.0$. On note $\alpha = R$ pour simplifier.

6. (i) Il est clair que $\{\overline{R}, R > 0\} \subset \{\overline{z}, z \in \mathbb{C}^*\} = X$. Maintenant, si $z_0 \in \mathbb{C}^*$ alors il existe $R_0 > 0$ tel que $\overline{R_0} = \overline{z_0}$ par la question (4), et ainsi $\overline{z_0} = \overline{R_0} \in \{\overline{R}, R > 0\}$. D'où l'on déduit $X \subset \{\overline{R}, R > 0\}$. Ceci démontre (i).

   (ii) Soit $z \in \mathbb{C}^*$ alors $z \in \overline{z} = \overline{R_0}$ pour $R_0 = |z|$. Donc $z \in \cup_{R>0} \overline{R}$. Puisque ceci est vrai pour tout $z \in \mathbb{C}^*$, on en déduit $\mathbb{C}^* \subset \cup_{R>0} \overline{R}$. Maintenant, on a par définition

$\overline{R} = \{\gamma \in \mathbb{C}^*, ...\}$, donc $\overline{R} \subset \mathbb{C}^*$ pour tout $R > 0$. D'où l'on déduit $\cup_{R>0} \overline{R} \subset \mathbb{C}^*$. Il s'ensuit l'égalité $\cup_{R>0} \overline{R} = \mathbb{C}^*$.

De plus, l'union des classes $\overline{R}$ est une union disjointe d'après la question (5). Ceci démontre (ii).

Remarque : On peut réécrire $X = \{\overline{R}, R > 0\} = \cup_{R>0}\{\overline{R}\}$ (X s'écrit comme réunion de ses éléments $\overline{R}$). Ceci n'est pas à confondre avec $\mathbb{C}^* = \cup_{R>0} \overline{R}$ (réunion des sous-ensembles $\overline{R}$ de $\mathbb{C}^*$).

7. (i) L'ensemble X est par définition l'ensemble des classes d'équivalence : c'est donc l'ensemble des cercles du plan concentriques en l'origine. (Faire un dessin de plusieurs cercles concentriques dans le plan. Attention on ne peut pas les dessiner tous car ils sont en nombre infini !).

   (ii) L'égalité $\mathbb{C}^* = \biguplus_{R>0} \overline{R}$ signifie que l'on a partitionné le plan privé de l'origine en la réunion des cercles concentriques. Ceci n'est que l'interprétation, dans ce cas particulier, de la théorie générale qui dit que l'ensemble des classes d'équivalence sur un ensemble E forme une partition de E. L'exemple ici est concret.

8. (a) Montrons que pour tous z_1, z_2, z_3, $z_4 \in \mathbb{C}^*$, tels que $\overline{z_1} = \overline{z_3}$ et $\overline{z_2} = \overline{z_4}$ alors $\overline{\widehat{(z_1 z_2)}} = \overline{\widehat{(z_3 z_4)}}$. (Le terme $\overline{\widehat{(z_1 z_2)}}$ désigne la classe du produit $(z_1 z_2)$ dans $\mathbb{C}^*$).

   En conséquence, nous posons $\overline{z_1} \star \overline{z_2} = \overline{\widehat{(z_1 z_2)}}$ pour z_1, $z_2 \in \mathbb{C}^*$ alors $\star$ définit bien une loi de composition interne sur X puisque le produit ne dépend pas des représentants des classes $\overline{z_1}$ et $\overline{z_2}$.

   Supposons que $\overline{z_1} = \overline{z_3}$ et $\overline{z_2} = \overline{z_4}$. Nous voulons montrer que $\overline{\widehat{(z_1 z_2)}} = \overline{\widehat{(z_3 z_4)}}$. Par hypothèse, on sait que $|z_1| = |z_3|$ et $|z_2| = |z_4|$. On en déduit $|z_1 z_2| = |z_1||z_2| = |z_3||z_4| = |z_3 z_4|$, c'est-à-dire $(z_1 z_2)\,\mathcal{R}\,(z_3 z_4)$, i.e $\overline{\widehat{(z_1 z_2)}} = \overline{\widehat{(z_3 z_4)}}$ d'après la question (2).

   (b) Montrons que $(X, \star)$ est un groupe. Décrivons l'élément neutre ainsi que l'inverse de toute classe $\overline{z}$ où $z \in \mathbb{C}^*$ (Nous donnerons un représentant de la classe de l'inverse $(\overline{z})^{-1}$).

   Associativité. Pour tous $z_1, z_2, z_3 \in \mathbb{C}^*$, on a

$$(\overline{z_1} \star \overline{z_2}) \star \overline{z_3} = \overline{\widehat{(z_1 z_2)}} \star \overline{z_3} = \overline{\widehat{(z_1 z_2) z_3}} = \overline{z_1 \widehat{(z_2 z_3)}} = \overline{z_1} \star \overline{\widehat{(z_2 z_3)}} = \overline{z_1} \star (\overline{z_2} \star \overline{z_3}),$$

   où on a utilisé l'associativité dans le groupe $(\mathbb{C}^*, \times)$.

   Commutativité. Pour tous $z_1, z_2 \in \mathbb{C}^*$, on a

$$\overline{z_1} \star \overline{z_2} = \overline{\widehat{(z_1 z_2)}} = \overline{\widehat{(z_2 z_1)}} = \overline{z_2} \star \overline{z_1}$$

   où on a utilisé la commutativité dans le groupe $(\mathbb{C}^*, \times)$.

   Le neutre. Posons $e = \overline{1}$. Pour tout $z \in \mathbb{C}^*$,

$$\overline{z} \star \overline{1} = \overline{1} \star \overline{z} = \overline{\widehat{(1 \times z)}} = \overline{\widehat{(z \times 1)}} = \overline{z}.$$

Ainsi, $\overline{1}$ est l'élément neutre pour la loi $\star$ sur X.

Inverses. Soit $z \in \mathbb{C}^*$. Alors l'inverse $\frac{1}{z}$ existe dans $\mathbb{C}^*$. Ainsi, $\overline{(\frac{1}{z})}$ est un bon candidat pour l'inverse de la classe $\overline{z}$. En effet, on a

$$\overline{z} \star \overline{(\frac{1}{z})} = \overline{(\frac{1}{z})} \star \overline{z} = \overline{\widehat{(\frac{1}{z}.z)}} = \overline{1}.$$

L'inverse de $\overline{z}$ noté $(\overline{z})^{-1}$ est égal à $\overline{(\frac{1}{z})}$. ($\frac{1}{z}$ est donc un représentant de la classe de $(\overline{z})^{-1}$).

Nous en concluons que $(X, \star)$ est un groupe abélien.

9. Montrons que l'application $\varphi : (X, \star) \to (]0, +\infty[, \times)$ définie par $\varphi(\overline{z}) = |z|$ est un isomorphisme de groupe, *i.e.*

   (a) Pour tous $z_1, z_2 \in \mathbb{C}^*$,

   $$\varphi(\overline{z_1} \star \overline{z_2}) = \varphi(\overline{z_1}).\varphi(\overline{z_2}) \qquad (h).$$

   Indication. Pour montrer que l'application φ est bien définie, nous commencerons par montrer que si γ est un représentant quelconque de la classe $\overline{z}$ alors $\varphi(\overline{\gamma}) = \varphi(\overline{z})$. Puis nous montrerons (a) et (b). (Rappel : $(]0, +\infty[, \times)$ est le groupe multiplicatif sur $]0, +\infty[$.)

   Montrons d'abord que φ est bien définie. Pour cela il faut montrer que si γ est un représentant quelconque de la classe $\overline{z}$, i.e. $\gamma \mathcal{R} z$, alors $\varphi(\overline{\gamma}) = \varphi(\overline{z})$. Ceci est bien le cas puisque $\gamma \mathcal{R} z$, i.e $|\gamma| = |z|$, c'est-à-dire $\varphi(\overline{\gamma}) = |\gamma| = |z| = \varphi(\overline{z})$.

   Montrons maintenant la formule d'homomorphisme (h). Soient z_1, $z_2 \in \mathbb{C}^*$. À l'aide des définitions et de la propriéte " le module d'un produit dans $\mathbb{C}$ est le produit des modules", on obtient

   $$\varphi(\overline{z_1} \star \overline{z_2}) = \varphi(\overline{\widehat{z_1 z_2}}) = |z_1 z_2| = |z_1|.|z_2| = \varphi(\overline{z_1}) \times \varphi(\overline{z_2}).$$

   (b) L'application φ est bijective de X dans $]0, \infty[$. Décrire puis interpréter φ^{-1}.

Montrons que φ est injective. Soient $\overline{z_1}, \overline{z_2} \in X$ (*i.e.* deux classes d'équivalence quelconques). Nous avons les équivalences suivantes :

$$\varphi(\overline{z_1}) = \varphi(\overline{z_2}) \Longleftrightarrow |z_1| = |z_2| \Longleftrightarrow z_1 \mathcal{R} z_2 \Longleftrightarrow \overline{z_1} = \overline{z_2}.$$

La dernière équivalence est obtenue par la question (2). D'où φ est injective.

Montrons que φ est surjective. Soit $R \in]0, \infty[$. On a

$$\varphi(\overline{R}) = |R| = R$$

car $R > 0$. Ainsi, nous pouvons prendre comme antécédent de R simplement la classe de R. L'application φ est bien surjective. La solution à la surjectivité permet de construire l'application inverse φ^{-1} : voir ci-dessous. En conclusion, φ est bijective.

Dernière remarque (hors devoir) : pour z_1, $z_2 \in \mathbb{C}^*$,

$$|z_1| = |z_2| \Longleftrightarrow |z_1 \times z_2^{-1}| = 1.$$

D'où l'on peut déduire aussi que $z_1 \mathcal{R} z_2$ si et seulement s'il existe $\gamma \in \mathbb{C}^*$ vérifiant $|\gamma| = 1$ et $z_1 = \gamma z_2$.

Description de φ^{-1}. On pose $\varphi^{-1} : (]0, +\infty[, \times) \to (X, \star)$ avec $\varphi^{-1}(\rho) = \overline{\rho}$ pour tout $\rho > 0$. On a bien $\varphi^{-1}(\rho) \in X = \{\overline{R}, R > 0\}$. Il reste à vérifier que

$$\varphi^{-1} \circ \varphi \colon X \longrightarrow X$$

et

$$\varphi \circ \varphi^{-1} \colon]0, +\infty[\longrightarrow]0, +\infty[$$

sont respectivement les applications identités Id_X et $Id_{]0,+\infty[}$. Par ailleurs, ceci démontrera une nouvelle fois que φ est bijective (voir cours ou td de L1).

(i) Soit $\overline{z} \in X$. On a $(\varphi^{-1} \circ \varphi)(\overline{z}) = \varphi^{-1}[\varphi(\overline{z})] = \varphi^{-1}(|z|) = \overline{\widehat{|z|}} = \overline{z}$.

La dernière égalité provient du fait que $|z| \mathcal{R} z$ donc les classes sont égales. On en conclut $\varphi^{-1} \circ \varphi = Id_X$.

(ii) Soit $\rho > 0$, on a $(\varphi \circ \varphi^{-1})(\rho) = \varphi[\varphi^{-1}(\rho)] = \varphi(\overline{\rho}) = |\rho| = \rho$ car $\rho > 0$. On en conclut $\varphi \circ \varphi^{-1} = Id_{]0,+\infty[}$.

Interprétation géométrique. L'application φ^{-1} associe à tout $\rho > 0$ le cercle de rayon ρ et de centre l'origine du plan.

□

Commentaires supplémentaires :

Un isomorphisme entre deux groupes signifie que les deux groupes « fonctionnent de manière semblable » en tant que groupes (et a priori uniquement en tant que groupe). Dans notre cas, le groupe des classes d'équivalence $(X, \star)$ « fonctionne » comme le groupe multiplicatif $(]0, +\infty[, \times)$! Vu du coté de X qui est l'ensemble des cercles concentriques en l'origine du plan, on peut donc définir une "multiplication" $\star$ entre les cercles ! (Dans ce qui suit, les cercles seront toujours des cercles de centre l'origine du plan.) Ainsi le cercle de rayon $R_1 > 0$ « multiplié » par le cercle de rayon $R_2 > 0$ est le cercle de rayon $R = R_1 R_2 > 0$! Le cercle unité $(R = 1)$ est l'unité pour cette multiplication ! « L'inverse du cercle de rayon $R > 0$ est le cercle de rayon $\frac{1}{R} > 0$! »

Exercice 131

Soit $(\mathrm{G}, \cdot)$ un groupe. Soient a et b deux éléments de G.

1. Montrer que si a et b sont conjugués, *i.e.* s'il existe $g \in \mathrm{G}$ tel que $b = gag^{-1}$, alors ils ont le même ordre (éventuellement infini).
2. La réciproque est-elle vraie ? Justifier (démonstration ou contre-exemple).
3. Montrer que ab et ba ont le même ordre (éventuellement infini).
4. Supposons a d'ordre $n \in \mathbb{N}^*$. Quel est l'ordre de a^2 ? Quel est l'ordre de a^k, où $k \in \mathbb{N}$? Quel est l'ordre de a^{-1} ? Quel est l'ordre de a^{-k} où $k \in \mathbb{N}$?

Éléments de réponse 131

1. Supposons que a et b soient conjugués, *i.e.* qu'il existe $g \in \mathrm{G}$ tel que $b = gag^{-1}$.

   Une rédaction possible :

   Rappelons le théorème suivant : soit $(\mathrm{G}, \cdot)$ un groupe et soit a un élément d'ordre k de G ; alors $a^n = e$ si et seulement si $k \,|\, n$.

   Notons k l'ordre de a et ℓ l'ordre de gag^{-1}. On vérifie que $(gag^{-1})^k = e$ donc ℓ divise k. Par ailleurs $g^{-1}(gag^{-1})g$ a pour ordre k et $(g^{-1}(gag^{-1})g)^\ell = e$ donc k divise ℓ. Il s'en suit que $k = \ell$.

   Une seconde rédaction possible :

   Notons k l'ordre de a. Rappelons que cela signifie d'une part que $a^k = e$, d'autre part que $a^p \neq e$ pour tout $1 \leq p < k$. Soit $\ell \geq 1$ un entier tel que $(gag^{-1})^\ell = e$; à partir de

   $$(gag^{-1})^\ell = e \quad \Longleftrightarrow \quad ga^\ell g^{-1} = e \quad \Longleftrightarrow \quad a^\ell = e$$

   nous obtenons que

   $$\mathrm{ord}(gag^{-1}) = \min\{\ell \geq 1 \,|\, (gag^{-1})^\ell = e\} = \min\{\ell \geq 1 \,|\, a^\ell = e\} = \mathrm{ord}(a).$$

2. La réciproque est fausse.

   Un premier exemple :

   Par exemple si $\mathrm{G} = \mathfrak{S}_4$, alors les permutations (1 2) et (1 2)(3 4) sont d'ordre 2 mais ne sont pas conjuguées (la première a deux points fixes, 3 et 4, alors que la seconde n'en a pas).

   Un second exemple :

   Considérons le groupe $\mathbb{U}_3 = \{z \in \mathbb{C} \,|\, z^3 = 1\}$ des racines 3-ème de l'unité ; le groupe $\mathbb{U}_3$ est formé des éléments

   $$1, \qquad z_1 = \exp\left(\frac{2\mathbf{i}\pi}{3}\right), \qquad z_2 = \exp\left(\frac{4\mathbf{i}\pi}{3}\right).$$

   Les éléments z_1 et z_2 sont d'ordre 3 (ce sont des générateurs de $\mathbb{U}_3$) ; par contre z_1 et z_2 ne sont pas conjugués. En effet, raisonnons par l'absurde : supposons que z_1 et z_2 soient conjugués, *i.e.* il existe $z \in \mathbb{U}_3$ tel que $z_1 = zz_2z^{-1}$. Comme $\mathbb{U}_3$ est abélien nous avons $zz_2z^{-1} = zz^{-1}z_2 = z_2$; par conséquent $z_1 = zz_2z^{-1}$ se réécrit $z_1 = z_2$: contradiction. Finalement z_1 et z_2 sont d'une part deux éléments d'ordre 3 de $\mathbb{U}_3$, d'autre part deux éléments non conjugués dans $\mathbb{U}_3$.

3. Remarquons que $ba = ba(bb^{-1}) = b(ab)b^{-1}$. D'après 1. $b(ab)b^{-1}$ et ab ont même ordre donc ba et ab ont même ordre.

4. Supposons a d'ordre $n \in \mathbb{N}^*$.

   Déterminons l'ordre de a^2.

   D'abord, remarquons que a^2 est d'ordre fini car $(a^2)^n = (a^n)^2 = e^2 = e$. De plus, l'ordre de a^2, que nous allons noter d, divise n. Distinguons alors deux cas :

- ◇ Si n est pair et s'écrit $2p$, alors $(a^2)^p = a^n = e$, et donc l'ordre de a^2 divise p. De plus, si l'ordre de a^2 est inférieur strict à p ($d < p$), alors nous avons $a^{2d} = e$ avec $1 \leq 2d < 2p = n$, ce qui contredit la définition de l'ordre de a. Ainsi, si n est pair, l'ordre de a^2 est $\frac{n}{2}$.
- ◇ Si n est impair, alors on a $a^{2d} = (a^2)^d = e$ et donc n divise $2d$. Mais comme n est premier avec 2, nous obtenons $n|d$. Puisque nous avions déjà remarqué que $d|n$, nous en déduisons que $d = n$. En résumé, si n est impair, l'ordre de a^2 est n.

Montrons que si $k \in \mathbb{N}$, alors l'ordre de a^k est $\frac{n}{\text{pgcd}(n,k)}$.

Rappelons que si $(\mathrm{G}, \cdot)$ est un groupe fini et si a est un élément de G d'ordre m, alors

- ◇ par définition m est le plus petit entier naturel non nul tel que $a^m = 1$;
- ◇ m divise $|\mathrm{G}|$ (en effet d'une part $m = |\langle a \rangle|$ et d'autre part le théorème de Lagrange assure que l'ordre d'un sous-groupe de G divise $|\mathrm{G}|$) ;
- ◇ les éléments 1, a, a^2, …, a^{m-1} sont tous distincts dans G ; de plus, $\langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}$ (cette égalité découle d'une part de l'inclusion $\{1, a, a^2, \ldots, a^{m-1}\} \subset \langle a \rangle$ et d'autre part de $|\langle a \rangle| = |\{1, a, a^2, \ldots, a^{m-1}\}|$).

D'après ce qui précède

$$|\langle a^k \rangle| = \min\{m \in \mathbb{N}^* \,|\, (a^k)^m = 1\} = \min\{m \in \mathbb{N}^* \,|\, a^{km} = 1\} = \min\{m \in \mathbb{N}^* \,|\, n|km\}$$

Soit $d = \text{pgcd}(n, k)$. Il existe alors deux entiers naturels n' et k' tels que $n = dn'$ et $k = dk'$ et $\text{pgcd}(n', k') = 1$. Ainsi, $n \,|\, km$ équivaut à $dn' \,|\, dk'm$ et à $n' \,|\, m$ car $\text{pgcd}(n', k') = 1$. Or, le plus petit entier $m \in \mathbb{N}^*$ tel que $n' \,|\, m$ est n', c'est-à-dire $\frac{n}{\text{pgcd}(n,k)}$. D'où pour tout $k \geq 1$

$$|\langle a^k \rangle| = \frac{n}{\text{pgcd}(n, k)}$$

Une rédaction possible :

L'ordre de a^{-1} est n. En effet, à partir de $a^n = e$ nous avons $a^{n-\ell}a^\ell = a^\ell a^{n-\ell} = a^n = e$ pour tout $1 \leq \ell \leq n-1$ d'où $a^{-\ell} = a^{n-\ell}$ ou encore $(a^{-1})^\ell = a^{n-\ell}$. Ainsi $\langle a^{-1} \rangle = \langle a \rangle$ et $|\langle a^{-1} \rangle| = |\langle a \rangle| = n$.

Pour tout $1 \leq k \leq n-1$ nous avons $a^{-k} = a^{n-k}$. Puisque $n - k \geq 1$ nous avons : l'ordre de a^{n-k} est $\frac{n}{\text{pgcd}(n,n-k)}$; par suite l'ordre de a^{-k} est $\frac{n}{\text{pgcd}(n,n-k)} = \frac{n}{\text{pgcd}(n,k)}$ (en effet s divise k et n si et seulement si s divise k et $n - k$).

Une seconde rédaction possible :

Soit $k \in \mathbb{N}^*$; nous avons

$$\begin{aligned}
\mathrm{ord}(a^{-k}) &= \min\{\ell \geq 1 \,|\, (a^{-k})^\ell = e\} \\
&= \min\{\ell \geq 1 \,|\, a^{-k\ell} = e\} \\
&= \min\{\ell \geq 1 \,|\, (a^{-k\ell})^{-1} = e^{-1}\} \\
&= \min\{\ell \geq 1 \,|\, (a^{-k\ell})^{-1} = e\} \\
&= \min\{\ell \geq 1 \,|\, a^{k\ell} = e\} \\
&= \mathrm{ord}(a^k) \\
&= \frac{n}{\mathrm{pgcd}(n,k)}
\end{aligned}$$

Exercice 132

1. Considérons l'ensemble
$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,|\, a,\, b,\, c,\, d \in \mathbb{Z},\, ad - bc = 1 \right\};$$
muni de la multiplication matricielle cet ensemble est un groupe.

   Soient A et B les éléments de $(\mathrm{SL}(2,\mathbb{Z}), \cdot)$ définis par
$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$
   a) Quel est l'ordre de A ?
   b) Quel est l'ordre de B ?
   c) Quel est l'ordre de AB ?
   d) Sans nouveau calcul, donner l'ordre de BA.
2. Existe-t-il un groupe d'ordre 6 qui ne contient aucun élément d'ordre 6 ? Justifier (démonstration ou contre-exemple).
3. Existe-t-il un élément d'ordre 4 dans le groupe $(\mathrm{GL}(2,\mathbb{R}), \cdot)$? Justifier (démonstration ou contre-exemple).
4. Existe-t-il un groupe infini dont tous les éléments sont d'ordre fini ? Justifier (démonstration ou contre-exemple).

Éléments de réponse 132

1. a) L'ordre de A est 4.
   b) L'ordre de B est 3.
   c) L'ordre de $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est infini car $AB^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.
   d) Nous avons vu précédemment que AB et BA ont même ordre donc c) assure que BA est d'ordre infini.

2. Le groupe $\mathfrak{S}_3$ est d'ordre 6 mais ne contient aucun élément d'ordre 6.

   Le groupe des isométries préservant un triangle équilatéral est d'ordre 6 mais ne contient aucun élément d'ordre 6.

3. La matrice $M = A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est un élément de $\big(\mathrm{GL}(2,\mathbb{R}),\cdot\big)$; de plus

$$M^2 = -\mathrm{id}, \qquad M^3 = -M, \qquad M^4 = \mathrm{id}.$$

4. Il existe des groupes infinis dont tous les éléments sont d'ordre fini, par exemple le groupe additif $\mathbb{Z}/2\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Un second exemple est le groupe multiplicatif de toutes les racines de l'unité de n'importe quel ordre. Un troisième exemple est le suivant : $(\mathrm{G},*) = \Big(\{-1,1\}^{\mathbb{N}},\times\Big)$ est un groupe infini (non dénombrable) dont l'ordre de chaque élément est 2 (donc uniformément borné) sauf $e = (1,1,\ldots,1)$.

Exercice 133

Pour chacune des questions qui suivent veillez à justifier votre réponse par une démonstration ou un contre-exemple.

Soit G un groupe.

1. Supposons que G soit abélien ; G est-il cyclique ?
2. Supposons que G soit cyclique ; G est-il abélien ?
3. Soit G un groupe cyclique ; le groupe G est-il d'ordre premier ?
4. Rappelons que si H est un sous-groupe d'un groupe G, on dit que H est propre si $\mathrm{H} \neq \mathrm{G}$.

   Soit G un groupe ayant la propriété suivante : tout sous-groupe propre H de G est cyclique. Le groupe G est-il cyclique ?

Éléments de réponse 133

1. L'assertion 1. est fausse, considérons par exemple $(\mathrm{G},*) = \Big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},+\Big)$, c'est un groupe abélien, non cyclique.

2. Si G est un groupe cyclique, alors G est abélien. En effet si G est cyclique, il existe $g \in \mathrm{G}$ tel que $\mathrm{G} = \langle g\rangle$. Soient a et b dans G, ils s'écrivent aussi g^ℓ et g^k, ℓ, $k \in \mathbb{Z}$ et

$$ab = g^\ell g^k = g^{\ell+k} = g^{k+\ell} = g^k g^\ell = ba.$$

3. L'assertion 3. est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z}$, c'est un groupe cyclique mais 4 n'est pas premier.

4. L'assertion 4. est fausse. Le groupe $(\mathrm{G},*) = \Big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},+\Big)$ n'est pas cyclique (il n'y a pas d'élément d'ordre 4) mais ses sous-groupes H sont d'ordre 1 ou 2 et sont donc cycliques.

Exercice 134

Considérons l'ensemble

$$\mathrm{H} = \{(x, y) \in \mathbb{Z}^2 \,|\, x + y \text{ est pair}\}.$$

1. Montrer que H est un sous-groupe de $(\mathbb{Z}^2, +)$.
2. Montrer que l'application

$$\varphi\colon \mathbb{Z}^2 \to \mathrm{H}, \qquad (a, b) \mapsto (a, 2b - a)$$

est un isomorphisme de groupes.

Éléments de réponse 134

1. Remarquons que
   - ◇ H est un sous-ensemble de $\mathbb{Z}^2$;
   - ◇ H n'est pas vide : $(0, 0)$ appartient à H ($0 + 0 = 0$ est pair) ;
   - ◇ H est stable par addition : soient (x, y) et (u, v) dans H, alors il existe deux entiers relatifs n et m tels que $x + y = 2n$ et $u + v = 2m$. Par ailleurs $(x, y) + (u, v) = (x + u, y + v)$ et
   $$(x + u) + (y + v) = \underbrace{(x + y)}_{2n} + \underbrace{(u + v)}_{2m} = 2n + 2m = 2\,\underbrace{(n + m)}_{\in\mathbb{Z}}$$
   i.e. $(x + u) + (y + v)$ est pair. Il en résulte que $(x, y) + (u, v)$ appartient à H.
   - ◇ H est stable par passage à l'inverse : soit (x, y) dans H, alors il existe un entier relatif n tel que $x + y = 2n$. Par ailleurs $-(x, y) = (-x, -y)$ et
   $$(-x) + (-y) = -\underbrace{(x + y)}_{2n} = -2n = 2\,\underbrace{(-n)}_{\in\mathbb{Z}}$$
   i.e. $-(x, y)$ appartient à H.

   Par conséquent H est un sous-groupe de $(\mathbb{Z}^2, +)$.
2. Remarquons que $\varphi(\mathbb{Z}^2) \subset \mathrm{H}$. Soit (a, b) dans $\mathbb{Z}^2$; alors $\varphi(a, b) = (a, 2b-a)$ et $a+(2b-a) = 2b$ est pair, *i.e.* $\varphi(a, b)$ appartient à H.

   Commençons par montrer que φ est un morphisme de groupes : soient (a, b) et (u, v) dans $\mathbb{Z}^2$; d'une part

$$\varphi((a, b)+(u, v)) = \varphi(a+u, b+v) = (a+u, 2(b+v)-(a+u)) = (a+u, 2b+2v-a-u) = (a+u, 2b-a+2v-u)$$

   et d'autre part

$$\varphi(a, b) + \varphi(u, v) = (a, 2b - a) + (u, 2v - u) = (a + u, 2b - a + 2v - u).$$

   Ainsi $\varphi((a, b) + (u, v)) = \varphi(a, b) + \varphi(u, v)$ et φ est un morphisme de groupes.

Montrons que φ est injectif. Soit (a,b) dans $\mathbb{Z}^2$ tel que $\varphi(a,b)=(0,0)$, *i.e.* tel que $(a,2b-a)=(0,0)$; alors $a=0$ et $2b-a=0$, soit $a=0$ et $b=0$. Il en résulte que le noyau de φ est réduit à $\{(0,0)\}$, c'est-à-dire que φ est injectif.

Montrons que φ est surjectif. Soit (a,b) dans H. On cherche (u,v) dans $\mathbb{Z}^2$ tel que $\varphi(u,v)=(a,b)$. Mais $\varphi(u,v)=(u,2v-u)$ donc $\varphi(u,v)=(a,b)$ si et seulement si $u=a$ et $v=\frac{a+b}{2}$. Comme $\left(a,\frac{a+b}{2}\right)$ appartient à $\mathbb{Z}^2$ nous obtenons que $\varphi\left(a,\frac{a+b}{2}\right)=(a,b)$. Il s'en suit que φ est surjectif.

Finalement φ est un morphisme de groupes injectif et surjectif, autrement dit un isomorphisme de groupes.

Exercice 135

Soit $(\mathrm{G},\cdot)$ un groupe d'élément neutre e.

1. Soit φ l'application de G dans G définie par $\varphi(g)=g^{-1}$.

   Montrer que φ est un morphisme de groupes si et seulement si G est abélien.

2. Soit h un élément de G d'ordre fini m. Justifier que la partie $\{e,\, h,\, h^2,\, \ldots, h^{m-1}\}$ est un sous-groupe de G. Montrer que les h^k, $0\leq k\leq m-1$ sont deux à deux distincts.

   Soit ψ l'application de G dans G définie par $\psi(g)=g^2$.

3. Supposons que G est fini d'ordre impair n. Montrer que ψ est surjective (indication : utiliser le théorème de Lagrange).

4. Donner une condition nécessaire et suffisante assurant que ψ est un morphisme de groupes.

Éléments de réponse 135

1. Si φ est un morphisme de groupes, alors pour tous g_1, g_2 dans G, nous avons $\varphi(g_1^{-1}g_2^{-1})=\varphi(g_1^{-1})\varphi(g_2^{-1})$, c'est-à-dire $(g_1^{-1}g_2^{-1})^{-1}=(g_1^{-1})^{-1}(g_2^{-1})^{-1}$, soit $(g_2^{-1})^{-1}(g_1^{-1})^{-1}=g_1g_2$, ou encore $g_2g_1=g_1g_2$ ce qui montre que le groupe G est abélien.

   Réciproquement si G est abélien. Alors pour tous g_1, g_2 dans G nous avons $g_1^{-1}g_2^{-1}=g_2^{-1}g_1^{-1}$ ce qui se réécrit $\underbrace{g_1^{-1}}_{\varphi(g_1)}\underbrace{g_2^{-1}}_{\varphi(g_2)}=\underbrace{(g_1g_2)^{-1}}_{\varphi(g_1g_2)}$ ou encore $\varphi(g_1)\varphi(g_2)=\varphi(g_1g_2)$.

2. $e\in\{e,\, x,\, x^2,\, \ldots,\, x^{m-1}\}$.

   Soient $g,\, h\in\{e,\, x\, x^2,\, \ldots,\, x^{m-1}\}$. Il existe a et b dans $\{0,\, 1,\, 2\,\ldots, m-1\}$ tels que $g=x^a$ et $h=x^b$. Alors $gh^{-1}=x^ax^{-b}=x^{a-b}$. Effectuons la division euclidienne de $a-b$ par m : il existe un unique couple $(q,r)\in\mathbb{Z}\times\{0,\, 1,\, 2,\, \ldots,\, m-1\}$ tel que $a-b=mq+r$; par conséquent

   $$gh^{-1}=x^{mq+r}=(x^m)^qx^r=e^qx^r=x^r\in\{e,\, x,\, x^2,\, \ldots,\, x^{m-1}\}.$$

   Ces deux propriétés montrent que $\{e,\, x,\, x^2,\, \ldots,\, x^{m-1}\}$ muni de $\cdot$ est un sous-groupe de $(\mathrm{G},\cdot)$.

Puisque h est d'ordre m, le groupe $\langle h\rangle = \{e, h, h^2, \dots, h^{m-1}\}$ est d'ordre m ; en particulier les h^k, $0 \leq k \leq m-1$ sont deux à deux distincts.

3. L'entier n est impair, il existe donc $n' \in \mathbb{N}$ tel que $n = 2n' - 1$; une des conséquences du théorème de Lagrange veut que, pour tout $g \in \mathrm{G}$, $g^n = e$. Par suite

$$g^n = e \iff g^{2n'-1} = e \iff g^{2n'} = g \iff (g^{n'})^2 = g \iff \psi(g^{n'}) = g$$

Ainsi pour tout $g \in \mathrm{G}$ il existe $h = g^{n'}$ tel que $g = \psi(h)$ ce qui montre que ψ est surjective.

4. L'application ψ est un morphisme si et seulement si

$$\begin{aligned} & \forall\, g_1,\, g_2 \in \mathrm{G},\ \psi(g_1 g_2) = \psi(g_1)\psi(g_2) \\ \iff\ & \forall\, g_1,\, g_2 \in \mathrm{G},\ (g_1 g_2)^2 = g_1^2 g_2^2 \\ \iff\ & \forall\, g_1,\, g_2 \in \mathrm{G},\ g_1 g_2 g_1 g_2 = g_1 g_1 g_2 g_2 \\ \iff\ & \forall\, g_1,\, g_2 \in \mathrm{G},\ g_2 g_1 = g_1 g_2 \end{aligned}$$

Autrement dit ψ est un morphisme si et seulement si G est abélien.

□

1.4. Premiers pas

Exercice 136

Deux éléments de même ordre d'un groupe G sont-ils nécessairement conjugués ?

Éléments de réponse 136

Deux éléments conjugués ont bien sûr le même ordre, fini ou pas. La réciproque est fausse : par exemple si $\mathrm{G} = \mathfrak{S}_4$, alors les permutations (1 2) et (1 2)(3 4) sont d'ordre 2 mais ne sont pas conjuguées (la première a deux points fixes alors que la seconde n'en a pas).

Exercice 137

Soit G un groupe tel que pour tout sous-groupe $\mathrm{H} \subsetneq \mathrm{G}$ le sous-groupe H est cyclique. Le groupe G est-il cyclique ?

Éléments de réponse 137

Pas nécessairement. Par exemple le groupe $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique (il n'y a pas d'élément d'ordre 4) mais ses sous-groupes $\mathrm{H} \subsetneq \mathrm{G}$ sont d'ordre 1 ou 2 et doivent donc être cycliques.

Exercice 138

Soit n un entier naturel non nul. Montrer que $\{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Éléments de réponse 138

On commence par poser $\mu_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$ qui est bien une partie non vide de $\mathbb{C}^*$, puisqu'elle contient 1. Soit $z \in \mu_n$. On a

$$\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1$$

donc $\frac{1}{z}$ appartient à μ_n et ce dernier est stable par passage à l'inverse. Soient à présent z, z' dans μ_n. Nous avons

$$(zz')^n = z^n z'^n = 1$$

donc zz' appartient à μ_n et μ_n est stable par produit.

Ainsi μ_n est un sous-groupe multiplicatif de $\mathbb{C}^*$.

Exercice 139

Donner un exemple de groupe non abélien.

Éléments de réponse 139

Le groupe $\mathrm{GL}(2, \mathbb{R})$ des matrices inversibles à coefficients réels n'est pas abélien. En effet

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

mais

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

Un autre exemple était donné par le groupe $\mathrm{Isom}(T)$ des isométries du plan préservant un triangle équilatéral ou encore par le groupe symétrique $\mathfrak{S}_3$, c'est-à-dire le groupe contenant les six bijections de l'ensemble $\{1, 2, 3\}$.

Exercice 140

Donner un exemple de groupe contenant exactement 3 éléments.

Éléments de réponse 140

Le groupe $\mathbb{Z}/3\mathbb{Z}$ des entiers modulo 3 muni de l'addition. En effet $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

Un autre exemple est donné par le groupe des rotations préservant un triangle équilatéral

$$\mathrm{Isom}^+(T) = \{\mathrm{id}, r_{2\pi/3}, r_{-2\pi/3}\}$$

ou encore le groupe

$$\mu_3 = \{1, \exp\left(\frac{2\mathbf{i}\pi}{3}\right), \exp\left(-\frac{2\mathbf{i}\pi}{3}\right)\}$$

des racines cubiques de l'unité.

Exercice 141

Donner un exemple de groupe cyclique, préciser l'ensemble et la loi, et expliciter un générateur.

Éléments de réponse 141

Le groupe multiplicatif $\mu_n \subset \mathbb{C}^*$ des racines $n$ièmes de l'unité ; par exemple $\mu_3 = \{1, \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}, \mathrm{e}^{\frac{4\mathrm{i}\pi}{3}}\}$, engendré par $\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$.

Exercice 142

Donner un exemple de groupe abélien, fini et non cyclique, préciser l'ensemble et la loi.

Éléments de réponse 142

Le groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un exemple de groupe abélien, fini et non cyclique.

Le groupe des isométries d'un rectangle, qui est en fait isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, est un exemple de groupe abélien, fini et non cyclique.

Exercice 143

Donner un exemple de groupe infini monogène, préciser l'ensemble et la loi, et expliciter un générateur.

Éléments de réponse 143

Le groupe additif $\mathbb{Z}$ des entiers relatifs est un exemple de groupe infini monogène (c'est en fait le seul à isomorphisme près) ; 1 est un générateur.

Exercice 144

Donner un exemple de groupe abélien, infini, non monogène, préciser l'ensemble et la loi.

Éléments de réponse 144

Le groupe multiplicatif $\mathbb{R}^*$ est un exemple de groupe abélien, infini, non monogène ; les groupes additifs $\mathbb{R}$ ou $\mathbb{Z} \times \mathbb{Z}$ en sont d'autres.

Exercice 145

Donner un exemple de groupe fini, non abélien, préciser l'ensemble et la loi, et expliciter deux éléments qui ne commutent pas.

Éléments de réponse 145

Rappelons que $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ est le groupe des quaternions. La multiplication est définie par la règle des signes et les formules

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

Le groupe ainsi obtenu est non abélien : $ij = -ji$. Plus précisément le groupe des quaternions est l'un des deux groupes non abéliens d'ordre 8.

Le groupe $\mathfrak{S}_3$ est un groupe fini, non abélien :

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \neq (2\ 3)(1\ 2) = (1\ 3\ 2).$$

Exercice 146

Donner un exemple de groupe infini, non abélien, préciser l'ensemble et la loi, et expliciter deux éléments qui ne commutent pas.

Éléments de réponse 146

Le groupe $\mathrm{GL}(2,\mathbb{R})$ des matrices inversibles 2×2 à coefficients réels est un exemple de groupe infini non abélien. Par exemple

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

mais

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}.$$

Exercice 147

Répondre par vrai ou faux en donnant suivant les cas un court argument ou un contre-exemple :

1. Si G est un groupe cyclique, il existe $n \geq 1$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$: vrai ou faux ?
2. Il existe un groupe d'ordre 6 qui ne contient aucun élément d'ordre 6 : vrai ou faux ?
3. Il existe un élément d'ordre 4 dans le groupe $\mathrm{GL}(2,\mathbb{R})$: vrai ou faux ?
4. Il existe un groupe infini dont tous les éléments sont d'ordre fini : vrai ou faux ?
5. Une relation sur un ensemble X qui est symétrique et transitive est automatiquement réflexive : vrai ou faux ?

Éléments de réponse 147

1. Vrai. Si G est un groupe cyclique, par définition il existe $g \in \mathrm{G}$ et $n \geq 1$ tel que $\mathrm{G} = \langle g\rangle = \{1, g, g^2, \ldots, g^{n-1}\}$. Alors l'application
$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{G}, \qquad \overline{a} \mapsto g^a$$
est un isomorphisme.
2. Vrai. Le groupe $\mathrm{Isom}(T)$ des isométries préservant un triangle équilatéral est d'ordre 6 mais ne contient aucun élément d'ordre 6.

   Le groupe $\mathfrak{S}_3$ est d'ordre 6 mais ne contient aucun élément d'ordre 6.
3. Vrai. Par exemple la matrice $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ correspond à une rotation d'un quart de tour, et on vérifie que $M^2 = -\mathrm{id}$, $M^3 = -M$ et $M^4 = \mathrm{id}$.
4. Vrai. Il existe des groupes infinis dont tous les éléments sont d'ordre fini, par exemple le groupe additif $\mathbb{Z}/2\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Un autre exemple est le groupe multiplicatif $\mu_\infty \subset \mathbb{C}^*$ de toutes les racines de l'unité de n'importe quel ordre.

5. Faux. Donnons un contre-exemple. Soit $X = \{0, 1\}$. Considérons la relation $\sim$ donnée par $1 \sim 1$ mais $1 \not\sim 0$, $0 \not\sim 1$ et $0 \not\sim 0$. Cette relation est symétrique ($x \sim y$ implique $y \sim x$) et transitive ($x \sim y$ et $y \sim z$ impliquent $x \sim z$) mais pas réflexive (0 n'est pas en relation avec lui même).

Exercice 148

1. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un exemple de groupe fini, abélien et non cyclique : vrai ou faux ?
2. Il existe deux groupes d'ordre 4 non isomorphes : vrai ou faux ?
3. Il existe exactement quatre éléments d'ordre 2 dans le groupe $\mathrm{Isom}(R)$ des isométries du plan préservant un rectangle (non carré) R : vrai ou faux ?
4. Tous les sous-groupes du groupe symétrique $\mathfrak{S}_3$ sont distingués : vrai ou faux ?
5. Le groupe symétrique $\mathfrak{S}_{10}$ contient au moins un élément d'ordre 30 : vrai ou faux ?

Éléments de réponse 148

1. Faux : le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique engendré par exemple par $(\overline{1}, \widehat{1})$: c'est un cas particulier du lemme chinois.
2. Vrai : les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont tous deux d'ordre 4 mais non isomorphes. En effet $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est non cyclique car il contient seulement des éléments d'ordre 2 à part le neutre.
3. Faux : il n'y en a que trois qui sont la symétrie centrale (que l'on peut aussi voir comme une rotation d'angle π), et les deux symétries axiales par rapport aux droites passant par des milieux des côtés opposés. Le dernier élément du groupe est id qui est d'ordre 1.
4. Faux : le sous-groupe $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ n'est pas distingué dans $\mathfrak{S}_3$:
$$(1\ 3) \circ (1\ 2) \circ (1\ 3)^{-1} = (3\ 2)$$
5. Vrai : $(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$ convient car $30 = \mathrm{ppcm}(2, 3, 5)$.

Exercice 149

Justifier en une ou deux phrases chacune des réponses :

1. Donner la liste des éléments d'ordre 4 dans le groupe multiplicatif $\mathbb{C}^*$ des complexes non nuls.
2. Donner un exemple de polygone P tel que le groupe $\mathrm{Isom}(P)$ des isométries du plan préservant P soit d'ordre 4.
3. Donner un exemple d'élément d'ordre 4 dans le groupe alterné $\mathcal{A}_8$.
4. Donner un isomorphisme entre le groupe $\mathrm{Isom}(T)$ des isométries du plan préservant un triangle équilatéral et le groupe symétrique $\mathfrak{S}_3$.

5. Donner un exemple de groupe contenant à la fois des éléments d'ordre fini non triviaux et à la fois des éléments d'ordre infini.

Éléments de réponse 149

1. $\mathbf{i}$ et $-\mathbf{i}$ sont les éléments d'ordre 4 dans $\mathbb{C}^*$. Les deux autres racines 4ièmes de l'unité, qui sont 1 et -1, sont d'ordre 1 et 2 respectivement.
2. On peut prendre P un rectangle (non carré) ou encore un losange (non carré également). Dans le cas d'un rectangle le groupe $\mathrm{Isom}(P)$ contient l'identité, la symétrie centrale et les deux symétries axiales pour les deux droites passant par les milieux de côtés opposés.
3. La permutation $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ est d'ordre 4, de signature 1 car se factorise à l'aide de six transpositions : $\sigma = (1\ 2)(2\ 3)(3\ 4)(5\ 6)(6\ 7)(7\ 8)$
4. En numérotant p_1, p_2 et p_3 les sommets du triangle et en posant
$$\phi\colon \mathrm{Isom}(T) \to \mathfrak{S}_3, \qquad f \mapsto \sigma$$
tel que $f(p_i) = p_{\sigma(i)}$, on obtient l'isomorphisme attendu.
5. Le groupe $\mathbb{S}^1 \subset \mathbb{C}^*$ des complexes de module 1, pour la multiplication, convient : un élément $\mathrm{e}^{\mathbf{i}\theta}$ est d'ordre fini si et seulement si $\theta = 2\pi\alpha$ avec $\alpha \in \mathbb{Q}$.

   Un autre exemple est donné par le produit direct de $\mathfrak{S}_3$ avec $\mathbb{Z}$: un élément $(\sigma, n) \in \mathfrak{S}_3 \times \mathbb{Z}$ est d'ordre fini si et seulement si $n = 0$.

Exercice 150

Quelle est la loi naturelle qui permet de munir l'ensemble $\mathbb{C}^*$ des complexes non nuls d'une structure de groupe ? Quel est l'ordre de $\mathbf{i}$ pour cette loi ? Quel est l'ordre de 2 ?

Éléments de réponse 150

La multiplication permet de munir $\mathbb{C}^*$ d'une structure de groupe et
$$\mathrm{ordre}(\mathbf{i}) = 4, \qquad \mathrm{ordre}(2) = \infty.$$

Exercice 151

Si R est un rectangle (non carré), donner la liste des isométries du plan préservant ce rectangle. Cet ensemble est-il un groupe ?

Éléments de réponse 151

L'ensemble en question est bien un groupe pour la composition ; en effet il s'agit d'un sous-groupe du groupe des isométries du plan.

Notons O le centre du rectangle, c'est-à-dire l'intersection de deux diagonales. La liste éléments de $\mathrm{Isom}(R)$ consiste en les 4 isométries suivantes : l'identité, la rotation d'angle π centrée en O et les deux symétries axiales dont les axes passent par les milieux des côtés opposés.

Exercice 152

Donner un exemple de groupe d'ordre fini, abélien et non cyclique.

Éléments de réponse 152

Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ convient.

On peut aussi prendre le groupe des isométries préservant un rectangle qui est en fait isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 153

Soit $\sigma \in \mathfrak{S}_8$ le produit de cycles suivant

$$\sigma = (1\ 2\ 3\ 4\ 5\ 6) \circ (7\ 5\ 3\ 1) \circ (8\ 2\ 3)$$

Calculer la décompositon canonique de σ.

Éléments de réponse 153

La décomposition canonique de σ est

$$\sigma = (1\ 7\ 6) \circ (3\ 8) \circ (4\ 5).$$

Exercice 154

Soient T un triangle équilatéral et $\mathrm{Isom}(T)$ le groupe des isométries du plan préservant ce triangle.

Expliciter un isomorphisme du groupe $\mathrm{Isom}(T)$ vers le groupe symétrique $\mathfrak{S}_3$.

Éléments de réponse 154

Si A_1, A_2 et A_3 sont les sommets du triangle T, alors l'isomorphisme souhaité est donné par $f \in \mathrm{Isom}(T) \mapsto \sigma \in \mathfrak{S}_3$ où σ est définie par $f(A_i) = A_{\sigma(i)}$.

Exercice 155

Soit T un triangle équilatéral de sommets A, B et C et soit $\mathrm{Isom}(T) = \left\{\mathrm{id},\ s_A,\ s_B,\ s_C,\ r_{\frac{2\pi}{3}},\ r_{-\frac{2\pi}{3}}\right\}$ le groupe des isométries du plan préservant ce triangle.

Si $\mathrm{H} = \left\{\mathrm{id},\ s_A\right\}$, donner un exemple d'élément $g \in \mathrm{Isom}(T)$ tel que les classes à gauche et à droite de g soient distinctes, *i.e.* $g\mathrm{H} \neq \mathrm{H}g$.

Éléments de réponse 155

Par exemple $g = s_B$ convient car

$$s_B\mathrm{H} = \left\{s_B,\ s_B \circ s_A\right\}, \qquad \mathrm{H}s_B = \left\{s_B,\ s_A \circ s_B\right\}$$

et $s_B \circ s_A \neq s_A \circ s_B$ sont deux rotations d'angles opposés.

Notons que le choix de g n'est pas unique : $g = s_C$, $g = r_{2\pi/3}$ ou $g = r_{-2\pi/3}$ convient aussi.

Exercice 156

Calculer l'ordre de la permutation $\sigma \in \mathfrak{S}_{10}$ suivante

$$\sigma = (1\ 2\ 3\ 4\ 5) \circ (6\ 7\ 8) \circ (9\ 10)$$

Éléments de réponse 156

La permutation σ est du type 2, 3, 5. Son ordre est donc $\mathrm{ppcm}(2,3,5) = 30$.

Exercice 157

Donner une permutation $\sigma \in \mathfrak{S}_6$ telle que $\sigma \circ (1\ 3\ 5) \circ \sigma^{-1} = (2\ 4\ 6)$.

Éléments de réponse 157

Nous avons

$$\sigma \circ (1\ 3\ 5) \circ \sigma^{-1} = (\sigma(1)\ \sigma(3)\ \sigma(5))$$

donc $\sigma = (1\ 2)(3\ 4)(5\ 6)$ convient. Notons que le choix de σ n'est pas unique.

Exercice 158

Donner la liste des classes de conjugaison avec leur cardinal pour le groupe alterné $\mathcal{A}_5$.

Éléments de réponse 158

Le groupe $\mathcal{A}_5$ admet 5 classes de conjugaison :

- ◇ la classe de l'identité, de cardinal 1 ;
- ◇ la classe des 3-cycles, de cardinal 20 ;
- ◇ la classe des doubles transpositions, de cardinal 15 ;
- ◇ deux classes de 5-cycles, chacune de cardinal 12.

Notons que dans $\mathfrak{S}_5$ la réponse serait différente, il n'y aurait qu'une seule classe de 5-cycles, de cardinal 24.

Exercice 159

Donner un exemple de deux groupes d'ordre 8 non abéliens et non isomorphes.

Éléments de réponse 159

Le groupe diédral D_8 (le groupe des isométries préservant un carré) est non abélien d'ordre 8.

Le groupe des quaternions $\mathbb{H}_8$ engendré par les matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}, \qquad \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

est également non abélien d'ordre 8.

Ces deux groupes ne sont pas isomorphes ; ils ne contiennent pas le même nombre d'éléments d'ordre 2 : le groupe D_8 en contient 5 alors que $\mathbb{H}_8$ n'en contient qu'un seul.

Exercice 160

Parmi les ensembles suivants lesquels sont des groupes pour l'opération donnée ?

1. $\mathbb{Q}^\times$, $+$;
2. $\mathbb{Q}^\times$, $\cdot$;

3. $\mathbb{Z}/n\mathbb{Z}, \cdot$;
4. $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}, \cdot$;
5. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\}, \cdot$;
6. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 0\}, +$.

Éléments de réponse 160

2. $\mathbb{Q}^*, \cdot$;
5. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\}, \cdot$

sont des groupes.

Remarque sur le 1. : que dire du neutre ?

Remarque sur le 3. : que dire de l'inverse d'un élément ?

Remarque sur le 4. : $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}, \cdot$ n'est pas un groupe en général. Si n est premier, alors $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} = \mathbb{Z}/n\mathbb{Z}^*$ est un groupe.

Remarque sur le 6. : l'opération + n'est pas interne. Soient

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix};$$

nous avons

$$\det A = 0 \qquad \det B = 0 \qquad \det A + B = 1 \neq 0.$$

Exercice 161

Parmi les groupes suivants lesquels sont abéliens ?

1. $\mathbb{R}[x]_{\leq 8}, +$ (les polynômes de degré $d \leq 8$ dans une variable x à coefficients réels) ;
2. $\mathrm{GL}(n, \mathbb{R}), \cdot$ (les matrices inversibles de taille $n \times n$ à coefficients réels) ;
3. $\mathfrak{S}_4, \circ$ (le groupe symétrique sur l'ensemble à 4 éléments).

Éléments de réponse 161

$\mathbb{R}[x]_{\leq 8}, +$ (les polynômes de degré $d \leq 8$ dans une variable x à coefficients réels) est un groupe abélien.

Exercice 162

Lesquels des ensembles A sont des sous-groupes du groupe G donné ?

1. $A = \mathbb{R}[x]_8, +$ (les polynômes de degré 8) et $\mathrm{G} = \mathbb{R}[x]_{\leq 8}, +$;
2. $A = 100\mathbb{Z}$ et $\mathrm{G} = 10\mathbb{Z}$;
3. $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}/100\mathbb{Z}$;

4. $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}$.

Éléments de réponse 162

$A = 100\mathbb{Z}$ est un sous-groupe de $\mathrm{G} = 10\mathbb{Z}$.

Remarque sur le 1. : $P = x^8 \in A$, $Q = -x^8 \in A$, $P + Q = 0 \notin A$.

Remarque sur le 3. : $\mathbb{Z}/10\mathbb{Z} \not\subseteq \mathbb{Z}/100\mathbb{Z}$.

Remarque sur le 4. : $\mathbb{Z}/10\mathbb{Z} \not\subseteq \mathbb{Z}$.

Exercice 163

Quels sont les éléments de $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$?

1. $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
2. $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
3. $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$;
4. $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$.

Éléments de réponse 163

1. $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$;
2. $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$

sont les éléments de $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$.

On dit que $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$ appelé inverse de a et noté a^{-1} tel que $ab = \overline{1}$. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$ où k est premier avec n. C'est une reformulation du théorème de Bézout ; en effet on a les équivalences suivantes :

$$\begin{aligned} &\text{Il existe } b \in \mathbb{Z} \text{ tel que } ab \equiv 1 \bmod n \\ &\quad \iff \text{il existe } b \in \mathbb{Z} \text{ et } k \in \mathbb{Z} \text{ tels que } ab = kn + 1 \\ &\quad a \text{ est premier avec } n \end{aligned}$$

Exercice 164

Pour quelles opérations parmi l'addition $+$ et la multiplication $\cdot$ l'ensemble suivant est-il un groupe ?

1. $\mathbb{Z}$;
2. $\mathbb{C}$;
3. $\mathbb{C}^*$;
4. $\mathbb{Z}/8\mathbb{Z}$;
5. $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$;

6. $\mathbb{Z}/7\mathbb{Z}$;
7. $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$;
8. $\{1, -1\}$.

Éléments de réponse 164

1. $\mathbb{Z}$, $+$;
2. $\mathbb{C}$, $+$;
3. $\mathbb{C}^*$, $\cdot$;
4. $\mathbb{Z}/8\mathbb{Z}$, $+$;
5. $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$, $\cdot$;
6. $\mathbb{Z}/7\mathbb{Z}$, $+$, $\cdot$;
7. $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$, $\cdot$;
8. $\{1, -1\}$, $\cdot$

sont des groupes.

Exercice 165

1. Quel est l'ordre de 0 dans $\mathbb{Z}$?
2. Quel est l'ordre de 1 dans $\mathbb{Z}$?
3. Quel est l'ordre de 2 dans $\mathbb{Z}$?
4. Quel est l'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$?
5. Quel est l'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$?
6. Quel est l'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?
7. Quel est l'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$?
8. Quel est l'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?

Éléments de réponse 165

1. L'ordre de 0 dans $\mathbb{Z}$ est : 1.
2. L'ordre de 1 dans $\mathbb{Z}$ est : ∞.
3. L'ordre de 2 dans $\mathbb{Z}$ est : ∞.
4. L'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$ est : 2.
5. L'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.

6. L'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 1.
7. L'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.
8. L'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 3.

Exercice 166

Compléter pour obtenir un énoncé correct : Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

1. k divise l'ordre de G ;
2. l'ordre de x divise k ;
3. k divise l'ordre de x.

Éléments de réponse 166

Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

2. l'ordre de x divise k.

Remarque sur l'assertion 1. : rappelons que $g^k = e$, $k \in \mathbb{N}^*$, si et seulement si l'ordre $o(g)$ de g divise k. Le théorème de Lagrange assure que $o(g) = |\langle g \rangle|$ divise $|\mathrm{G}|$. Si $k = o(g) + |\mathrm{G}|$, alors

$$g^k = g^{o(g)+|\mathrm{G}|} = g^{o(g)} g^{|\mathrm{G}|} = ee = e$$

mais $k = o(g) + |\mathrm{G}|$ ne divise pas $|\mathrm{G}|$.

Exercice 167

Compléter pour obtenir un énoncé correct : Soit G le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Soit $g = ([1]_4, [4]_6)$.

1. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6)\}$;
2. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6), ([1]_4, [2]_6), ([2]_4, [0]_6), ([3]_4, [4]_6), ([0]_4, [2]_6), ([1]_4, [0]_6), ([2]_4, [4]_6), ([3]_4, [2]_6), ([0]_4, [0]_6)\}$;
3. $\langle g \rangle = \mathrm{G}$.

Éléments de réponse 167

Soit G le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Soit $g = ([1]_4, [4]_6)$.

2. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6), ([1]_4, [2]_6), ([2]_4, [0]_6), ([3]_4, [4]_6), ([0]_4, [2]_6), ([1]_4,$

Exercice 168

Quelles sont les assertions correctes ?

1. Si G est un groupe abélien, alors G est cyclique.
2. Si G est un groupe cyclique, alors G est abélien.
3. Si G est d'ordre p, avec p un nombre premier, alors G est cyclique.

4. Si G est d'ordre fini et cyclique, alors G est d'ordre premier.

Éléments de réponse 168

Les assertions correctes sont :

2. Si G est un groupe cyclique, alors G est abélien ; en effet si G est cyclique, il existe $g \in \mathrm{G}$ tel que $\mathrm{G} = \langle g \rangle$. Soient a et b dans G, ils s'écrivent aussi g^ℓ et g^k, ℓ, $k \in \mathbb{Z}$ et
$$ab = g^\ell g^k = g^{\ell+k} = g^{k+\ell} = g^k g^\ell = ba.$$
3. Si G est d'ordre p, avec p un nombre premier, alors G est cyclique. En effet soit $g \in \mathrm{G} \setminus \{e\}$. Le théorème de Lagrange assure que l'ordre de g divise p. Puisque p est premier, l'ordre de g est p et g est un générateur de G.

Remarque sur le 1. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, c'est un groupe abélien, non cyclique.

Remarque sur le 4. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z}$, c'est un groupe d'ordre fini et cyclique mais 4 n'est pas premier.

Exercice 169

La décomposition de la permutation (1 2 3 4)(2 3)(1 4 3) de $\mathfrak{S}_4$ en cycles disjoints est :

1. (3 2 4) ;
2. id ;
3. (2 4 3)(1) ;
4. (1)(2)(3)(4).

Éléments de réponse 169

La décomposition de la permutation (1 2 3 4)(2 3)(1 4 3) de $\mathfrak{S}_4$ en cycles disjoints est :

1. (3 2 4) ;
3. (2 4 3)(1).

Exercice 170

L'ordre de l'élément (1 3)(2 4 5)(6 9 8 7) dans $\mathfrak{S}_{11}$ est

1. 9 ;
2. 11 ;
3. 12 ;
4. 24.

Éléments de réponse 170

L'ordre de l'élément (1 3)(2 4 5)(6 9 8 7) dans $\mathfrak{S}_{11}$ est 12. En effet l'élément (1 3)(2 4 5)(6 9 8 7) a pour décomposition en cycles à supports disjoints (1 3)(2 4 5)(6 9 8 7). De plus

$$o\big((1\ 3)\big) = 2 \qquad o\big((2\ 4\ 5)\big) = 3 \qquad o\big((6\ 9\ 8\ 7)\big) = 4$$

L'ordre de (1 3)(2 4 5)(6 9 8 7) est $\mathrm{ppcm}(2, 3, 4) = 12$.

Exercice 171

Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. Parmi les énoncés suivants lesquels sont vrais ?

1. Dans D_8 il y a 4 réflexions et 4 rotations ;
2. Dans D_8 il y a exactement 4 éléments d'ordre 2 ;
3. Dans D_8 il y a exactement 4 éléments d'ordre 4.

Éléments de réponse 171

Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. L'énoncé suivant est vrai :

1. Dans D_8 il y a 4 réflexions et 4 rotations.

Les autres assertions sont fausses. En effet id, r, r^2 et r^3 sont des rotations alors que s, sr, sr^2 et sr^3 sont des réflexions. Les éléments d'ordre 2 sont les réflexions et r^2. Les éléments d'ordre 4 sont r et r^3.

Exercice 172

Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Parmi les énoncés suivants lesquels sont corrects ?

1. $\mathrm{G} = \mathrm{D}_{10}$;
2. $\mathrm{G} = \mathrm{D}_5$;
3. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;
4. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement deux sommets de $\mathcal{P}$;
5. Dans G, il y a des éléments d'ordre 1, 2 et 5 ;
6. Dans G, il y a des éléments d'ordre 1, 2, 5 et 10.

Éléments de réponse 172

Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Les énoncés suivants sont corrects :

1. $\mathrm{G} = \mathrm{D}_{10}$;
3. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;

5. Dans G, il y a des éléments d'ordre 1, 2 et 5.

Exercice 173

Soit $(\mathrm{G}, *) = (\mathbb{Z}, +)$, $\mathrm{H} = 4\mathbb{Z}$ et $g = 3$. Alors $g * \mathrm{H}$ est égal à :

1. $3 + 4\mathbb{Z}$;
2. $12\mathbb{Z}$;
3. $\{\ldots, -1, 3, 7, 11, \ldots\}$;
4. $-5 * \mathrm{H}$.

Éléments de réponse 173

Soit $(\mathrm{G}, *) = (\mathbb{Z}, +)$, $\mathrm{H} = 4\mathbb{Z}$ et $g = 3$. Alors $g * \mathrm{H}$ est égal à :

1. $3 + 4\mathbb{Z}$;
3. $\{\ldots, -1, 3, 7, 11, \ldots\}$;
4. $-5 * \mathrm{H}$.

Exercice 174

Soient G un groupe et H un sous-groupe distingué de G. Parmi les énoncés suivants lesquels sont corrects ?

1. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$;
2. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $g^{-1}hg \in \mathrm{H}$;
3. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $hgh^{-1} \in \mathrm{H}$;
4. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $h^{-1}gh \in \mathrm{H}$.

Éléments de réponse 174

Soient G un groupe et H un sous-groupe distingué de G. Les énoncés suivants sont corrects :

1. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$;
2. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $g^{-1}hg \in \mathrm{H}$.

Exercice 175

Soient G un groupe et H un sous-groupe propre de G. Parmi les énoncés suivants lesquels sont corrects ?

1. En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.
2. Si H est distingué dans G, alors les classes à gauche dans G suivant H sont des sous-groupes de G ;
3. En général, il y a autant de classes à gauche que de classes à droite ;
4. Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;

5. Soit $g \in \mathrm{G}$. Si H est distingué dans G, alors $g\mathrm{H} = \mathrm{H}g$.

Éléments de réponse 175

Soient G un groupe et H un sous-groupe propre de G. Les énoncés suivants sont corrects :

1. En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.
3. En général, il y a autant de classes à gauche que de classes à droite ;
4. Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;
5. Soit $g \in \mathrm{G}$. Si H est distingué dans G, alors $g\mathrm{H} = \mathrm{H}g$.

Exercice 176

Soit G un groupe. Parmi les énoncés suivants lesquels sont corrects ?

1. Si G n'est pas abélien, alors G a au moins un sous-groupe propre (*i.e.* distinct de $\{e_\mathrm{G}\}$ et de G) qui n'est pas distingué dans G ;
2. Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ;
3. Si G est abélien et H est un sous-groupe propre de G, alors G/H est abélien ;
4. Si G n'est pas abélien et H est un sous-groupe distingué propre de G, alors G/H n'est pas abélien ;
5. Si G est cyclique et H est un sous-groupe de G, alors G/H est cyclique ;
6. Si G n'est pas cyclique et H est un sous-groupe de G, alors G/H n'est pas cyclique.

Éléments de réponse 176

Soit G un groupe. Les énoncés suivants sont corrects :

2. Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ; cela découle de la définition de sous-groupe distingué.
3. Si G est abélien et H est un sous-groupe propre de G, alors G/H est abélien ; En effet soient $g_1\mathrm{H}$ et $g_2\mathrm{H}$ deux éléments de G/H, alors

$$\begin{aligned} g_1\mathrm{H} \cdot g_2\mathrm{H} &= g_1g_2\mathrm{H} \text{ (définition de cette opération)} \\ &= g_2g_1\mathrm{H} \text{ (car G est abélien)} \\ &= g_2\mathrm{H} \cdot g_1\mathrm{H} \text{ (définition de cette opération)} \end{aligned}$$

5. Si G est cyclique et H est un sous-groupe de G, alors G/H est cyclique. En effet soit x un générateur de G. Soit $g\mathrm{H}$ un élément de G/H. Il existe $k \in \mathbb{Z}$ tel que $g = x^k$ donc $g\mathrm{H} = x^k\mathrm{H} = (x\mathrm{H})^k$. Ainsi $x\mathrm{H}$ est un générateur de G/H.

L'assertion 1. est fausse. Le groupe des quaternions $\mathbb{H}_8$ n'est pas abélien et n'a pas de sous-groupe propre qui n'est pas distingué.

L'assertion 4. est fausse. Considérons par exemple les groupes $\mathrm{G} = \mathrm{D}_8$ et $\mathrm{H} = \langle r \rangle$, alors $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$ et donc G/H est abélien.

L'assertion 6. est fausse. Considérons par exemple les groupes $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{H} = \langle(\overline{1}, \overline{0})\rangle$. Le groupe G n'est pas cyclique mais $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$ est cyclique.

Exercice 177

Soient G un groupe et H un sous-groupe de G. Parmi les énoncés suivants lesquels sont corrects ?

1. Si l'ordre de G est infini, alors le nombre de classes à gauche dans G suivant H est infini ;
2. Si l'ordre de G est infini et l'ordre de H est infini, alors le nombre de classes à gauche dans G suivant H est infini ;
3. Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini ;
4. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de H ;
5. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G.

Éléments de réponse 177

Soient G un groupe et H un sous-groupe de G. Les énoncés suivants sont corrects :

3. Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini. En effet les classes à gauche forment une partition de G. Toute classe à gauche suivant H est en bijection avec H. S'il n'y avait qu'un nombre fini de classes à gauche suivant H, alors G serait fini.
5. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G. Cela découle du théorème de Lagrange.

L'assertion 1. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

L'assertion 2. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

Exercice 178

Pour l'action $\cdot$ donnée du groupe G sur l'ensemble A, déterminer :

1. l'élément $\overline{1} \cdot \overline{3}$ si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation ;

2. l'élément $\overline{5} \cdot \overline{1}$ si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation ;
3. l'élément $(1\ 2) \cdot 2$ si $\cdot$ est l'action triviale de $\mathrm{G} = \mathfrak{S}_3$ sur $A = \{1, 2, 3, 4\}$;
4. l'élément $(1\ 2) \cdot (3\ 4)$ si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathfrak{S}_4$ sur lui-même ($A = \mathrm{G}$).

Éléments de réponse 178

1. Si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{1} \cdot \overline{3}$ est $\overline{1} + \overline{3} = \overline{4}$;
2. si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{5} \cdot \overline{1}$ est $\overline{5}$;
3. si $\cdot$ est l'action triviale de $\mathrm{G} = \mathfrak{S}_3$ sur $A = \{1, 2, 3, 4\}$, alors l'élément $(1\ 2) \cdot 2$ est 2 ;
4. si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathfrak{S}_4$ sur lui-même ($A = \mathrm{G}$) l'élément $(1\ 2) \cdot (3\ 4)$ est
$$(1\ 2) \circ (3\ 4) \circ (1\ 2)^{-1} = (3\ 4).$$

Exercice 179

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. L'élément $g \cdot a$ à quel ensemble appartient-il ?
2. Si $g = e_{\mathrm{G}}$, alors que vaut $g \cdot a$?
3. Est-ce que l'orbite de a est un sous-ensemble de A ou de G ?
4. Est-ce que le stabilisateur de a est un sous-ensemble de A ou de G ?
5. De quel ensemble est-ce que le noyau de l'action est un sous-groupe ?

Éléments de réponse 179

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. L'élément $g \cdot a$ appartient à A.
2. Si $g = e_{\mathrm{G}}$, alors $g \cdot a = a$.
3. L'orbite de a est un sous-ensemble de A.
4. Le stabilisateur de a est un sous-ensemble de G ?
5. Le noyau de l'action est un sous-groupe de G.

Exercice 180

Soit G un groupe.

1. Supposons que G agisse sur un ensemble X. Montrer que les orbites de l'action de G sur X forment une partition de X.

2. Supposons que G agisse sur lui-même par translation à gauche.

   i) Décrire les orbites des éléments de G sous cette action.

   ii) Décrire les stabilisateurs des éléments de G sous cette action.

3. Supposons que G agisse sur lui-même par conjugaison.

   i) Décrire les orbites des éléments de G sous cette action.

   ii) Décrire les stabilisateurs des éléments de G sous cette action.

Éléments de réponse 180

Soit G un groupe agissant sur un ensemble X.

1. Les orbites de l'action de G sur X forment une partition de X car la relation

$$x\mathcal{R}y \quad \Leftrightarrow \quad \exists\, g \in \mathrm{G},\, y = g \cdot x$$

   est une relation d'équivalence (associée à l'action).

2. Supposons que G agisse sur lui-même (c'est-à-dire $X = \mathrm{G}$) par translation à gauche :

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, h) \mapsto g \cdot h = gh.$$

   i) Décrivons les orbites des éléments de G sous cette action.

   Il n'y a qu'une seule orbite. En effet si x et y sont dans G alors $y = (yx^{-1})x = (yx^{-1}) \cdot x$.

   ii) Décrivons les stabilisateurs des éléments de G sous cette action.

   La relation $x = g \cdot x$, c'est-à-dire $x = gx$ implique $g = e$: le stabilisateur de tout élément est réduit au neutre.

3. Supposons que G agisse sur lui-même (c'est-à-dire $X = \mathrm{G}$) par conjugaison :

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, h) \mapsto g \cdot h = ghg^{-1}.$$

   i) Décrivons les orbites des éléments de G sous cette action.

   L'orbite de x est

$$\begin{aligned} \mathcal{O}_x &= \{g \cdot x \,|\, g \in \mathrm{G}\} \\ &= \{gxg^{-1} \,|\, g \in \mathrm{G}\}; \end{aligned}$$

   autrement dit l'orbite de $x \in \mathrm{G}$ sous l'action de G est la classe de conjugaison de $x \in \mathrm{G}$.

ii) Décrivons les stabilisateurs des éléments de G sous cette action.

Le stabilisateur de x est

$$\begin{aligned} \mathrm{St}(x) &= \{g \in \mathrm{G} \,|\, g \cdot x = x\} \\ &= \{g \in \mathrm{G} \,|\, gxg^{-1} = x\} \\ &= \{g \in \mathrm{G} \,|\, gx = xg\} \end{aligned}$$

Autrement dit le stabilisateur de x sous l'action de G est le centralisateur de x dans G.

Exercice 181

Soit $\mathrm{SL}(2,\mathbb{R})$ le groupe des matrices 2×2 à coefficients réels et de déterminant égal à 1 :

$$\mathrm{SL}(2,\mathbb{R}) = \{M \in \mathrm{GL}(2,\mathbb{R}) \,|\, \det M = 1\}.$$

Rappelons que le demi-plan de Poincaré $\mathbb{H}$ est l'ensemble des complexes de partie imaginaire strictement positive :

$$\mathbb{H} = \{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}.$$

1. À $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ et $z \in \mathbb{H}$, on peut associer :

$$h \cdot z = \frac{az+b}{cz+d};$$

montrer que ceci définit une action de $\mathrm{SL}(2,\mathbb{R})$ sur $\mathbb{H}$.

2. Que signifie « l'action d'un groupe G sur un ensemble X est fidèle » ? L'action de $\mathrm{SL}(2,\mathbb{R})$ sur $\mathbb{H}$ est-elle fidèle ?
3. Donner la définition du stabilisateur de **i** sous l'action de $\mathrm{SL}(2,\mathbb{R})$. Déterminer le stabilisateur de **i** sous l'action de $\mathrm{SL}(2,\mathbb{R})$.
4. Donner la définition de l'orbite de **i** sous l'action de $\mathrm{SL}(2,\mathbb{R})$. Montrer que l'orbite de **i** sous l'action de $\mathrm{SL}(2,\mathbb{R})$ est $\mathbb{H}$.
5. Que signifie « l'action d'un groupe G sur un ensemble X est transitive » ? L'action est-elle transitive ?

Éléments de réponse 181

1. Montrons que $\mathrm{SL}(2,\mathbb{R})$ opère sur $\mathbb{H}$.

Soit h la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; alors

$$h \cdot z = \frac{az+b}{cz+d} = \frac{ac|z|^2 + (bc\overline{z} + adz) + bd}{|cz+d|^2}$$

La partie imaginaire de $h \cdot z$ est donc

$$\frac{(ad-bc)\mathrm{Im}\, z}{|bz+d|^2}$$

Puisque par hypothèse le déterminant de h est 1, tout complexe de partie imaginaire strictement positive a pour image un complexe de partie imaginaire strictement positive.

De plus

- ◇ d'une part pour tous h, h' dans $\mathrm{SL}(2,\mathbb{R})$ et tout z dans $\mathbb{H}$ nous avons

$$h \cdot (h' \cdot z) = \frac{a\frac{a'z+c'}{b'z+d'} + c}{b\frac{a'z+c'}{b'z+d'} + d} = \frac{(aa'+cb')z + ac' + cd'}{(a'b+db')z + bc' + dd'} = (hh') \cdot z$$

- ◇ d'autre part pour tout z dans $\mathbb{H}$ nous avons

$$\mathrm{id} \cdot z = \frac{1 \times z + 0}{0 \times z + 1} = z$$

2. Le groupe G *opère fidèlement* sur l'ensemble X si $\varphi\colon \mathrm{G} \to \mathfrak{S}(X)$ est injectif, *i.e.* si $g \cdot x = x$ pour tout $x \in X$ implique $g = 1$. L'action de $\mathrm{SL}(2,\mathbb{R})$ n'est pas fidèle : $-\mathrm{id}\}$ appartient à $\ker \varphi$.

3. Le stabilisateur de $\mathbf{i}$ sous l'action de $\mathrm{SL}(2,\mathbb{R})$ est :

$$\{h \in \mathrm{SL}(2,\mathbb{R}) \,|\, h \cdot \mathbf{i} = \mathbf{i}\}.$$

Or

$$\begin{aligned} h \cdot \mathbf{i} = \mathbf{i} \quad &\Longleftrightarrow \quad \frac{a\mathbf{i}+b}{c\mathbf{i}+d} = \mathbf{i} \quad \Longleftrightarrow \quad a\mathbf{i}+b = \mathbf{i}(c\mathbf{i}+d) \quad \Longleftrightarrow \quad a\mathbf{i}+b = -c+d\mathbf{i}. \\ &\Longleftrightarrow \quad (a-d)\mathbf{i} + (b+c) = 0 \quad \Longleftrightarrow \quad a = d \text{ et } b = -c. \end{aligned}$$

Comme le déterminant est égal à 1 le stabilisateur de $\mathbf{i}$ sous l'action de $\mathrm{SL}(2,\mathbb{R})$ est l'ensemble des matrices orthogonales directes.

4. L'orbite de $\mathbf{i} \in \mathbb{H}$ sous l'action de $\mathrm{SL}(2,\mathbb{R})$ est notée $\mathcal{O}_{\mathbf{i}}$:

$$\mathcal{O}_{\mathbf{i}} = \{g \cdot \mathbf{i} \,|\, g \in \mathrm{SL}(2,\mathbb{R})\};$$

L'orbite de $\mathbf{i}$ est le demi-plan de Poincaré tout entier. En effet, le complexe $x + \mathbf{i}y$ où x est réel et y est réel strictement positif est l'image de $\mathbf{i}$ par $h = \begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix}$:

$$\begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix} \cdot \mathbf{i} = \frac{\sqrt{y}\mathbf{i} + \frac{x}{\sqrt{y}}}{\frac{1}{\sqrt{y}}} = \sqrt{y}\left(\sqrt{y}\mathbf{i} + \frac{x}{\sqrt{y}}\right) = y\mathbf{i} + x.$$

5. Le groupe G *opère transitivement* sur l'ensemble X si

$$\forall\, x \in X,\ \forall\, y \in X,\ \exists\, g \in \mathrm{G},\ g \cdot x = y.$$

L'orbite de $\mathbf{i}$ étant $\mathbb{H}$, l'action est transitive. En effet, soient x et y dans $\mathbb{H}$. Puisque $\mathcal{O}_{\mathbf{i}} = \mathbb{H}$ il existe g_1, g_2 dans $\mathrm{SL}(2,\mathbb{R})$ tels que $g_1 \cdot \mathbf{i} = x$ et $g_2 \cdot \mathbf{i} = y$; alors $(g_1 g_2^{-1}) \cdot y = x$.

Exercice 182

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$. Les assertions suivantes sont-elles vraies ou fausses ?

1. Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$;
2. Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$;
3. L'orbite de a est un groupe ;
4. Le stabilisateur de g est un groupe ;
5. Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ;
6. L'action est transitive si et seulement s'il n'y a qu'une seule orbite ;
7. Le stabilisateur de g est un sous-groupe distingué de G.

Éléments de réponse 182

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$; faux : écrire a^{-1} n'a pas de sens.
2. Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$; vrai : si $g \cdot a = b$, alors $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot b$ soit $(g^{-1} g) \cdot a = g^{-1} \cdot b$ ou encore $a = g^{-1} b$.
3. L'orbite de a est un groupe ; faux : les orbites forment une partition de A, ce sont des ensembles sans structure.
4. Le stabilisateur de g est un groupe ; vrai.
5. Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ; vrai.
6. L'action est transitive si et seulement s'il n'y a qu'une seule orbite ; vrai.
7. Le stabilisateur de g est un sous-groupe distingué de G ; faux.

Exercice 183

Soit G un groupe. Soient a, b deux éléments de G d'ordre fini. Le groupe engendré par a et b est-il fini ?

Éléments de réponse 183

Non (considérer par exemple le groupe G des permutations de $\mathbb{Z}$ engendré par $f(x) = -x$ et $g(x) = 1 - x$. Alors $f \circ f = \mathrm{id}$, $g \circ g = \mathrm{id}$ mais $f \circ g \colon x \mapsto x - 1$ donc $(f \circ g)^n \colon x \mapsto x - n$. Le groupe G contient donc tous les éléments de la forme $x \mapsto x - n$ avec n dans $\mathbb{Z}$. En particulier il est infini.

Exercice 184

Dans le lemme chinois expliciter rapidement comment on construit l'isomorphisme.

Éléments de réponse 184 **Lemme chinois.** *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Soit $\overline{n}$, respectivement $\widehat{n}$, respectivement $\overline{n}$ la classe de n modulo pq, respectivement p, respectivement q. Considérons le morphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \overline{n})$$

Il est injectif car $\text{pgcd}(p,q) = 1$. On conclut grâce à l'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$.

Exercice 185

Donner un exemple de groupe fini simple.

Éléments de réponse 185

Le groupe des permutations $\mathcal{A}_n$ dès que $n \geq 5$.

Exercice 186

Soit G un groupe. Les applications suivantes de G dans G sont-elles toujours des morphismes ?

a) $x \mapsto ax$, où $a \in \text{G}$ est fixé.

b) $x \mapsto x^n$ pour $n \in \mathbb{N}^*$.

c) $x \mapsto x^{-1}$.

Éléments de réponse 186

Exercice 187

Soit $\Bbbk$ un corps. Soit A une partie de $M(n, \Bbbk)$ telle que A soit un groupe pour la multiplication des matrices. A est-elle toujours un sous-groupe de $\text{GL}(n, \Bbbk)$?

Éléments de réponse 187

Exercice 188

Soit $(\text{A}, +)$ un groupe abélien.

a) Soit $n > 0$. Montrer que l'ensemble $A[n] = \{x \in \text{A},\ nx = 0\}$ est un sous-groupe de A, appelé sous-groupe de n-torsion de A.

b) Montrer que $\text{A}_{\text{tors}} := \bigcup_{n>0} A[n]$ est un sous-groupe de A, appelé sous-groupe de torsion de A.

c) Quel est le cardinal de A_{tors} lorsque $\text{A} = \mathbb{R}$? Lorsque $A = \Bbbk$, où $\Bbbk$ est un corps commutatif quelconque ?

Éléments de réponse 188

Exercice 189

Soit G un groupe. Soit H un sous-groupe de G. Montrer que $aH \mapsto Ha$ est une bijection de l'ensemble G/H des classes à gauche sur l'ensemble $H \backslash G$ des classes à droite. Le cardinal de ces ensembles, s'il est fini, se note [G : H] et s'appelle l'indice de H dans G (c'est aussi l'ordre du groupe G/H si H est distingué dans G).

Éléments de réponse 189

Exercice 190

Soient H et N deux groupes. On dit qu'un groupe E est une extension de H par N s'il existe un morphisme surjectif $E \to H$ dont le noyau est isomorphe à N. Montrer que les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ sont tous deux des extensions de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 190

1.5. Seconds pas

Exercice 191

Soit G un groupe fini d'ordre pair et de neutre e. Montrer qu'il existe un élément x d'ordre 2.

Éléments de réponse 191

Remarquons qu'un élément x est d'ordre 2 si et seulement si $x \neq e$ et $x^2 = e$ c'est-à-dire si et seulement si $x \neq e$ et $x = x^{-1}$. Pour tout $x \in G$ on note $[x] = \{x, x^{-1}\}$. Nous avons $[e] = \{e\}$ et pour $x \neq e$ $|[x]| = 1$ si et seulement si x est d'ordre 2. Le groupe G est réunion disjointe d'ensembles de la forme $[x]$: il existe $x_0 = e$, x_1, …, x_r tels que

$$G = [x_0] \sqcup [x_1] \sqcup [x_2] \sqcup \ldots \sqcup [x_r]$$

Par conséquent $|G| = |[e]| + \sum_{i=1}^{r} |[x_i]|$. Si tous les éléments de G différents de e étaient d'ordre différent de 2 nous aurions $|[x_i]| = 2$ pour tout $1 \leq i \leq r$ et $|G|$ serait impair : contradiction. Il en résulte que G a au moins un élément d'ordre 2.

Exercice 192

Soit $G = \{a + b\sqrt{2} \,|\, a \in \mathbb{Q}, b \in \mathbb{Q}\} \subset \mathbb{R}$.

1. Montrer que G est un groupe pour l'addition.
2. Montrer que l'ensemble des éléments non nuls de G est un groupe pour la multiplication.

Éléments de réponse 192

Soit $G = \{a + b\sqrt{2} \,|\, a \in \mathbb{Q}, b \in \mathbb{Q}\} \subset \mathbb{R}$.

1. Montrons que G est un groupe pour l'addition. Il suffit de montrer que G est un sous-groupe du groupe additif $\mathbb{R}$. Or on a
$$(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2}.$$
2. Montrons que l'ensemble des éléments non nuls de G est un groupe pour la multiplication. Il suffit de montrer que $\mathrm{G} \setminus \{0\}$ est un sous-groupe du groupe multiplicatif $\mathbb{R}^*$. Introduisons la quantité conjuguée $a' - b'\sqrt{2}$ de $a' + b'\sqrt{2}$. En multipliant numérateur et dénominateur par la quantité conjuguée nous obtenons
$$\frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} = \frac{(a + b\sqrt{2})(a' + b'\sqrt{2})}{a'^2 - 2b'^2} = \frac{aa' - 2bb' + (ab' + a'b)\sqrt{2}}{a'^2 - 2b'^2}$$
Ainsi $\mathrm{G} \setminus \{0\}$ est bien un sous-groupe du groupe multiplicatif $\mathbb{R}^*$.

Exercice 193

Soit G un groupe. Soient H et K deux sous-groupes de G.

Montrer que $\mathrm{H} \cup \mathrm{K}$ est un sous-groupe de G si et seulement si $\mathrm{H} \subset \mathrm{K}$ ou $\mathrm{K} \subset \mathrm{H}$.

En déduire qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.

Éléments de réponse 193

Soit G un groupe. Soient H et K deux sous-groupes de G.

Montrons que $\mathrm{H} \cup \mathrm{K}$ est un sous-groupe de G si et seulement si $\mathrm{H} \subset \mathrm{K}$ ou $\mathrm{K} \subset \mathrm{H}$.

Si $\mathrm{K} \subset \mathrm{H}$ alors $\mathrm{H} \cup \mathrm{K} = \mathrm{H}$ et $\mathrm{H} \cup \mathrm{K}$ est donc un sous-groupe de G (de même $\mathrm{H} \subset \mathrm{K}$ alors $\mathrm{H} \cup \mathrm{K} = \mathrm{K}$ et $\mathrm{H} \cup \mathrm{K}$ est donc un sous-groupe de G).

Réciproquement si $\mathrm{H} \cup \mathrm{K}$ est un sous-groupe de G et si H n'est pas inclus dans K il existe $h \in \mathrm{H}$ tel que $h \notin \mathrm{K}$, en particulier h n'est pas l'élément neutre. Alors pour tout $k \in \mathrm{K}$ nous avons $hk \in \mathrm{H} \cup \mathrm{K}$ (car $\mathrm{H} \cup \mathrm{K}$ est un sous-groupe de G) ; ainsi pour tout $k \in \mathrm{K}$ nous avons l'alternative : hk appartient à H ou hk appartient à K. Si hk appartient à K, alors puisque K est un sous-groupe de G nous avons $h = (hk)k^{-1}$ appartient à K : contradiction avec l'hypothèse. Par conséquent hk appartient à H ; comme H est un sous-groupe de G nous avons : $k = h^{-1}(hk)$ appartient à H. Il en résulte que $\mathrm{K} \subset \mathrm{H}$.

Montrons qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.

Raisonnons par l'absurde : supposons que G soit la réunion de deux de ses sous-groupes propres H et K, *i.e.* $\mathrm{K} \cup \mathrm{H} = \mathrm{G}$; alors

- ◇ ou bien $\mathrm{H} \subset \mathrm{K}$ et $\mathrm{H} \cup \mathrm{K} = \mathrm{G}$ donc $\mathrm{H} \cup \mathrm{K} = \mathrm{G}$ équivaut à $\mathrm{K} = \mathrm{G}$: contradiction avec l'hypothèse K propre ;
- ◇ ou bien $\mathrm{K} \subset \mathrm{H}$ et $\mathrm{H} \cup \mathrm{K} = \mathrm{G}$ donc $\mathrm{H} \cup \mathrm{K} = \mathrm{G}$ équivaut à $\mathrm{H} = \mathrm{G}$: contradiction avec l'hypothèse H propre.

Exercice 194

On dit qu'un élément g d'un groupe G est indéfiniment divisible si pour tout $n \in \mathbb{N}^*$ il existe un élément h de G tel que $h^n = g$.

1. Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q},+)$? Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*,\times)$?
2. Soit $\varphi\colon (\mathbb{Q},+)\to(\mathbb{Q}_+^*,\times)$ un morphisme de groupes.

   Pour tout entier $n>0$ calculer $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$.
3. Montrer que φ est constant.
4. En déduire que $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$ ne sont pas isomorphes.

Remarque : par contre $(\mathbb{R},+)$ et $(\mathbb{R}_+^*,\times)$ sont isomorphes ; la fonction $x\mapsto \exp x$ réalise un isomorphisme entre ces deux groupes.

Éléments de réponse 194

1. Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q},+)$.

   Soit $x\in\mathbb{Q}$. Cet élément est indéfiniment divisible pour la loi d'addition car pour tout entier naturel n non nul nous avons $n\times\frac{x}{n}=x$. Autrement dit tous les éléments de $\mathbb{Q}$ sont indéfiniment divisibles pour l'addition.

   Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*,\times)$.

   Soit $x\in\mathbb{Q}^*$ indéfiniment divisible. Alors pour tout $n\in\mathbb{N}^*$ $x^{1/n}$ existe et appartient à $\mathbb{Q}_+^*$. Il en résulte que $x=1$.
2. Soit $\varphi\colon (\mathbb{Q},+)\to(\mathbb{Q}_+^*,\times)$ un morphisme de groupes.

   Pour tout entier $n>0$ calculons $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$. Pour tout entier $n>0$ nous avons

   $$\varphi(n)=\varphi(1+1+\ldots+1)=\varphi(1)^n.$$

   Pour tout entier $n>0$ nous avons

   $$\varphi(1)=\varphi\left(n\times\frac{1}{n}\right)=\varphi\left(\frac{1}{n}+\frac{1}{n}+\ldots+\frac{1}{n}\right)=\varphi\left(\frac{1}{n}\right)^n$$

   d'où $\varphi\left(\frac{1}{n}\right)=\varphi(1)^{1/n}$.
3. Montrons que φ est constant.

   Pour tout $n>0$ il existe $h=\varphi\left(\frac{1}{n}\right)$ tel que $h^n=\varphi(1)$. Ainsi $\varphi(1)$ est indéfiniment divisible pour la multiplication. D'après ce qui précède nous avons donc $\varphi(1)=1$.

   Ainsi pour tout n, nous avons $\varphi(n)=1$ et $\varphi\left(\frac{1}{n}\right)=1$. De plus pour tout rationnel $\frac{p}{q}$ nous avons $\varphi\left(\frac{p}{q}\right)=\left(\varphi\left(\frac{1}{q}\right)\right)^p=1$. Le morphisme φ est donc constant.
4. Montrons $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$ ne sont pas isomorphes.

   Raisonnons par l'absurde : supposons qu'il existe un isomorphisme ψ entre $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$. En particulier ψ est un morphisme entre ces deux groupes. D'après ce qui précède ψ est donc constant ce qui n'est pas possible pour un isomorphisme.

Exercice 195

Soit G un groupe fini. Montrer que, pour tout g et tout h dans G

1. g et g^{-1} ont même ordre ;
2. g et hgh^{-1} ont même ordre ;
3. gh et hg ont même ordre.

Éléments de réponse 195

Soit G un groupe fini.

1. Soit g dans G. Montrons que g et g^{-1} ont même ordre.

   Soit $g \in$ G. Notons k l'ordre de g et ℓ l'ordre de g^{-1}. D'une part $(g^{-1})^k = e$ donc ℓ divise k. D'autre part $g^\ell = e$ donc k divise ℓ. Finalement $k = \ell$.

2. Montrons que, pour tout g et tout h du groupe G les éléments g et hgh^{-1} ont même ordre.

   Notons k l'ordre de g et ℓ l'ordre de hgh^{-1}.

   On vérifie que $(hgh^{-1})^k = e$ donc ℓ divise k.

   Par ailleurs $h^{-1}(hgh^{-1})h$ a pour ordre k et $\left(h^{-1}(hgh^{-1})h\right)^\ell = e$ donc k divise ℓ.

   Il s'en suit que $k = \ell$.

3. Montrons que, pour tout g et tout h du groupe G, les éléments gh et hg ont même ordre.

   Désignons par k l'ordre de gh et par ℓ l'ordre de hg. Remarquons que $hg = h(gh)h^{-1}$. D'après 2. $h(gh)h^{-1}$ et gh ont même ordre donc hg et gh ont même ordre.

Exercice 196

Soit G un groupe abélien.

Montrer que les éléments d'ordre fini de G forment un sous-groupe de G.

Éléments de réponse 196

Soit G un groupe abélien. Soit H l'ensemble des éléments d'ordre fini. Puisque G est abélien, si $g \in$ H et $h \in$ H, alors gh appartient à H ; en effet $(gh)^k = g^k h^k$ et donc l'ordre de gh divise le produit des ordres de g et h.

Soit $g \in$ H. Notons k l'ordre de g et ℓ l'ordre de g^{-1}. D'une part $(g^{-1})^k = e$ donc ℓ divise k. D'autre part $g^\ell = e$ donc k divise ℓ. Finalement $k = \ell$.

L'élément e est d'ordre fini donc dans H.

Ainsi H est un sous-groupe de G.

Exercice 197

Soit G un groupe possédant un seul élément d'ordre 2. Notons le g.

Montrer que g est dans le centre de G.

Éléments de réponse 197

Soit h un élément quelconque de G. Nous avons

$$(h^{-1}gh)(h^{-1}gh) = h^{-1}g(hh^{-1})gh = h^{-1}g^2h = h^{-1}h = e.$$

Or g est l'unique élément d'ordre 2 de G donc :

- ou bien $h^{-1}gh = e$ soit $g = e$: contradiction ;
- ou bien $h^{-1}gh = g$ soit $gh = hg$.

Il en résulte que g commute avec tous les éléments de G ; c'est-à-dire $g \in Z(\mathrm{G})$.

Exercice 198

Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Montrer que pour tout élément g de G il existe un élément h de G tel que $g = h^n$.

(Indication : considérer l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(h) = h^n$ et montrer que φ est un isomorphisme de G).

Éléments de réponse 198

Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Considérons l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(g) = g^n$.

Montrons que φ est un isomorphisme.

Tout d'abord c'est un morphisme ; en effet G est abélien donc $(gh)^n = g^n h^n$, *i.e.* $\varphi(gh) = \varphi(g)\varphi(h)$.

Le noyau $\ker\varphi$ de φ est constitué des éléments g de G tels que $g^n = e$. Donc non seulement n est premier avec k mais n est divisible par l'ordre de g qui divise k par suite $n = 1$ ou $g = e$. Pour $n > 1$ nécessairement $\ker\varphi = \{e\}$. Il en résulte que φ est une injection d'un ensemble fini dans lui-même, c'est donc un morphisme bijectif de groupes et donc un isomorphisme.

Il s'en suit que φ est surjective, *i.e.* pour tout élément g de G il existe $h \in \mathrm{G}$ tel que $\varphi(h) = g$ soit tel que $h^n = g$.

Exercice 199

Montrer de la façon la plus élémentaire possible que tout groupe d'ordre 4 est abélien (Indication : utiliser le théorème de Lagrange).

Éléments de réponse 199

Soit G un groupe d'ordre 4.

D'après le théorème de Lagrange tout élément non trivial de G est d'ordre 2 ou 4.

Si G admet un élément d'ordre 4, alors il est cyclique donc abélien (car isomorphe à $\mathbb{Z}/4\mathbb{Z}$).

Supposons que $\mathrm{G} \setminus \{e\}$ est constitué d'éléments d'ordre 2. Montrons que G est abélien. Soient a et b dans G.

$\diamond$ Si $ab = 1$, alors $a^{-1} = b$ et

- ou bien $a = 1$ et $a^{-1} = b$ conduit à $b = 1$ auquel cas a et b commutent ;

- ou bien $a \neq 1$, alors a est, par hypothèse, d'ordre 2 ; par suite $a = a^{-1}$ et $a^{-1} = b$ se réecrit $a = b$ auquel cas a et b commutent.

◇ Sinon ab est un élément de $\mathrm{G} \setminus \{e\}$ donc lui aussi d'ordre 2, *i.e.* $(ab)^2 = 1$ soit $abab = 1$ ou encore $ab = b^{-1}a^{-1}$. Mais $a = a^{-1}$ (que a soit 1 ou d'ordre 2) et $b = b^{-1}$ (que b soit 1 ou d'ordre 2 ; par conséquent $ab = b^{-1}a^{-1}$ se réécrit $ab = ba$: les éléments a et b commutent.

Exercice 200

Montrer qu'un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 200

Dans un groupe d'ordre 4 tous les éléments exceptés le neutre sont d'ordre 2 ou 4.
Si G contient un élément d'ordre 4, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
Sinon il n'y a que des éléments d'ordre 2 et G est isomorphe à $(\mathbb{Z}/4\mathbb{Z})^2$. (1)

Exercice 201

1. Montrer qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2, \mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.
2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Déterminer l'ordre de A, l'ordre de B et l'ordre de AB.

Éléments de réponse 201

1. Montrons qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2, \mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.

   Le déterminant d'une matrice à coefficients entiers est entier. Soit A une matrice à coefficents dans $\mathbb{Z}$; supposons que A soit inversible et que son inverse soit aussi à coefficients entiers. Nous avons $\det(AA^{-1}) = \det A(\det A)^{-1} = 1$. Par suite $\det A$ est inversible dans $\mathbb{Z}$ et est égal à ± 1.

---

1. Montrons qu'un groupe G où chaque élément est son propre inverse est abélien. Si tout élément de G est son propre inverse, alors pour tout couple (a, b) d'éléments de G nous avons $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Par conséquent G est abélien.

Montrons qu'on peut munir G d'une structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$. Pour définir une structure d'espace vectoriel sur G (qui est déjà muni d'une structure de groupe abélien) il faut définir la loi externe et la seule définition possible est

$$[0]_a = [0], \qquad [1]_a = a.$$

Les quatre conditions pour que cette loi externe soit celle d'un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ sont vérifiées.

En déduire que, si G est d'ordre fini, l'ordre de G est une puissance de 2. Puisque G est d'ordre fini, c'est un espace vectoriel de dimension finie sur $\mathbb{Z}/2\mathbb{Z}$, soit n. Il en résulte que G est isomorphe en tant qu'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ à $(\mathbb{Z}/2\mathbb{Z})^n$ et l'ordre de G est 2^n.

Réciproquement soit A une matrice carrée de taille $n \times n$ à coefficients dans $\mathbb{Z}$ de déterminant égal à ± 1. En tant que matrice à coefficients réels A est inversible et son inverse a pour coefficients les quotients des mineurs de taille $(n-1) \times (n-1)$ et de $\det A = \pm 1$. Ces mineurs sont des entiers, donc ces quotients sont des entiers et l'inverse de A est à coefficients dans $\mathbb{Z}$.

2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'ordre de A est 4, l'ordre de B est 3, l'ordre de $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est infini car $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Exercice 202

Montrer que $C_n = \left\{ \exp\left(\frac{2\mathbf{i}\pi k}{n}\right), | \, k \in \mathbb{Z} \right\}$ est un groupe cyclique d'ordre n pour la multiplication des nombres complexes.

Éléments de réponse 202

Montrons que $C_n = \left\{ \exp\left(\frac{2\mathbf{i}\pi k}{n}\right), | \, k \in \mathbb{Z} \right\}$ est un groupe cyclique d'ordre n pour la multiplication des nombres complexes.

Si $k = \ell \pmod n$, alors $\exp\left(\frac{2\mathbf{i}\pi k}{n}\right) = \exp\left(\frac{2\mathbf{i}\pi \ell}{n}\right)$. On peut donc définir l'application φ de $\mathbb{Z}/n\mathbb{Z}$ dans C_n par $\varphi([k]) = \exp\left(\frac{2\mathbf{i}\pi k}{n}\right)$. C'est un morphisme de groupes. De plus $\ker \varphi = \{[0]\}$ et $\mathbb{Z}/n\mathbb{Z}$ et C_n ont même ordre. Il en résulte que φ est un isomorphisme de groupes.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant cyclique C_n est aussi un groupe cyclique.

Exercice 203

Soit p un nombre premier. Montrer qu'à isomorphisme près il y a un seul groupe d'ordre p.

Éléments de réponse 203

Soit p un nombre premier. Soit G un groupe d'ordre p. Remarquons que G n'est pas réduit à $\{e\}$ puisque $p \geq 2$. Soit g un élément de $\mathrm{G} \setminus \{e\}$; il est nécessairement d'ordre p. Le groupe G est donc cyclique. Comme il est d'ordre p, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 204

Soit G un groupe d'ordre $n > 2$. Montrer qu'il n'existe aucun sous-groupe de G d'ordre $n-1$.

Éléments de réponse 204

Soit G un groupe d'ordre $n > 2$. Montrons qu'il n'existe aucun sous-groupe de G d'ordre $n-1$.

Si $n > 2$, alors $\mathrm{pgcd}(n, n-1) = 1$ donc aucun sous-groupe ne peut avoir pour ordre $n-1$ qui sinon diviserait n.

Exercice 205

1. Montrer que l'ordre de 1 dans $\mathbb{Z}/n\mathbb{Z}$ vaut n.
2. Montrer que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ vaut n si et seulement si k est premier avec n.
3. Si k est un diviseur de n, montrer que l'ordre de k est le quotient de n par k.
4. Soit $(\mathrm{G}, *)$ un groupe. Supposons que G contienne un élément a d'ordre n. Notons f l'application de $\{0, 1, \ldots, n-1\}$ dans G qui à
   - ◇ 0 associe l'élément neutre de G ;
   - ◇ $k \geq 1$ associe la puissance k-ième de a dans G.

   Montrer que f est un isomorphisme de groupes entre $\mathbb{Z}/n\mathbb{Z}$ et $\langle a \rangle$.

Éléments de réponse 205

Exercice 206

1. Soient S un ensemble quelconque et $E = \{0, 1\}^S$ l'ensemble des applications de S dans $\{0, 1\}$. Munissons E de l'addition $\oplus$: pour tous f, g dans E, $f \oplus g$ est définie par :

$$f \oplus g \colon S \to \{0, 1\}, \qquad x \mapsto \begin{cases} 1 \text{ si } f(x) \neq g(x) \\ 0 \text{ si } f(x) = g(x) \end{cases}$$

   1.a) Montrer que $(E, \oplus)$ est un groupe abélien.

   1.b) Montrer que chaque élément de $(E, \oplus)$ est son propre symétrique.

2. Soit $F = \mathcal{P}(S)$ l'ensemble des parties de S. Munissons F de la différence symétrique ensembliste : si A, B appartiennent à F, alors

$$A \,\Delta\, B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = (A \cap \complement B) \cup (B \cap \complement A).$$

   Considérons l'application ϕ de F dans E qui à une partie de S associe sa fonction indicatrice :

$$\phi \colon F \to E, \qquad A \mapsto \mathbb{1}_A$$

   où pour tout $x \in S$, $\mathbb{1}_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ sinon} \end{cases}$

   2.a) Montrer que φ est un isomorphisme de E vers F pour les lois $\oplus$ et Δ.

   2.b) En déduire que (F, Δ) est un groupe abélien dans lequel chaque élément est son propre symétrique.

Dans toute la suite G *désigne un groupe dans lequel chaque élément est son propre symétrique.*

3. Montrer que G est abélien.

4. Notons e l'élément neutre de G. Soit g un élément quelconque de $\mathrm{G} \setminus \{e\}$. Considérons que G la relation $\mathcal{R}$ définie par
$$\forall\, x,\, y \in \mathrm{G}, \quad x \mathcal{R} y \iff \Big(x = y \text{ ou } x = gy\Big).$$
   4.a) Montrer que $\mathcal{R}$ est une relation d'équivalence sur G.
   4.b) Montrer que chaque classe d'équivalence a deux éléments.
5. Notons $\overline{x}$ la classe d'équivalence de x. Définissons la loi $*$ sur l'ensemble quotient $\mathrm{G}/\mathcal{R}$ par
$$\forall\, x,\, y \in \mathrm{G} \quad \overline{x}\,\overline{y} = \overline{xy}.$$
   5.a) Montrer que $*$ est une loi de composition interne sur $\mathrm{G}/\mathcal{R}$.
   5.b) Montrer que $\mathrm{G}/\mathcal{R}$ muni de $*$ est un groupe abélien.
   5.c) Montrer que chaque élément de $\mathrm{G}/\mathcal{R}$ est son propre symétrique.
6. Supposons que G est fini. Déduire des questions précédentes que l'ordre de G est une puissance de 2.

Éléments de réponse 206

Exercice 207

1. Déterminer l'ensemble des éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$).
2. Soit H' l'ensemble des éléments d'ordre infini de G. Considérons $\mathrm{H} = \mathrm{H}' \cup \{e\}$ où e est l'élément neutre de G.

   Montrer que, même si H n'est pas vide, H n'est pas un sous-groupe de G.

Éléments de réponse 207

1. Les éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$) sont les couples $(0, x)$.
2. Soit H' l'ensemble des éléments d'ordre infini de G. Considérons $\mathrm{H} = \mathrm{H}' \cup \{(0, [0])\}$, l'élément neutre de G est $(0, [0])$.

   Montrons que, même si H n'est pas vide, H n'est pas un sous-groupe de G. Soient $(1, [0])$ et $(-1, [1])$. Ce sont des éléments de H. Leur somme $(0, [1])$ n'appartient pas à H. Il s'en suit que H n'est pas un sous-groupe de G.

Exercice 208 Considérons les applications suivantes de $\mathbb{R} \setminus \{0,\, 1\}$ dans lui-même :
$$f_1 \colon x \mapsto x, \qquad f_2 \colon x \mapsto 1 - x, \qquad f_3 \colon x \mapsto \frac{1}{1-x},$$
$$f_4 \colon x \mapsto \frac{1}{x}, \qquad f_5 \colon x \mapsto \frac{x}{x-1}, \qquad f_6 \colon x \mapsto \frac{x-1}{x}.$$
Munissons l'ensemble $E = \{f_1,\, f_2,\, f_3,\, f_4,\, f_5,\, f_6\}$ de la composition des applications.

1. Écrire la table de composition de $(E, \circ)$.
2. Montrer que $\mathrm{G} = (E, \circ)$ est un groupe.
3. Est-ce un groupe abélien ?
4. Déterminer tous les sous-groupes de G.
5. Déterminer l'ordre de chacun des éléments de G.
6. Quels sont les éléments de $\langle f_2 \rangle$?
7. Quels sont les éléments de $\langle f_3 \rangle$?

Éléments de réponse 208

Exercice 209 Soient $(E, \star)$ et $(F, \cdot)$ deux groupes. Munissons l'ensemble produit $E \times F$ de la loi de composition $\odot$ définie par :

$$\forall\, (x, y),\ (x', y') \in E \times F \quad (x, y) \odot (x', y') = (x * x', y \cdot y').$$

1. Montrer que $(E \times F, \odot)$ est un groupe.
2. Soient E' un sous-groupe de E et F' un sous-groupe de F. Montrer que $E' \times F'$ est un sous-groupe de $E \times F$ muni de la loi $\odot$.

Éléments de réponse 209

Exercice 210
Montrer que $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Éléments de réponse 210
Montrons que $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Raisonnons par l'absurde. Supposons que $\mathbb{Z}\times\mathbb{Z} = \langle (x, y) \rangle$. Notons que nécessairement $xy \neq 0$. Remarquons que $\langle (x, y) \rangle = \{(kx, ky) \,|\, k \in \mathbb{Z}\}$, en particulier $(x, 2y)$ n'appartient pas à $\langle (x, y) \rangle$ mais $(x, 2y)$ appartient à $\mathbb{Z} \times \mathbb{Z}$: contradiction.

Exercice 211
Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ne sont pas isomorphes.

Éléments de réponse 211
Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ne sont pas isomorphes. Le groupe $\mathbb{Z}$ ne contient pas d'élément d'ordre 2 alors que $(0, 1)$ est un élément d'ordre 2 de $\mathbb{Z}\times{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Par conséquent ces deux groupes ne sont pas isomorphes.

Exercice 212

1. Montrer que pour tout $n \in \mathbb{N}^*$ le groupe ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ contient exactement un sous-groupe cyclique d'ordre n.

2. Montrer que tout groupe est la réunion de ses sous-groupes monogènes.
3. Comparer les ordres de deux sous-groupes cycliques G et H de $\mathbb{Q}/\mathbb{Z}$ qui vérifient $G \subset H$.
4. Soit α un élément de $\mathbb{Q}/\mathbb{Z}$; déterminer tous les sous-groupes cycliques qui le contiennent.
5. Déterminer les morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$.
6. Déterminer les morphismes de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$.

Éléments de réponse 212

1. Montrons que pour tout $n \in \mathbb{N}^*$ le groupe $\mathbb{Q}/\mathbb{Z}$ contient exactement un sous-groupe cyclique d'ordre n.

   Tout élément $\overline{r} \in \mathbb{Q}/\mathbb{Z}$ admet un représentant r dans l'intervalle $[0, 1[$. Écrivons r sous la forme $\frac{p}{q}$ avec p et q premiers entre eux et $p < q$ ou $p = 0$.

   Soit H un sous-groupe cyclique d'ordre n, engendré par $\overline{r}$ avec $r = \frac{p}{q}$, $(p, q) = 1$ et $p < q$. Nous avons $n\overline{r} = \overline{r0}$, *i.e.* $\frac{np}{q} \in \mathbb{Z}$. Puisque p et q sont premiers entre eux q divise n ; autrement dit $n = qq'$ avec q' dans $\mathbb{Z}$ et $r = \frac{pq'}{n} = \frac{a}{n}$.

   Par conséquent le sous-groupe cyclique H est dans $\langle [1/n] \rangle$. Or $[1/n]$ est d'ordre n donc $H = \langle [1/n] \rangle$ est le seul sous-groupe d'ordre n cyclique de $\mathbb{Q}/\mathbb{Z}$.
2. Montrons que tout groupe est la réunion de ses sous-groupes monogènes.

   Tout élément d'un groupe engendre un sous-groupe monogène donc tout groupe est réunion de ses sous-groupes monogènes.
3. Comparons les ordres de deux sous-groupes cycliques G et H de $\mathbb{Q}/\mathbb{Z}$ qui vérifient $G \subset H$.

   Soit G un sous-groupe cyclique d'ordre p contenu dans le sous-groupe cyclique H d'ordre n. Nous avons $G = \langle [1/p] \rangle$, $H = \langle [1/n] \rangle$ et p divise n.
4. Soit α un élément de $\mathbb{Q}/\mathbb{Z}$; déterminons tous les sous-groupes cycliques qui le contiennent.

   Tout élément non nul α de $\mathbb{Q}/\mathbb{Z}$ est de la forme $\alpha = \overline{p/q}$ avec $(p, q) = 1$ et $p < q$. Cet élément est donc élément du sous-groupe cyclique d'ordre q de $\mathbb{Q}/\mathbb{Z}$ soit $\langle \overline{1}q \rangle$. Ainsi l'élément α est dans tous les sous-groupes cycliques $\langle \overline{1/n} \rangle$ où q divise n. De plus tous les sous-groupes monogènes de $\mathbb{Q}/\mathbb{Z}$ sont cyclique.
5. Déterminons les morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$.

   Soit φ un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$. L'image de φ est un sous-groupe cyclique de $\mathbb{Q}/\mathbb{Z}$ contenu dans le sous-groupe cyclique $\langle [1/n] \rangle$. Pour déterminer φ il suffit donc de se donner l'image de $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ dans $\langle \frac{\overline{1}}{n} \rangle$. Il y a donc n morphismes possibles.
6. Déterminons les morphismes de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$.

   L'image d'un élément d'ordre fini par un morphisme est un élément d'ordre fini. Le groupe $\mathbb{Z}$ possède un unique élément d'ordre fini : 0. Il s'en suit que tous les éléments

d'ordre fini de $\mathbb{Q}/\mathbb{Z}$ ont pour image 0. La question 2. assure que tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini. Par suite le seul morphisme de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$ est le morphisme nul.

Exercice 213

Montrer qu'un groupe est fini si et seulement si il n'a qu'un nombre fini de sous-groupes.

Éléments de réponse 213

Soit G un groupe fini. L'ensemble des sous-groupes de G est un sous-ensemble de l'ensemble des parties de G qui est de cardinal fini. Ainsi G ne contient qu'un nombre fini de sous-groupes.

Réciproquement soit G un groupe ne possédant qu'un nombre fini de sous-groupes. Nous avons

$$\mathrm{G} = \bigcup_{g\in\mathrm{G}} \langle g\rangle.$$

Les sous-groupes de la forme $\langle g\rangle$, qui sont les sous-groupes monogènes, sont en nombre fini. En fixant dans chacun d'eux un générateur nous les écrivons $\langle g_1\rangle$, $\langle g_2\rangle$, …, $\langle g_k\rangle$ de sorte que

$$\mathrm{G} = \bigcup_{i=1}^{k} \langle g_i\rangle.$$

Si l'un des $\langle g_i\rangle$ est infini, il est isomorphe à $\mathbb{Z}$ et contient de ce fait une infinité de sous-groupes : contradiction avec l'hypothèse « G contient un nombre fini de sous-groupes ». Ainsi tous les sous-groupes $\langle g_i\rangle$, $i = 1, 2, \ldots, k$, sont d'ordre fini. Leur réunion est donc de cardinal fini mais cette réunion est G. Par conséquent G est un groupe fini.

Exercice 214

Quels sont les éléments d'ordre 3 du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Éléments de réponse 214

On cherche $(\overline{x}, \overline{y}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ tel que $3 = o(\overline{x}, \overline{y}) = \mathrm{ppcm}(o(\overline{x}), o(\overline{y}))$, *i.e.* tel que

- $o(\overline{x}) = 1$ et $o(\overline{y}) = 3$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 1$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 3$.

Par ailleurs

- $o(\overline{x}) = 3$ si et seulement si $\overline{x} \in \{\overline{1}, \overline{2}\}$,
- $o(\overline{x}) = 1$ si et seulement si $\overline{x} = \overline{0}$,
- $o(\overline{y}) = 3$ si et seulement si $\overline{y} \in \{\overline{2}, \overline{4}\}$,
- $o(\overline{y}) = 1$ si et seulement si $\overline{y} = \overline{0}$.

Il en résulte que les éléments d'ordre 3 de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sont

$$(\overline{0},\overline{2}), \quad (\overline{0},\overline{4}), \quad (\overline{1},\overline{0}), \quad (\overline{2},\overline{0}), \quad (\overline{1},\overline{2}), \quad (\overline{1},\overline{4}), \quad (\overline{2},\overline{2}), \quad (\overline{2},\overline{4}).$$

Exercice 215

Étudier le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 215

La table de multiplication de $\mathrm{G} = \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) = \{e,\, a_1,\, a_2,\, a_3\}$ est :

- $\forall i \; ea_i = a_i$;
- $\forall\, i \; a_i^2 = e$;
- $\forall\, i \; \forall\, j \neq i \; a_i a_j = a_k$ où $k \neq i$, $k \neq j$, où $i,\, j,\, k \in \{1,\, 2,\, 3\}$.

Tout automorphisme φ de G laisse fixe e. Il permute donc les autres éléments a_1, a_2 et a_3.

Réciproquement pour toute permutation φ de ces trois éléments, en posant $\varphi(e) = e$, on obtient une bijection de G sur G qui respecte la table de multiplication ci-dessus. C'est donc un automorphisme.

Ainsi Aut(G) est d'ordre $3! = 6$ et isomorphe au groupe $\mathfrak{S}_3$ des permutations de $\{1,\, 2,\, 3\}$.

Exercice 216

Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Éléments de réponse 216

Dans $\mathbb{Z}$ la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un groupe. En effet la somme $2+3 = 5$ d'un élément de $2\mathbb{Z}$ et d'un élément de $3\mathbb{Z}$ n'est ni multiple de 2, ni multiple de 3.

Exercice 217

Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}(2,\mathbb{R})$;

(b) le groupe alterné $\mathcal{A}_8$;

(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;

(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Éléments de réponse 217

(a) La rotation d'angle $\frac{\pi}{2}$ est un exemple d'élément d'ordre 4 dans $\mathrm{GL}(2,\mathbb{R})$, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

(b) $(1\,2\,3\,4)(5\,6)$ est un exemple d'élément d'ordre 4 dans $\mathcal{A}_8$.

(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ ne contient pas d'élément d'ordre 4. Il contient douze éléments dont huit d'ordre 3, trois d'ordre 2 et l'identité.

Autre justification possible : $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ est isomorphe à $\mathcal{A}_4$ et $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4 (les 4-cycles ne sont pas de signature 1).

(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui contient le neutre d'ordre 1 et des éléments d'ordre 2.

Exercice 218

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.

Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.

Montrer que G/T est sans torsion.

Éléments de réponse 218 Notons $o(g)$ l'ordre d'un élément $g \in \mathrm{G}$.

Puisque $o(e) = 1$, on a $e \in \mathrm{T}$. Soient x, $y \in \mathrm{T}$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m(y^m)^k = e$ donc $xy \in \mathrm{T}$. Comme $o(x) = o(x^{-1})$, on a $x^{-1} \in \mathrm{T}$. Ainsi T est un sous-groupe de G.

Considérons l'application canonique $\varphi\colon \mathrm{G} \to \mathrm{G}/\mathrm{T}$. Soit $a \in \mathrm{G}/\mathrm{T}$ d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in \mathrm{G}$ tel que $a = \varphi(x)$. On a

$$\varphi(x^s) = a^s = e$$

donc $x^s \in \mathrm{T} = \ker\varphi$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$ ce qui prouve que $x \in \mathrm{T}$ et donc que $a = \varphi(x) = e$. Par suite G/T est sans torsion.

Exercice 219

Soit G un groupe tel que $g^2 = e$ pour tout g dans G.

Montrer que G est abélien.

Éléments de réponse 219

Pour tous g, h dans G on a $(gh)^2 = e$, soit $ghgh = e$, d'où $(ghgh)(hg) = hg$. Mais $(ghgh)(hg) = ghgh^2g$. Or h appartient à G donc $h^2 = e$ et $ghgh^2g = ghg^2$. Puisque g est dans G on a $g^2 = e$ et $ghg^2 = gh$. Ainsi $(ghgh)(hg) = hg$ se réécrit $gh = hg$.

Exercice 220

Soit G un groupe fini.

a) Montrer que des éléments conjugués dans G sont de même ordre.

b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?

c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Éléments de réponse 220

a) Soient g, h dans G et n dans $\mathbb{N}$. On a $(hgh^{-1})^n = hg^nh^{-1}$. Ainsi $(hgh^{-1})^n = e$ si et seulement si $hg^nh^{-1} = e$ si et seulement si $g^n = h^{-1}eh$ autrement dit si et seulement si $g^n = e$.

b) Deux éléments de même ordre dans un groupe fini ne sont pas toujours conjugués. Considérons par exemple le groupe $\mathbb{Z}/3\mathbb{Z}$; il contient deux éléments d'ordre 3 qui ne sont pas conjugués.

c) Soit G un groupe abélien fini. Les classes de conjugaison de G sont réduites à un élément. La question précédente a une réponse positive si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe contient un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Ainsi les seuls groupes abéliens qui conviennent sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Si G est le groupe des permutations $\mathfrak{S}_3$, alors les éléments d'ordre 2 sont les transpositions (1 2), (1 3) et (2 3) qui sont conjuguées et les éléments d'ordre 3 sont les 3-cyles (1 2 3) et (1 3 2) qui sont également conjugués. Le groupe $G = \mathfrak{S}_3$ est donc un groupe fini non abélien tel que deux éléments de même ordre dans G sont toujours conjugués.

Exercice 221

Soit $\varphi\colon \mathrm{G}_1 \to \mathrm{G}_2$ un morphisme de groupes. Soit g un élément de G_1 d'ordre fini.
Montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.

Éléments de réponse 221

Soit n l'ordre de g. On a $g^n = e$ donc $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$, autrement dit l'ordre de $\varphi(g)$ divise n.

Exercice 222

a) Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Montrer que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

b) Soient α et β deux réels non nuls. Discuter de la nature du sous-groupe additif qu'ils engendrent.

c) Soit $\beta \notin \mathbb{Q}$. Montrer que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrer que $\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^1$ de $\mathbb{C}$.

En déduire

i) qu'un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$;

ii) les valeurs d'adhérence de la suite $(\sin(n))_{n\geq 0}$.

Éléments de réponse 222

a) Soit G un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$. Montrons que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a>0$ (donc discret).

Si G est monogène, *i.e.* si $\mathrm{G}=a\mathbb{Z}$, avec $a>0$, alors a est le plus petit élément strictement positif de G. Si G est dense dans $\mathbb{R}$, alors $\mathrm{G}\cap\mathbb{R}_+^*$ n'a pas de plus petit élément mais une borne inférieure non nulle. On introduit donc

$$\mathrm{G}_+=\mathrm{G}\cap\mathbb{R}_+^* \qquad\qquad a=\inf \mathrm{G}_+$$

Le réel $a\geq 0$ est bien défini car G_+ est non vide et minorée. En effet il existe un élément g dans G non nul donc x ou $-x$ est dans G_+ qui est minoré par 0.

On va distinguer le cas $a>0$ du cas $a=0$.

- ◇ Supposons $a>0$. Montrons que a appartient à G puis que $\mathrm{G}=a\mathbb{Z}$.

  Raisonnons par l'absurde : supposons que a n'appartienne pas à G. Puisque $a>0$, on a $2a>a$. Il existe g dans G_+ tel que $g<2a$. Comme a n'appartient pas à G, on a les inégalités $a<g<2a$. Il existe alors h dans G_+ tel que $h<g$. On a $a<h<g<2a$ car a n'appartient pas à G. De plus comme g et h appartiennent à G, la différence $g-h$ appartient à G et on a même $g-h$ appartient à G_+. D'une part $a<h$ donc $a-h<0$ et $2a-h<a$, d'autre part $g<2a$ donc $g-h<2a-h$. Par conséquent $g-h<a$: contradiction avec la définition de a. Par suite a appartient à G. Ainsi le groupe $a\mathbb{Z}$ engendré par a est inclus dans G.

  Réciproquement soit g un élément de G. Posons $k=E\left(\frac{g}{a}\right)\in\mathbb{Z}$. Puisque G est un groupe le réel $g-ak$ appartient à G. Comme $k\leq\frac{g}{a}<k+1$ on a $0\leq g-ak<a=\min \mathrm{G}_+$. Nécessairement $g-ak=0$ et $g=ak\in a\mathbb{Z}$. Il en résulte que $\mathrm{G}=a\mathbb{Z}$.

- ◇ Supposons que $a=0$. Montrons qu'alors G est dense dans $\mathbb{R}$, autrement dit que G rencontre tout intervalle ouvert de $\mathbb{R}$. Soit $I=]\alpha,\beta[$ un intervalle ouvert de $\mathbb{R}$. Comme $a=0$ il existe $g\in\mathrm{G}$ tel que $0<g<\beta-\alpha$. Le sous-groupe $g\mathbb{Z}$ engendré par g est inclus dans G et intersecte I (sinon il existerait $k\in\mathbb{Z}$ tel que $I\subset]kg,(k+1)g[$ ce qui contredirait l'inégalité $g<\beta-\alpha$). Il s'en suit que G est dense dans $\mathbb{R}$.

b) Il s'agit d'étudier le groupe $\mathrm{G}=\alpha\mathbb{Z}+\beta\mathbb{Z}\neq\{0\}$.

Supposons qu'il existe $a>0$ tel que $\mathrm{G}=a\mathbb{Z}$. Puisque α et β appartiennent à G, il existe k et ℓ dans $\mathbb{Z}$ tels que $\alpha=ka$ et $\beta=\ell a$. Le rapport $\frac{\alpha}{\beta}$ s'écrit aussi $\frac{k}{\ell}$ et appartient à $\mathbb{Q}$.

Réciproquement supposons que $\frac{\alpha}{\beta}$ soit rationnel. Écrivons $\frac{\alpha}{\beta}$ sous la forme $\frac{k}{\ell}$ avec k et ℓ premiers entre eux. Alors

$$\alpha\mathbb{Z}+\beta\mathbb{Z}=\beta\left(\frac{k}{\ell}\mathbb{Z}+\mathbb{Z}\right)=\frac{\beta}{\ell}(k\mathbb{Z}+\ell\mathbb{Z})=\frac{\beta}{\ell}\mathbb{Z}$$

car k et ℓ sont premiers entre eux.

Ainsi si $\frac{\alpha}{\beta}$ appartient à $\mathbb{Q}$, alors G est monogène et sinon G est dense dans $\mathbb{R}$.

c) Soit $\beta \notin \mathbb{Q}$. Montrons que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.

Le sous-groupe additif $\mathrm{G} = \mathbb{Z} + \beta\mathbb{Z}$ de $\mathbb{R}$ est dense d'après b). Montrons que l'ensemble $\mathbb{N}\beta + \mathbb{Z}$ reste encore dense. Soient $a < b$ deux réels. Nous pouvons trouver un élément $x = v\beta + u \in \mathrm{G}$ tel que $0 < x < b - a$.

- ◇ Supposons que v soit un entier naturel, *i.e.* que x appartienne à $\mathbb{N}\beta + \mathbb{Z}$. Choisissons un entier $n_0 < a$. Les éléments de la suite $(kx + n_0)_{k\geq 0}$ appartiennent à $\mathbb{N}\beta + \mathbb{Z}$ et un argument analogue à celui de a) assure que l'un d'eux au moins appartient à $]a, b[$.
- ◇ Supposons que $v < 0$. Alors $-x$ appartient à $\mathbb{N}\beta + \mathbb{Z}$ et $-(b-a) < -x < 0$. Choisissons $n_0 \in \mathbb{Z}$ avec $n_0 > b$. Alors au moins un élément de la suite $(n_0 - kx)_{k\geq 0}$ appartient à $]a, b[$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrons que $\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^1$ de $\mathbb{C}$.

Posons $\Omega = \{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$. Il s'agit de l'image par l'application $f\colon x \mapsto \exp(2\mathbf{i}\pi x)$ de l'ensemble $\mathbb{Z} + \frac{\vartheta}{2\pi}\mathbb{N}$. Puisque f est continue et que Ω est dense dans $\mathbb{R}$ d'après c) l'image $f(\Omega)$ de Ω par f est dense dans $f(\mathbb{R}) = \mathbb{S}^1$.

i) D'après a) un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$.

ii) Si $\vartheta = 1$, alors $\frac{1}{\pi}$ n'est pas rationnel et l'ensemble $\{\exp(\mathbf{i}n) \,|\, n \in \mathbb{N}\}$ est dense dans $\mathbb{S}^1$. Puisque l'application qui à un nombre complexe associe sa partie imaginaire est continue, l'ensemble $\{\sin(n) \,|\, n \in \mathbb{N}\}$ est dense dans $[-1, 1]$. Pour tout $-1 \leq a \leq 1$, pour tout $\varepsilon > 0$ et pour tout $N \in \mathbb{N}$ nous sommes alors assurés de trouver un entier $n \geq N$ tel que $|\sin(n) - a| \leq \varepsilon$. Autrement dit tout réel de $[-1, 1]$ est une valeur d'adhérence de la suite $(\sin(n))_{n\geq 0}$. L'autre inclusion est directe. Finalement l'ensemble des valeurs d'adhérences de la suite $(\sin(n))_{n\geq 0}$ est le segment $[-1, 1]$.

Exercice 223

Montrer que le morphisme $\xi\colon \mathbb{R} \to \mathbb{U}$, $x \mapsto \exp(\mathbf{i}x)$ est un morphisme surjectif du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{U}$.

Éléments de réponse 223

Exercice 224

Montrer que si $n \geq 2$, le seul sous-groupe fini de $(\mathbb{C}^*, \cdot)$ d'ordre n est le groupe μ_n des racines $n$ième de l'unité.

Éléments de réponse 224

Soit G un sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n. Soit g un élément de G. L'ordre de g divise n ; en particulier $g^n = \mathrm{id}$. Il en résulte que $\mathrm{G} \subset \mu_n$.

De plus $|\mathrm{G}| = |\mu_n|$.
Il en résulte que $\mathrm{G} = \mu_n$.

Exercice 225

Soit $p > 2$ un nombre premier. Soit G un groupe non abélien d'ordre $2p$.

(1) Montrer qu'il existe x, y dans G avec x d'ordre 2, y d'ordre p et $\mathrm{G} = \langle x, y\rangle$.

(2) Montrer que $xyx = y^i$ pour un certain $2 \leq i \leq p-1$, puis montrer que $i^2 \equiv 1 \bmod p$, et en déduire que $i = p-1$.

(3) Montrer que G est isomorphe au groupe diédral D_{2p}.

Éléments de réponse 225

(1) Le fait qu'il existe $x \in \mathrm{G}$ d'ordre 2 et $y \in \mathrm{G}$ d'ordre p découle du théorème de Cauchy [2]. Comme $\langle x\rangle \subsetneq \langle x, y\rangle$ et $\langle y\rangle \subsetneq \langle x, y\rangle$ par Lagrange l'ordre du sous-groupe $\langle x, y\rangle \subset \mathrm{G}$ est un multiple strict de 2 et de p, et un diviseur de $2p$. Il s'en suit que cet ordre est égal à $2p$, et donc $\langle x, y\rangle = \mathrm{G}$.

(2) Le groupe $\langle y\rangle$ est d'indice 2 dans G, donc est distingué dans G. Par suite $xyx^{-1} = xyx \in \langle y\rangle$ ce qui revient à dire qu'il existe $1 \leq i \leq p-1$ tel que $xyx = y^i$ (notons que si $i = 0$, alors $xyx = y^0$ se réecrit $xyx^{-1} = \mathrm{id}$, soit $y = \mathrm{id}$: contradiction avec y d'ordre p). Enfin $i \neq 1$, car sinon x et y commutent, et comme ils engendrent G le groupe G serait abélien, en contradiction avec l'hypothèse. Puisque $x^2 = 1$, on a

$$y = x^2yx^2 = x(xyx)x = xy^ix = (xyx)^i = (y^i)^i = y^{i^2},$$

d'où $i^2 \equiv 1 \bmod p$ puisque y est d'ordre p. L'équation $x^2 = 1$ a deux solutions sur le corps $\mathbb{Z}/p\mathbb{Z}$: $x = \overline{1}$ et $x = -\overline{1}$. Mais comme on a $i \geq 2$, on en déduit que $\overline{i} = -\overline{1}$ et $i = p-1$.

(3) Le groupe diédral D_{2p} est engendré par une rotation r d'ordre p et une symétrie axiale s : on peut prendre r la rotation d'angle $\frac{2\pi}{p}$ et s la symétrie par rapport à l'axe des abscisses. On a alors

$$\mathrm{D}_{2p} = \{\mathrm{id},\, s,\, r,\, rs,\, r^2,\, r^2s,\, \ldots,\, r^{p-1},\, r^{p-1}s\}$$

et la loi de groupe sur D_{2p} se déduit des relations $s^2 = \mathrm{id}$, $r^p = \mathrm{id}$ et $srs = r^{-1}$. Par les questions précédentes, tout groupe G non abélien d'ordre $2p$ peut s'écrire $\mathrm{G} = \{\mathrm{id},\, x,\, y,\, yx,\, y^2,\, y^2x,\, \ldots,\, y^{p-1},\, y^{p-1}x\}$ avec $x^2 = \mathrm{id}$, $y^p = \mathrm{id}$ et $xyx = y^{-1}$. On en déduit que G est isomorphe à D_{2p} via l'isomorphisme qui envoie x sur s et y sur r.

Exercice 226

2. Le théorème de Cauchy sur les groupes finis dit que si G est un groupe fini d'ordre n alors pour tout entier premier p divisant n il existe un élément de G d'ordre p, autrement dit il existe un sous-groupe de G d'ordre p.

(1) Montrer que le sous-groupe $\mathbb{H}_{12}$ de $\mathrm{SL}(2,\mathbb{C})$ engendré par les matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{et} \qquad K = \begin{pmatrix} \mathbf{j} & 0 \\ 0 & \mathbf{j}^2 \end{pmatrix}$$

est d'ordre 12 (où on a noté $\mathbf{j} = \exp\left(\frac{2i\pi}{3}\right)$).

(2) Montrer que les groupes d'ordre 12 suivants sont deux à deux non isomorphes : $\mathbb{H}_{12}$, $\mathcal{A}_4$ (groupe alterné) et D_{12} (groupe diédral).

Éléments de réponse 226

(1) On peut vérifier que la matrice I est d'ordre 4 et la matrice K d'ordre 3. De plus $IK = K^2I$; en effet

$$IK = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \mathbf{j} & 0 \\ 0 & \mathbf{j}^2 \end{pmatrix} = \begin{pmatrix} 0 & \mathbf{j}^2 \\ -\mathbf{j} & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{j}^2 & 0 \\ 0 & \mathbf{j} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = K^2I$$

Par suite $\mathbb{H}_{12} = \langle I,\, K\rangle$ est constitué des 12 matrices suivantes :

$$\mathbb{H}_{12} = \{\mathrm{id},\, I,\, I^2,\, I^3,\, K,\, KI,\, KI^2,\, KI^3,\, K^{-1},\, K^{-1}I,\, K^{-1}I^2,\, K^{-1}I^3\}.$$

(2) L'élément $KI^2 = \begin{pmatrix} -\mathbf{j} & 0 \\ 0 & -\mathbf{j}^2 \end{pmatrix}$ est d'ordre 6 dans $\mathbb{H}_{12}$, alors que $\mathcal{A}_4$ ne contient aucun élément d'ordre 6, donc $\mathbb{H}_{12}$ et $\mathcal{A}_4$ ne sont pas isomorphes. Le groupe D_{12} contient sept éléments d'ordre 2 (six symétries axiales et la rotation d'angle π), alors que $\mathcal{A}_4$ n'en contient que trois (les doubles transpositions), donc D_{12} et $\mathcal{A}_4$ ne sont pas isomorphes. L'élément I est d'ordre 4 dans $\mathbb{H}_{12}$, alors que D_{12} ne contient aucun élément d'ordre 4. Il s'en suit que $\mathbb{H}_{12}$ et D_{12} ne sont pas isomorphes.

Exercice 227

Notons $\mathrm{T} \subset \mathrm{GL}\left(3, \mathbb{Z}/3\mathbb{Z}\right)$ le sous-groupe des matrices de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

avec a, b et c dans $\mathbb{Z}/3\mathbb{Z}$.

(1) Montrer que tout élément non trivial de T est d'ordre 3.

(2) Le groupe T est-il isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?

(3) En quoi cet exemple est-il intéressant ?

Éléments de réponse 227

(1) On peut utiliser le fait que sur n'importe quel corps $\mathbb{k}$, toute matrice de la forme

$$N = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

est nilpotente d'indice 3, c'est-à-dire $N^3 = 0$ (plutôt que de le vérifier en faisant le produit matriciel, on peut juste constater que les vecteurs e_1, e_2 et e_3 de la base satisfont

$$N(e_1) = 0, \qquad N^2(e_2) = N(ae_1) = 0 \qquad \text{et} \qquad N^3(e_3) = N^2(be_1 + ce_2) = 0.$$

Donc une matrice de la forme $\mathrm{id} + N$ vérifie

$$(\mathrm{id} + N)^3 = \mathrm{id} + 3N + 3N^2.$$

Si maintenant le corps est de caractéristique 3 (comme ici $\mathbb{Z}/3\mathbb{Z}$), alors $(\mathrm{id} + N)^3 = \mathrm{id}$ et donc tout élément non trivial de T est d'ordre 3.

(2) Le groupe T n'est pas isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ car T n'est pas abélien. En effet par exemple :

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

(3) Cet exercice permet de réaliser que le raisonnement suivant n'est pas correct :

« Montrons que $\mathfrak{S}_3$ et $\mathrm{Isom}(T)$, où T est un triangle, sont isomorphes. Le groupe $\mathfrak{S}_3$ contient le neutre, trois éléments d'ordre 2 (les transpositions) et deux éléments d'ordre 3 (les 3-cycles). De même, $\mathrm{Isom}(T)$ contient le neutre, trois éléments d'ordre 2 (les symétries axiales) et deux rotations d'ordre 3. Comme ces groupes ont des éléments deux à deux du même ordre ils sont isomorphes. »

Exercice 228

Soit G un groupe fini d'ordre impair.

1. Montrer que l'application $f\colon \mathrm{G} \to \mathrm{G}$, $x \mapsto x^2$ est une bijection.
2. En déduire que pour $x \in \mathrm{G}$ l'équation $x^2 = e$ admet une unique solution ; laquelle ?

Éléments de réponse 228

Soit n tel que $|\mathrm{G}| = 2n + 1$. Pour tout $x \in \mathrm{G}$ on a $x^{2n+1} = e$.

1. Montrons que f est surjective, elle sera alors bijective. Soit $y \in \mathrm{G}$; nous cherchons $x \in \mathrm{G}$ tel que $f(x) = y$. Posons $x = y^{n+1}$, alors
$$f(x) = x^2 = (y^{n+1})^2 = y^{2n+2} = y^{2n+1}y = y$$
ce qui démontre le résultat.
2. D'après ce qui précède l'application f est bijective et il existe un unique $x \in \mathrm{G}$ tel que $x^2 = e$, c'est $x = e$.

Exercice 229

Soit $\mathbb{H} \subset \mathrm{GL}(2, \mathbb{C})$ le sous-ensemble suivant
$$\mathbb{H} = \{\mathbf{1},\ -\mathbf{1},\ I,\ -I,\ J,\ -J,\ K,\ -K\}$$
avec
$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$$
1. Montrer que $\mathbb{H}$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{C})$.
2. Le groupe $\mathbb{H}$ est-il abélien ?
3. Déterminer tous les sous-groupes de $\mathbb{H}$.

Éléments de réponse 229

1. On vérifie les formules suivantes : $I^2 = J^2 = K^2 = -\mathbf{1}$. En particulier $I^{-1} = -I$, $J^{-1} = -J$ et $K^{-1} = -K$ sont dans $\mathbb{H}$. De même $(-I)^{-1} = I$, $(-J)^{-1} = J$ et $(-K)^{-1} = K$ sont dans $\mathbb{H}$. Ainsi les inverses des éléments de $\mathbb{H}$ sont dans $\mathbb{H}$.

   On vérifie les formules $IJ = K$, $JI = -K$, $IK = -J$, $KI = J$, $JK = I$ et $KJ = -I$. Ainsi le produit de deux éléments de $\mathbb{H}$ est encore dans $\mathbb{H}$ et $\mathbb{H}$ est un sous-groupe de $\mathrm{GL}(2, \mathbb{C})$.
2. Non car $IJ = -JI$.
3. Le groupe $\mathbb{H}$ est d'ordre 8. Ces sous-groupes sont donc d'ordre 1, 2, 4 ou 8.

   Le seul sous-groupe d'ordre 1 est $\{\mathbf{1}\}$.

   Comme $I^2 = J^2 = K^2 = -\mathbf{1}$ les éléments I, J et K sont d'ordre 4. Il en est de même pour $-I$, $-J$ et $-K$. Ainsi le seul élément d'ordre 2 de $\mathbb{H}$ est $-\mathbf{1}$. Le seul sous-groupe d'ordre 2 est donc $\{\pm\mathbf{1}\}$.

   Un sous-groupe d'ordre 4 doit donc contenir au moins un élément d'ordre 4 et est donc engendré par cet élément. Les possibilités sont
   $$\langle I \rangle = \{\pm\mathbf{1},\ \pm I\}, \qquad \langle J \rangle = \{\pm\mathbf{1},\ \pm J\}, \qquad \langle K \rangle = \{\pm\mathbf{1},\ \pm K\},$$
   Enfin il y a un sous-groupe d'ordre 8 : $\mathbb{H}$.

   Finalement les sous-groupes de $\mathbb{H}$ sont
   $$\{\mathbf{1}\}, \qquad \{\pm\mathbf{1}\}, \qquad \langle I \rangle \qquad \langle J \rangle \qquad \langle K \rangle \qquad \mathbb{H}$$

Exercice 230

Soit $B \subset \mathrm{GL}(n,\mathbb{R})$ le sous-ensemble des matrices triangulaires supérieures. Soit $T \subset B$ le sous-ensemble des matrices diagonales et soit $U \subset B$ le sous-ensemble des matrices triangulaires supérieures ayant un 1 sur la diagonale.

1. Montrer que B, T et U sont des sous-groupes de $\mathrm{GL}(n,\mathbb{R})$.
2. Montrer que l'application $\varphi\colon B \to T$ qui à une matrice supérieure associe sa partie diagonale est un morphisme de groupes.
3. Montrer que $U = \ker\varphi$ et en déduire que $U \triangleleft B$.
4. Montrer que le groupe quotient B/U est isomorphe à T.

Éléments de réponse 230

1. Soit $(e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$. Montrons que nous avons

   $$B = \{g \in \mathrm{GL}(n,\mathbb{R}) \,|\, g(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle \text{ pour tout } 1 \leq i \leq n\}.$$

   Si g appartient à B, alors $g(e_i)$ appartient à $\langle e_1, e_2, \ldots, e_i\rangle$ d'où l'inclusion $g(\langle e_1, e_2, \ldots, e_i\rangle) \subset \langle e_1, e_2, \ldots, e_i\rangle$. Puisque g est bijective nous avons l'égalité. Réciproquement si $g(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle$ pour tout $1 \leq i \leq n$, alors $g(e_i) = \sum_{j=1}^{i} g_{ji}e_j$ donc g est triangulaire supérieure et g appartient à B.

   Montrons maintenant que B est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$. Si g et h appartiennent à B, nous avons

   $$g(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle \qquad h(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle$$

   donc

   $$h^{-1}(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle$$

   et

   $$gh^{-1}(\langle e_1, e_2, \ldots, e_i\rangle) = g(\langle e_1, e_2, \ldots, e_i\rangle) = \langle e_1, e_2, \ldots, e_i\rangle$$

   dont gh^{-1} appartient à B qui est bien un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$.

   De la même manière montrons que nous avons

   $$T = \{g \in \mathrm{GL}(n,\mathbb{R}) \,|\, g(\langle e_i\rangle) = \langle e_i\rangle \text{ pour tout } 1 \leq i \leq n\}.$$

   Si g appartient à T, alors g envoie e_i dans $\langle e_i\rangle$ d'où l'inclusion $g(\langle e_i\rangle) \subset \langle e_i\rangle$. Comme g est bijective, on a égalité. Réciproquement si $g(\langle e_i\rangle) = \langle e_i\rangle$ pour tout $1 \leq i \leq n$, alors $g(e_i) = g_{ii}e_i$ donc g est diagonale et g appartient à T.

   Montrons maintenant que T est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$. Si g et h appartiennent à T, nous avons $g(\langle e_i\rangle) = \langle e_i\rangle$ et $h(\langle e_i\rangle) = \langle e_i\rangle$ donc $h^{-1}(\langle e_i\rangle) = \langle e_i\rangle$ et $gh^{-1}(\langle e_i\rangle) = g(\langle e_i\rangle) = \langle e_i\rangle$ donc gh^{-1} appartient à T qui est bien un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$.

   Nous montrons que U est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$ un peu après.

2. Montrons que φ est un morphisme de groupes. Si g, h appartiennent à B, alors en écrivant $g = (g_{ij})$ et $h = (h_{ij})$ nous avons $gh = (a_{ij})$ avec $a_{ij} = \sum_{k=1}^{n} g_{ik}h_{kj}$. Nous nous intéressons à la partie diagonale donc à a_{ii}. Nous avons $g_{ij} = 0 = h_{ij}$ pour $i > j$; nous obtenons
$$a_{ii} = \sum_{k=1}^{n} g_{ik}h_{ki} = \sum_{k=1}^{i-1} g_{ik}h_{ki} + g_{ii}h_{ii} + g_{ii}h_{ii} + \sum_{k=i+1}^{n} g_{ik}h_{ki}$$
donc
$$a_{ii} = \sum_{k=1}^{i-1} 0 \times h_{ki} + g_{ii}h_{ii} + \sum_{k=i+1}^{n} g_{ik} \times 0 = g_{ii}h_{ii}.$$
Il en résulte que φ est un morphisme de groupes.
3. Par définition de U, nous avons $U = \ker\varphi$. Ainsi U est un sous-groupe de B et donc de $\mathrm{GL}(n,\mathbb{R})$ et il est distingué dans B.
4. Le morphisme de groupes $\varphi\colon B \to T$ est surjectif ; en effet pour $g \in T \subset B$, on a $\varphi(g) = g$. Ainsi on a un isomorphisme
$$B/U = B/\ker\varphi \simeq \operatorname{im}\varphi = T.$$

Exercice 231

Notons D_8 le groupe des isométries qui préservent un carré. Montrer que les groupes
$$\mathbb{Z}/8\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{D}_8, \qquad \mathbb{H}$$
sont 2 à 2 non isomorphes.

Lesquels sont abéliens ?

Éléments de réponse 231

On regarde les ordres des éléments.

Le seul groupe ayant un élément d'ordre 8 est $\mathbb{Z}/8\mathbb{Z}$; il n'est donc isomorphe à aucun autre. Il est abélien.

Le seul groupe ayant uniquement des éléments d'ordre 2 est $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$, il n'est isomorphe à aucun autre. Il est abélien.

Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{R}$ est abélien alors que D_8 et $\mathbb{H}$ ne le sont pas, il n'est donc isomorphe à aucun autre. Il est abélien.

Le groupe D_8 des isométries d'un carré $ABCD$ de centre O contient la rotation r de centre O et d'angle $\frac{\pi}{2}$ qui est d'ordre 4. De plus il contient la symétrie s_{AB} par rapport à la médiatrice de $[AB]$. De plus nous avons $rs_{AB}r^{-1} = s_{CB}$ la symétrie par rapport à la médiatrice de $[BC]$. Par conséquent D_8 n'est pas abélien. Enfin le groupe D_8 contient s_{AB} et s_{BC} qui sont d'ordre 2 donc il contient 2 éléments d'ordre 2. Ce n'est pas le cas du groupe $\mathbb{H}$ donc D_8 n'est isomorphe à aucun autre. Il n'est pas abélien.

D'après ce qui précède le groupe $\mathbb{H}$ n'est isomorphe à aucun autre. Il n'est pas abélien.

Exercice 232

1. Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est cyclique. Le groupe G est-il abélien ? Justifier.
2. Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est abélien. Le groupe G est-il abélien ? Justifier.
3. Montrer que la probabilité que deux éléments d'un groupe fini non abélien commutent est $\leq \frac{5}{8}$ (indication : on pourra utiliser 1.).

Éléments de réponse 232

1. Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est cyclique. Le groupe G est abélien. En effet le groupe $\mathrm{G}/Z(\mathrm{G})$ étant cyclique il existe $\overline{a} \in \mathrm{G}/Z(\mathrm{G})$ tel que $\mathrm{G}/Z(\mathrm{G}) = \langle \overline{a} \rangle$. Tout élément de G est alors de la forme $a^m z$ avec m dans $\mathbb{N}$ et z dans $Z(\mathrm{G})$. Soient g, h deux éléments de G ; alors g (resp. h) s'écrit $a^m z_1$ (resp. $a^p z_2$) avec m (resp. p) dans $\mathbb{N}$ et z_1 (resp. z_2) dans $Z(\mathrm{G})$. En particulier

$$\begin{aligned}
gh &= (a^m z_1)(a^p z_2) \\
&= a^m z_1 a^p z_2 \\
&= a^m a^p z_1 z_2 \qquad \text{car } z_1 \text{ appartient à } Z(\mathrm{G}) \\
&= a^m a^p z_2 z_1 \qquad \text{car } z_1 \text{ appartient à } Z(\mathrm{G}) \\
&= a^{m+p} z_2 z_1 \\
&= a^{p+m} z_2 z_1 \\
&= a^p a^m z_2 z_1 \\
&= a^p z_2 a^m z_1 \qquad \text{car } z_2 \text{ appartient à } Z(\mathrm{G}) \\
&= (a^p z_2)(a^m z_1) \\
&= hg
\end{aligned}$$

2. Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est abélien. Le groupe G n'est pas nécessairement abélien, considérer par exemple $\mathrm{G} = \mathbb{H}_8$.
3. Montrer que la probabilité que deux éléments d'un groupe fini non abélien commutent est $\leq \frac{5}{8}$ (indication : on pourra utiliser 1.).

   Soit G un groupe fini non abélien. Désignons par n l'ordre de G et par z l'ordre de $Z(\mathrm{G})$. Puisque G n'est pas abĺien le 1. assure que $\mathrm{G}/Z(\mathrm{G})$ ne peut pas ˆetre cyclique et est donc d'ordre au moins 4. Ainsi $n \geq 4z$.

   Soit $x \in Z(\mathrm{G})$; par définition du centre x commute avec tout élément y de G. Soit $x \in \mathrm{G} \setminus Z(\mathrm{G})$; les éléments y de G qui commutent avec x sont les éléments du centralisateur de x pour l'action par conjugaison. Nous obtenons alors un sous-groupe strict de G (car x n'est pas central) d'ordre $\leq \frac{n}{2}$. Nous obtenons finalement que le nombre de couples

$(x, y) \in \mathrm{G} \times \mathrm{G}$ qui commutent vérifie

$$\leq zn + (n-z)\frac{n}{2} = \frac{zn}{2} + \frac{n^2}{2} \leq \frac{n^2}{8} + \frac{n^2}{2} = \frac{5}{8}n^2.$$

Il reste à diviser par $|\mathrm{G} \times \mathrm{G}| = n^2$ pour obtenir que la probabilité est $\leq \frac{5}{8}$.

Exercice 233

Soient G_1, G_2, …, G_n des groupes cycliques d'ordres respectifs α_1, α_2, …, α_n. Posons $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2 \times \ldots \times \mathrm{G}_n$.

a) Pour tout i, soit x_i un élément de G_i d'ordre β_i. Montrer que $x = (x_1, x_2, \ldots, x_n)$ est d'ordre $\mathrm{ppcm}(\beta_1, \beta_2, \ldots, \beta_n)$ dans G.

b) Donner une condition nécessaire et suffisante portant sur les α_i pour que le groupe G soit cyclique.

Éléments de réponse 233

a) Pour $1 \leq i \leq n$ notons e_i l'élément neutre de G_i de sorte que $e = (e_1, e_2, \ldots, e_n)$ est l'élément neutre de G. Nous avons

$$x^p = e \iff \forall\, i \quad x_i^p = e_i \iff \forall\, i \quad \beta_i \text{ divise } p.$$

Le plus petit entier naturel non nul p tel que $x^p = e$ est donc le plus petit multiple commun aux β_i.

b) Montrons la condition nécessaire et suffisante : le groupe G est cyclique si et seulement si les α_i sont premiers entre eux deux à deux.

Condition nécessaire. Soit $x = (x_1, x_2, \ldots, x_n)$ engendrant G. Pour tout i, x_i engendre G_i donc est d'ordre α_i. D'après a) l'ordre de x est $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Comme x engendre G son ordre est aussi $|\mathrm{G}| = \alpha_1\alpha_2 \ldots \alpha_n$. Ainsi $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1\alpha_2 \ldots \alpha_n$ ce qui entraîne que les α_i sont premiers entre eux deux à deux.

Condition suffisante. Pour tout i, considérons $x_i \in \mathrm{G}_i$ d'ordre α_i (x_i existe puisque G_i est cyclique par hypothèse). D'après a) $x = (x_1, x_2, \ldots, x_n)$ est d'ordre $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ dans G et ce dernier terme est égal à $\alpha_1\alpha_2 \ldots \alpha_n = |\mathrm{G}|$ puisque les α_i sont premiers entre eux deux à deux. Finalement $\mathrm{G} = \langle x \rangle$ est cyclique.

Exercice 234

Déterminer tous les morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Éléments de réponse 234

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. L'image de f est un sous-groupe de $\mathbb{Z}$, c'est-à-dire un certain $n\mathbb{Z}$, $n \in \mathbb{N}$.

◇ Si $n \geq 1$, on choisit un antécédent x de n. Nous obtenons alors $2f\left(\frac{x}{2}\right) = f\left(\frac{x}{2} + \frac{x}{2}\right) = f(x) = n$ et $\frac{n}{2} = f\left(\frac{x}{2}\right) \in n\mathbb{Z}$ ce qui est absurde.

$\diamond$ Si $n = 0$, alors f est le morphisme nul.

Ainsi un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est nul.

Exercice 235

Caractériser les groupes dont l'ensemble des sous-groupes est fini.

Éléments de réponse 235

Les groupes finis vérifient de manière évidente cette condition. Démontrons que ce sont les seuls. Soit G un groupe dont l'ensemble E des sous-groupes est fini. Tout élément x de G est d'ordre fini car un élément d'ordre infini engendre un sous-groupe isomorphe à $\mathbb{Z}$ et $\mathbb{Z}$ admet une infinité de sous-groupes. Si E' désigne le sous-ensemble de E formé des groupes monogènes nous avons $\mathrm{G} = \bigcup_{\mathrm{H} \in E'} \mathrm{H}$. Puisque E' est fini et que les éléments de E' sont des ensembles finis d'après ce qui précède G est fini.

Exercice 236

Montrer que pour tout $n \geq 1$ il existe un unique sous-groupe de $\left(\mathbb{Q}/\mathbb{Z}, +\right)$ d'ordre n.

Éléments de réponse 236

Soit $n \geq 1$. Soit G un sous-groupe d'ordre n de $\mathbb{Q}/\mathbb{Z}$. Si $x \in \mathbb{Q}$ est tel que $\overline{x}$ appartienne à G, l'ordre de $\overline{x}$ divise n et donc $\overline{nx} = n\overline{x} = \overline{0}$. Nous en déduisons qu'il existe $p \in \mathbb{Z}$ tel que $x = \frac{p}{n}$. Si r désigne le résidu de p modulo n, nous avons $\overline{x} = \overline{\left(\frac{r}{n}\right)}$. Ceci montre que

$$\mathrm{G} \subset \left\{ \overline{\left(\frac{r}{n}\right)} \,|\, 0 \leq r \leq n-1 \right\}.$$

Les n éléments de cet ensemble sont distincts et forment un sous-groupe de $\mathbb{Q}/\mathbb{Z}$, le sous-groupe engendré par $\overline{\left(\frac{1}{n}\right)}$. D'après ce qui précède c'est le seul sous-groupe de $\left(\mathbb{Q}/\mathbb{Z}, +\right)$ d'ordre n.

Exercice 237

Montrer que $(\mathbb{C}^n, +)$ est isomorphe à un sous-groupe de $\mathrm{GL}(n+1, \mathbb{C})$.

Éléments de réponse 237

Considérons l'ensemble des matrices de $\mathrm{M}(n+1, \mathbb{C})$ de la forme

$$A_X = \begin{pmatrix} 1 & X \\ 0_n & I_n \end{pmatrix}, X \in \mathbb{C}^n.$$

La matrice A_X est inversible. Un calcul par blocs assure que $A_X A_Y = A_{X+Y}$. Nous en déduisons que l'application

$$\mathbb{C}^n \to \mathrm{GL}(n+1, \mathbb{C}) \qquad\qquad X \mapsto A_X$$

définit un morphisme de $(\mathbb{C}^n, +)$ dans $\mathrm{GL}(n+1, \mathbb{C})$. Puisque ce morphisme est injectif, $(\mathbb{C}^n, +)$ est isomorphe à un sous-groupe de $\mathrm{GL}(n+1, \mathbb{C})$.

Exercice 238

Soit G un groupe et soit e son élément neutre. Supposons que tout élément x de G vérifie $x^2 = e$.

a) Montrer que G est un groupe abélien.

b) Si G est fini et non trivial, montrer qu'il existe un entier n tel que G soit isomorphe au groupe $\left(\mathbb{Z}/2\mathbb{Z}\right)^n$.

Éléments de réponse 238

a) Soit $x \in \mathrm{G}$. L'égalité $x^2 = e$ s'écrit aussi $x = x^{-1}$. Si x et y sont dans G nous avons donc $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

b) Soit $(x_1, x_2, \ldots, x_n)$ un système de générateurs minimal de G (un tel système existe car G est fini). Si $\overline{a} = \overline{b}$ dans $\mathbb{Z}/2\mathbb{Z}$ alors 2 divise $a - b$ autrement dit $a - b = 2\ell$ pour un certain $\ell \in \mathbb{Z}$; ainsi pour $x \in \mathrm{G}$ $x^{a-b} = x^{2\ell} = (x^2)^\ell = e^\ell = e$ soit $x^a = x^b$. Ceci permet d'affirmer que l'application

$$\varphi\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^n \to \mathrm{G}, \qquad (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \mapsto x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$$

est bien définie. Le groupe G étant abélien, φ est un morphisme de groupes et il est surjectif par définition d'un système de générateurs. Montrons que φ est injectif. Soit $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})$ un élément de $\ker\varphi$. S'il existe un entier i tel que $\overline{a_i} = \overline{1}$, par exemple $\overline{a_n} = \overline{1}$, l'égalité $x_1^{a_1} x_2^{a_2} \ldots x_n = e$ entraîne

$$x_n = x_n^{-1} = x_1^{a_1} x_2^{a_2} \ldots x_{n-1}^{a_{n-1}}.$$

Par suite $(x_1, x_2, \ldots, x_{n-1})$ est un système de générateurs de G : contradiction avec le fait que $(x_1, x_2, \ldots, x_n)$ est un système de générateurs minimal de G. Finalement $\ker\varphi = \{(\overline{0}, \overline{0}, \ldots, \overline{0})\}$ et φ est injectif. Il en résulte que φ est un isomorphisme entre G et $\left(\mathbb{Z}/2\mathbb{Z}\right)^n$.

1.6. Actions de groupes, sous-groupes distingués

Exercice 239

Soit G un groupe fini d'ordre pair $2n$ (avec $n \in \mathbb{N}^*$).

1. Soit H un sous-groupe de G d'ordre n. Montrer que H est distingué dans G.
2. Supposons qu'il existe deux sous-groupes H_1 et H_2 de G d'ordre n tels que $\mathrm{H}_1 \cap \mathrm{H}_2 = \{e\}$ où e désigne l'élément neutre de G. Montrer que $n = 1$ ou $n = 2$.

3. Supposons qu'il existe deux sous-groupes H_1 et H_2 de G distincts et tout deux d'ordre n. Montrer que $H = H_1 \cap H_2$ est un sous-groupe distingué dans G. En déduire que l'ordre de G est un multiple de 4.

Éléments de réponse 239

1. Il s'agit de montrer : $xH = Hx$ pour tout $x \in G$.
   - ◇ Si x appartient à H, on a $xH = Hx = H$.
   - ◇ Si x n'appartient pas à H, alors $xH \cap H = \emptyset$ (en effet si y appartient à $xH \cap H$, il existe $a \in H$ tel que $y = xa$ donc $x = ya^{-1} \in H$: absurde), c'est-à-dire $xH \subset G \setminus H$. Or xH et $G \setminus H$ sont de cardinal n, donc $xH = G \setminus H$. On montre de même que $Hx = G \setminus H$ donc $xH = Hx$.
2. Puisque
$$\mathrm{Card}(H_1 \cup H_2) = |H_1| + |H_2| - \mathrm{Card}(H_1 \cap H_2) = 2n - 1$$
il existe $\alpha \in G$, $\alpha \notin H_1$, $\alpha \notin H_2$ tel que $G = H_1 \cup H_2 \cup \{\alpha\}$.

   Si $n = 1$ c'est terminé.

   Si $n \geq 2$, on remarque que
$$\forall\, (x, y) \in (H_1 \setminus \{e\}) \times (H_2 \setminus \{e\}) \qquad xy = \alpha$$
(En effet si xy appartient à H_1 alors y appartient à $x^{-1}H_1 = H_1$ donc y appartient à $H_1 \cap H_2 = \{e\}$, *i.e.* $y = e$: contradiction. De même xy n'appartient pas à H_2.) Ceci n'est possible que si
$$\mathrm{Card}(H_1 \setminus \{e\}) = \mathrm{Card}(H_2 \setminus \{e\}) = 1,$$
i.e. $n = 2$.
3. D'après a) H_1 et H_2 sont distingués dans G. Par conséquent pour tout $x \in G$ nous avons
$$xH = xH_1 \cap xH_2 = H_1x \cap H_2x = Hx$$
ce qui prouve que H est distingué dans G.

   Notons π la surjection canonique de G dans le groupe quotient G/H. Puisque H est un sous-groupe de H_1, $\pi(H_1) = H_1/H$ est d'ordre $\frac{|H_1|}{|H|} = \frac{n}{|H|}$. De même $\pi(H_2) = H_2/H$ est d'ordre $\frac{n}{|H|}$. Or
$$H_1/H \cap H_2/H = H_1 \cap H_2/H$$
est réduit à l'élément neutre de G/H. Le groupe quotient G/H étant d'ordre $\frac{2n}{|H|}$, on peut appliquer b) à G/H, H_1/H et H_2/H ce qui donne $\frac{n}{|H|} \in \{1, 2\}$. Puisque $H_1 \neq H_2$ nous avons $|H| = |H_1 \cap H_2| < n$ donc $\frac{n}{|H|} = 2$. Finalement $|G| = 2n = 4|H|$.

Exercice 240

Soit $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ ac \neq 0 \right\}$.

1. Montrer que G est un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$.
2. Montrer que
$$\mathrm{G}\times\mathbb{R}\to\mathbb{R}, \qquad \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, x\right) \mapsto \frac{ax+b}{c}$$
définit une action du groupe G sur $\mathbb{R}$.
3. Déterminer l'orbite de 0 pour cette action.
4. Déterminer le stabilisateur de 0 pour cette action.
5. L'action de G sur $\mathbb{R}$ est-elle transitive ?

Éléments de réponse 240

1. Remarquons que la matrice identité appartient à G (il suffit de prendre $a=c=1$, $b=0$).
Soient $M = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ et $N = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ deux éléments de G. Alors $N^{-1} = \begin{pmatrix} \frac{1}{\alpha} & -\frac{\gamma}{\alpha\beta} \\ 0 & \frac{1}{\gamma} \end{pmatrix}$ appartient à G et $MN^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \frac{1}{\alpha} & -\frac{\gamma}{\alpha\beta} \\ 0 & \frac{1}{\gamma} \end{pmatrix} = \begin{pmatrix} \frac{a}{\alpha} & \frac{b\alpha\beta-a\gamma^2}{\alpha\beta\gamma} \\ 0 & \frac{c}{\gamma} \end{pmatrix}$ appartient aussi à G.
2. Montrons que
$$\mathrm{G}\times\mathbb{R}\to\mathbb{R}, \qquad \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, x\right) \mapsto \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot x = \frac{ax+b}{c}$$
définit une action du groupe G sur $\mathbb{R}$.
Pour tout x dans $\mathbb{R}$ nous avons
$$\mathrm{Id}\cdot x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\cdot x = \frac{1\times x+0}{1} = x.$$
Pour tous $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ dans G et pour tout réel x nous avons d'une part
$$\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\right)\cdot x = \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\right)\cdot x = \begin{pmatrix} a\alpha & a\beta+b\gamma \\ 0 & c\gamma \end{pmatrix}\cdot x = \frac{a\alpha x+a\beta+b\gamma}{c\gamma}$$
et d'autre part
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot\left(\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\cdot x\right) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot\frac{\alpha x+\beta}{\gamma} = \frac{a\times\frac{\alpha x+\beta}{\gamma}+b}{c} = \frac{a\alpha x+a\beta+b\gamma}{c\gamma}.$$
En particulier, pour tous $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ dans G et pour tout réel x nous avons
$$\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\right)\cdot x = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot\left(\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\cdot x\right).$$

3. L'orbite de 0 sous l'action de G sur $\mathbb{R}$ est
$$\mathcal{O}_0 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot 0 \,\middle|\, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{G} \right\} = \left\{ \frac{a \times 0 + b}{c} \,\middle|\, a, c \in \mathbb{R}^\times, b \in \mathbb{R} \right\} = \left\{ \frac{b}{c} \,\middle|\, c \in \mathbb{R}^\times, b \in \mathbb{R} \right\} = \mathbb{R}.$$
4. Le stabilisateur de 0 pour cette action est
$$\begin{aligned} \mathrm{St}_\mathrm{G}(0) &= \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{G} \,\middle|\, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot 0 = 0 \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{G} \,\middle|\, \frac{a \times 0 + b}{c} = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{G} \,\middle|\, b = 0 \right\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^\times \right\} \end{aligned}$$
5. L'action de G sur $\mathbb{R}$ est transitive car $\mathcal{O}_0 = \mathbb{R}$.

Exercice 241

Soit $E \subset \mathfrak{S}_4$ l'ensemble des produits de deux transpositions à supports disjoints
$$E = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$
Le groupe $\mathfrak{S}_4$ agit par conjugaison sur E.

1. En déduire l'existence d'un morphisme de groupes $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$.
2. Montrer que φ est surjectif.
3. Quel est le noyau de φ ?

   Soit N le sous-groupe de $\mathfrak{S}_4$ engendré par les éléments de E.
4. Quel est l'ordre de N ?
5. Montrer que N est un sous-groupe distingué de $\mathfrak{S}_4$.
6. a) Montrer que $\mathrm{H} = \langle (1\ 2)(3\ 4) \rangle$ est un sous-groupe distingué de N.

   b) Le groupe H est-il distingué dans $\mathfrak{S}_4$?
7. Montrer que $\mathfrak{S}_4 / \mathrm{N}$ est isomorphe à $\mathfrak{S}_3$.

Éléments de réponse 241

1. Se donner une action de groupe de $\mathfrak{S}_4$ sur E revient à se donner un morphisme de groupes de $\mathfrak{S}_4$ dans $\mathfrak{S}_E$. Or $\#E = 3$ donc $\mathfrak{S}_E \simeq \mathfrak{S}_3$ et l'action de groupe de $\mathfrak{S}_4$ sur E définit un morphisme de groupes $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$.
2. L'action de $\mathfrak{S}_4$ sur E par conjugaison est
$$\mathfrak{S}_4 \times E \to E, \qquad (\sigma, \tau) \mapsto \sigma \cdot \tau = \sigma\tau\sigma^{-1}.$$
   On en déduit que φ est le morphisme
$$\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_E, \qquad \sigma \mapsto \varphi(\sigma)\colon E \to E,\ \tau \mapsto \sigma\tau\sigma^{-1}$$

ou encore

$$\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3, \qquad \sigma \mapsto \varphi(\sigma)\colon \{1,2,3\} \to \{1,2,3\}, \quad \tau_i \mapsto \tau_{\varphi(\sigma)(i)}$$

où $E = \{\tau_1, \tau_2, \tau_3\}$ avec

$$\tau_1 = (1\ 2)(3\ 4), \qquad \tau_2 = (1\ 3)(2\ 4), \qquad \tau_3 = (1\ 4)(2\ 3)$$

Les deux transpositions (1 2) et (1 3) engendrent $\mathfrak{S}_3$; il suffit donc de montrer qu'elles sont dans $\operatorname{im}\varphi$ pour montrer que φ est surjective. Remarquons que $(1\ 2\ 4)\tau_1(1\ 2\ 4)^{-1} = \tau_2$, *i.e.* (1 2) appartient à $\operatorname{im}\varphi$. Notons que $(1\ 2\ 3\ 4)\tau_1(1\ 2\ 3\ 4)^{-1} = \tau_3$, *i.e.* (1 3) appartient à $\operatorname{im}\varphi$. Nous en déduisons que φ est surjective.

3. Le noyau de φ est $\ker\varphi = \bigcap_{x\in E} \mathrm{St}_{\mathfrak{S}_4}(x)$. Or pour tout $1 \leq i \leq 3$

$$\mathrm{St}_{\mathfrak{S}_4}(\tau_i) = \{\sigma \in \mathfrak{S}_4 \,|\, \sigma\cdot\tau_i = \tau_i\} = \{\sigma \in \mathfrak{S}_4 \,|\, \sigma\tau_i\sigma^{-1} = \tau_i\} = \{\mathrm{id}, \tau_1, \tau_2, \tau_3\}$$

d'où $\ker\varphi = \{\mathrm{id}, \tau_1, \tau_2, \tau_3\}$.

4. Le groupe N est engendré par les trois éléments d'ordre 2

$$\tau_1 = (1\ 2)(3\ 4), \qquad \tau_2 = (1\ 3)(2\ 4), \qquad \tau_3 = (1\ 4)(2\ 3)$$

Remarquons que si i, j sont deux éléments distints de $\{1, 2, 3\}$, alors $\tau_i\tau_j = \tau_k$ avec $k \neq i$, $k \neq j$. Par suite $\mathrm{N} = \{\mathrm{id}, \tau_1, \tau_2, \tau_3\}$. En particulier, il est d'ordre 4.

5. D'après 3. et 4. $\ker\varphi = \mathrm{N}$; il en résulte que N est un sous-groupe distingué de $\mathfrak{S}_4$.

6. a) Le sous-groupe H est d'indice 2 dans N ; il s'en suit que H est un sous-groupe distingué de N.

   b) Le groupe H n'est pas distingué dans $\mathfrak{S}_4$; en effet

$$(1\ 2\ 4)\underbrace{(1\ 2)(3\ 4)}_{\in \mathrm{H}}(1\ 2\ 4)^{-1} = (1\ 3)(2\ 4) \notin \mathrm{H}.$$

7. Puisque $\ker\varphi = \mathrm{N}$ et φ est surjectif, φ réalise un isomorphisme entre $\mathfrak{S}_4/\mathrm{N}$ et $\mathfrak{S}_3$.

Exercice 242

Soit G un groupe fini. Soit p le plus petit facteur premier de $|\mathrm{G}|$. Soit H un sous-groupe de G d'ordre p distingué dans G. En faisant agir G sur H par conjugaison montrer que H est contenu dans le centre de G.

Éléments de réponse 242

Puisque H est distingué dans G l'application

$$\mathrm{G}\times\mathrm{H} \to \mathrm{H}, \qquad (g,h) \mapsto ghg^{-1}$$

définit une action du groupe G sur l'ensemble H. Puisque $|\mathrm{H}| \geq 2$ il existe $h \in \mathrm{H} \smallsetminus \{e\}$. Soit $\mathcal{O}_h$ l'orbite de h. D'une part $|\mathcal{O}_h|$ divise $|\mathrm{G}|$ (car $\mathcal{O}_h$ est en bijection avec ${}^{\mathrm{G}}\!/_{\mathrm{St}(h)}$ d'où $\#\mathcal{O}_h = \left|{}^{\mathrm{G}}\!/_{\mathrm{St}(h)}\right|$ et $\#\mathcal{O}_h|\mathrm{St}(h)| = |\mathrm{G}|$) et d'autre part H étant réunion des orbites nous avons $|\mathcal{O}_h| \leq |\mathrm{H}| = p$. Si $|\mathcal{O}_h| > 1$, alors p étant le plus petit diviseur de $|\mathrm{G}|$ distinct de 1, nous avons $|\mathcal{O}_h| \geq p$; par suite $|\mathcal{O}_h| = |\mathrm{H}|$. Il en résulte que $\mathcal{O}_h = \mathrm{H}$. En particulier, e appartient à $\mathcal{O}_h$ et donc $h = e$: contradiction. Ainsi toutes les orbites sont des singletons, donc si (g, h) appartient à $\mathrm{G} \times \mathrm{H} \to \mathrm{H}$ alors $ghg^{-1} = h$, *i.e.* $gh = hg$ et $\mathrm{H} \subset Z(\mathrm{G})$.

Exercice 243

Soient $\Bbbk$ un corps et $\mathrm{G} \subset \mathrm{GL}(2, \Bbbk)$ le sous-groupe des matrices 2×2 triangulaires supérieures. Déterminer si chacune des conditions suivantes définit un sous-groupe distingué de G, et si oui, utiliser le théorème d'isomorphisme pour identifier le quotient :

(i) $a_{11} = 1$;

(ii) $a_{12} = 0$;

(iii) $a_{11} = a_{22}$;

(iv) $a_{11} = a_{22} = 1$.

Éléments de réponse 243

Le groupe G est

$$\mathrm{G} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \,\middle|\, a_{11},\, a_{22} \in \Bbbk^*,\, a_{12} \in \Bbbk \right\}$$

La loi de composition sur G est :

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} \tag{1.6.1}$$

(i) Le sous-groupe défini par la condition $a_{11} = 1$ est

$$\mathrm{K} = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \,\middle|\, b \in \Bbbk,\, c \in \Bbbk^* \right\}$$

Posons

$$\varphi \colon \mathrm{G} \to \Bbbk^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

La relation (1.6.1) assure que φ est un morphisme, et on constate que $\mathrm{K} = \ker \varphi$; en particulier K est distingué dans G. De plus φ est surjectif, car étant donné $a \in \Bbbk^*$ la matrice $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ est un antécédent de a par φ. Le théorème d'isomorphisme permet de conclure que le quotient ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ est isomorphe à $\Bbbk^*$.

Remarque : on peut vérifier directement avec la définition que K est distingué dans G (c'est-à-dire vérifier que pour toutes matrices $A \in \mathrm{K}$ et $B \in \mathrm{G}$ on a $BAB^{-1} \in \mathrm{K}$) ; ceci étant il faut identifier K à un noyau pour utiliser le théorème d'isomorphisme...

On peut chercher à voir s'il existe un sous-groupe H de G tel que $\mathrm{G} = \mathrm{K} \rtimes \mathrm{H}$. Posons

$$\mathrm{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \Bbbk^* \right\}$$

On voit que $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et $\mathrm{KH} = \mathrm{G}$ (à nouveau par (1.6.1)) dont H convient.

Remarquons que H n'est pas uniquement déterminé ; par exemple

$$\mathrm{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in \Bbbk^* \right\}$$

convient aussi.

En fait il y a une infinité d'autres choix possibles pour H.

(ii) Le sous-groupe défini par la condition $a_{12} = 0$ est

$$\mathrm{K} = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \,\middle|\, a,\, c \in \Bbbk^* \right\}.$$

Si $\Bbbk \neq \mathbb{F}_2$, alors ce groupe n'est pas distingué dans G : pour tout $b \neq 0$ et $a \neq c$ nous avons

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b(c-a) \\ 0 & c \end{pmatrix} \notin \mathrm{K}.$$

Si $\Bbbk = \mathbb{F}_2$, alors on ne peut pas choisir deux éléments $a \neq c$ dans $\Bbbk^*$, et donc le contre-exemple ne tient plus. Dans ce cas le groupe K est trivial, donc en particulier distingué dans G...

(iii) Le sous-groupe défini par la condition $a_{11} = a_{22}$ est

$$\mathrm{K} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \,\middle|\, a \in \Bbbk^*,\, b \in \Bbbk \right\}.$$

Posons

$$\varphi \colon \mathrm{G} \to \Bbbk^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \frac{a}{c}$$

La relation (1.6.1) montre que φ est un morphisme, et donc $\mathrm{K} = \ker \varphi$ est distingué dans G. De plus φ est surjectif, donc le théorème d'isomorphisme permet de conclure que le quotient G/K est isomorphe à $\Bbbk^*$.

Notons que $\mathrm{G} = \mathrm{K} \rtimes \mathrm{H}$ pour le choix suivant de sous-groupe H :

$$\mathrm{K} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \Bbbk^* \right\}.$$

À noter qu'il y a une infinité d'autres choix possibles pour H.

(iv) Le sous-groupe défini par la condition $a_{11} = a_{22} = 1$ est

$$\mathrm{K} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \right\}$$

Posons

$$\varphi \colon \mathrm{G} \to \Bbbk^* \times \Bbbk^*, \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

De nouveau la relation (1.6.1) assure que φ est un morphisme surjectif, donc $\mathrm{K} = \ker \varphi$ est distingué ; d'après le théorème d'isomorphisme le quotient G/K est isomorphe à $\Bbbk^* \times \Bbbk^*$.

Notons que $\mathrm{G} = \mathrm{K} \rtimes \mathrm{H}$ par exemple pour le choix suivant de sous-groupe H :

$$\mathrm{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a,\, c \in \Bbbk^* \right\}$$

À noter qu'il y a une infinité d'autres choix possibles pour H.

Les exemples dans cet exercice peuvent donner la fausse idée que dès que $\mathrm{K} \subset \mathrm{G}$ est un sous-groupe distingué, il existe un sous-groupe $\mathrm{H} \subset \mathrm{G}$ tel que . C'est faux ; considérer par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ et $\mathrm{K} = \{\overline{0}, \overline{2}\}$ et se convaincre qu'un tel H n'existe pas dans ce cas...

Exercice 244

Soit G un groupe fini.

1. On définit l'application suivante

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x = gxg^{-1}$$

Montrer qu'il s'agit d'une action du groupe G sur lui-même.

2. Lorsqu'un groupe G agit sur un ensemble X on appelle *points fixes* les éléments de X qui sont invariants sous l'action de G. Ils forment l'ensemble $\{x \in X \mid g \cdot x = x \quad \forall\, g \in \mathrm{G}\}$.

Décrire les points fixes de l'action par conjugaison d'un groupe G sur lui-même.

3. Dans le cas $\mathrm{G} = \mathfrak{S}_4$ décrire les orbites et les stabilisateurs.

Éléments de réponse 244

Soit G un groupe fini.

1. On définit l'application suivante

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x = gxg^{-1}.$$

Montrons qu'il s'agit d'une action du groupe G sur lui-même.

Le neutre agit trivialement :

$$e \cdot x = exe^{-1} = exe = x.$$

Pour tous g_1, g_2, x dans G nous avons

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) \cdot x.$$

2. Lorsqu'un groupe G agit sur un ensemble X on appelle *points fixes* les éléments de X qui sont invariants sous l'action de G. Ils forment l'ensemble $\{x \in X \,|\, g \cdot x = x \quad \forall\, g \in \mathrm{G}\}$.

   Un élément $x \in \mathrm{G}$ est un point fixe si et seulement si pour tout $g \in \mathrm{G}$ $g \cdot x = x$. Or $g \cdot x = x$ se réécrit $gxg^{-1} = x$ ou encore $gx = xg$. Les points fixes pour l'action par conjugaison d'un groupe sur lui-même sont donc les éléments qui commutent avec tous les autres, c'est-à-dire les éléments du centre de G.

3. Supposons $\mathrm{G} = \mathfrak{S}_4$.

   Rappelons que $\mathfrak{S}_4$ compte $24 = 4!$ éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

   Les différentes orbites sont

   - $\mathcal{O}_{\mathrm{id}} = \{g \cdot \mathrm{id} \,|\, g \in \mathrm{G}\} = \{g\mathrm{id}g^{-1} \,|\, g \in \mathrm{G}\} = \{\mathrm{id} \,|\, g \in \mathrm{G}\} = \{\mathrm{id}\}$;
   - $\mathcal{O}_{(1\ 2)} = \{g \cdot (1\ 2) \,|\, g \in \mathrm{G}\} = \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\}$;
   - $\mathcal{O}_{(1\ 2)(3\ 4)} = \{g \cdot (1\ 2)(3\ 4) \,|\, g \in \mathrm{G}\} = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$;
   - $\mathcal{O}_{(1\ 2\ 3)} = \{g \cdot (1\ 2\ 3) \,|\, g \in \mathrm{G}\} = \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2\ 4),\ (1\ 4\ 2)\}$;

◇ $\mathcal{O}_{(1\ 2\ 3\ 4)} = \{g\cdot(1\ 2\ 3\ 4)\,|\,g\in \mathrm{G}\} = \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}$.

Les stabilisateurs correspondants sont

◇ $\mathrm{St}(\mathrm{id}) = \{g\in \mathrm{G}\,|\,g\cdot \mathrm{id} = \mathrm{id}\} = \{g\in \mathrm{G}\,|\,g\mathrm{id}g^{-1} = \mathrm{id}\} = \mathrm{G}$

◇ $\mathrm{St}((1\ 2)) = \{g\in \mathrm{G}\,|\,g\cdot(1\ 2) = (1\ 2)\} = \{g\in \mathrm{G}\,|\,g(1\ 2)g^{-1} = (1\ 2)\} = \{g\in \mathrm{G}\,|\,g(1\ 2) = (1\ 2)g\} = \{\mathrm{id},\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$

◇ $\mathrm{St}((1\ 2)(3\ 4)) = \{g\in \mathrm{G}\,|\,g\cdot(1\ 2)(3\ 4) = (1\ 2)(3\ 4)\} = \{g\in \mathrm{G}\,|\,g(1\ 2)(3\ 4)g^{-1} = (1\ 2)(3\ 4)\} = \{g\in \mathrm{G}\,|\,g(1\ 2)(3\ 4) = (1\ 2)(3\ 4)g\} = \{\mathrm{id},\ (12),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3$

◇ $\mathrm{St}((1\ 2\ 3)) = \{g\in \mathrm{G}\,|\,g\cdot(1\ 2\ 3) = (1\ 2\ 3)\} = \{g\in \mathrm{G}\,|\,g(1\ 2\ 3)g^{-1} = (1\ 2\ 3)\} = \{g\in \mathrm{G}\,|\,g(1\ 2\ 3) = (1\ 2\ 3)g\} = \{\mathrm{id},\ (1\ 2\ 3),\ (1\ 3\ 2)\}$

◇ $\mathrm{St}((1\ 2\ 3\ 4)) = \{g\in \mathrm{G}\,|\,g\cdot(1\ 2\ 3\ 4) = (1\ 2\ 3\ 4)\} = \{g\in \mathrm{G}\,|\,g(1\ 2\ 3\ 4)g^{-1} = (1\ 2\ 3\ 4)\} = \{g\in \mathrm{G}\,|\,g(1\ 2\ 3\ 4) = (1\ 2\ 3\ 4)g\} = \{\mathrm{id},\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2)\}$

Notons que dans chaque cas nous avons $|\mathrm{G}| = |\mathrm{St}(x)|\times|\mathcal{O}_x|$.

Exercice 245

Soit G un sous-groupe de $\mathfrak{S}_4$ agissant sur $\{1, 2, 3, 4\}$ par l'action naturelle de $\mathfrak{S}_4$. Pour $1\leq i\leq 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i. Déterminer $\mathcal{O}_i$ et S_i pour les cas suivants :

◇ G est le groupe engendré par le 3-cycle (1 2 3).

◇ G est le groupe engendré par le 4-cycle (1 2 3 4).

◇ G est le groupe engendré par les double transpositions.

◇ $\mathrm{G} = \mathcal{A}_4$.

Éléments de réponse 245

◇ Par symétrie il suffit d'étudier les cas $i = 1$ et $i = 4$.

Pour $i = 4$ c'est plus facile car aucun élément de G ne modifie 4. Ainsi $\mathcal{O}_4 = \{4\}$ et $S_4 = \mathrm{G}$.

Ensuite si $s = (1\ 2\ 3)$, alors $s(1) = 2$ et $s\circ s(1) = 3$ d'où

$$\mathcal{O}_1 = \{g\cdot 1\,|\,g\in \mathrm{G}\} = \{g(1)\,|\,g\in \mathrm{G}\} = \{\mathrm{id}(1),\ s(1),\ s\circ s(1)\} = \{1, 2, 3\}.$$

Puisque $\mathrm{G} = \{\mathrm{id}, s, s^2\}$ nous obtenons que

$$S_1 = \{g\in \mathrm{G}\,|\,g\cdot 1 = 1\} = \{g\in \mathrm{G}\,|\,g(1) = 1\} = \{\mathrm{id}\}$$

◇ Par symétrie il suffit d'étudier le cas $i = 1$. Par un raisonnement analogue au précédent nous constatons que

$$S_1 = \{g\in \mathrm{G}\,|\,g\cdot 1 = 1\} = \{g\in \mathrm{G}\,|\,g(1) = 1\} = \{\mathrm{id}\}$$

et

$$\mathcal{O}_1 = \{g\cdot 1\,|\,g\in \mathrm{G}\} = \{g(1)\,|\,g\in \mathrm{G}\} = \{1, 2, 3, 4\}.$$

En effet si $s = (1\ 2\ 3\ 4)$, alors $\mathrm{G} = \{\mathrm{id}, s, s^2, s^3\}$.

◇ Par symétrie il suffit d'étudier le cas $i = 1$.

Le produit de deux double transpositions est ou bien l'identité, ou bien une double transposition. Une double transposition ne fixe aucun élément de $\{1, 2, 3, 4\}$ et on peut trouver une double transposition qui envoie 1 sur n'importe quel élément de $\{2, 3, 4\}$. En résumé nous avons

$$\mathcal{O}_1 = \{1, 2, 3, 4\} \qquad\qquad S_1 = \{\mathrm{id}\}.$$

◇ Par symétrie il suffit d'étudier le cas $i = 1$.

Les éléments de $\mathcal{A}_4$ sont l'identité, les double transpositions et les 3-cycles. D'après la question précédente $\mathcal{O}_1 = \{1, 2, 3, 4\}$ puisque l'orbite de 1 par $\mathcal{A}_4$ contient au moins l'orbite de 1 par les double transpositions. Déterminons maintenant le stabilisateur de 1. Une double transposition ne peut pas être dans le stabilisateur de 1. D'après la première question les 3-cycles qui stabilisent 1 sont ceux qui n'ont pas 1 dans leur support, on a donc $S_1 = \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}$.

Exercice 246

Soit G un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$. On fait agir G sur le plan affine euclidien en choisissant un point O de cet espace et en identifiant $\mathbb{R}^2$ et les vecteurs d'origine O. Décrire l'orbite d'un point A quand G est le sous-groupe engendré par

◇ une symétrie s par rapport à une droite D passant par O ;

◇ une rotation d'angle $\frac{\pi}{2}$ de centre O ;

◇ une rotation d'angle $\frac{2\pi}{n}$, $n \in \mathbb{N}^*$, de centre O et une symétrie s par rapport à une droite D passant par O.

Éléments de réponse 246

◇ Puisque $s = s^{-1}$ nous avons $\mathrm{G} = \{\mathrm{id}, s\}$ et l'orbite de A est constituée de A et de son image par la symétrie (ces deux points sont confondus si et seulement si $A = O$) :

$$\mathcal{O}_A = \{g \cdot A \,|\, g \in \mathrm{G}\} = \{g(A) \,|\, g \in \mathrm{G}\} = \{\mathrm{id}(A)\} \cup \{s(A)\} = \{A, s(A)\}.$$

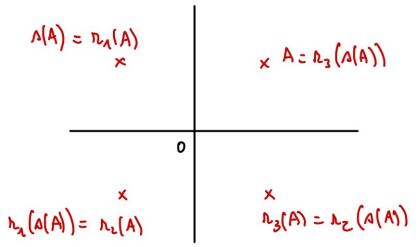
◇ Le groupe engendré par cette rotation est le groupe des rotations d'angle $\frac{k\pi}{2}$ avec $0 \leq k \leq 3$. Ainsi l'orbite du point A est constituée des sommets du carré de centre O et dont un des sommets est A :

$$\mathcal{O}_A = \{g \cdot A \,|\, g \in \mathrm{G}\} = \{g(A) \,|\, g \in \mathrm{G}\} = \{A, r_{\pi/2}(A), r_\pi(A), r_{3\pi/2}(A)\}$$

où r_α désigne la rotation de centre O et d'angle α.

◇ Notons r_k la rotation d'angle $\frac{2k\pi}{n}$. Alors le groupe G est constitué des éléments r_k et $r_k \circ s$. L'orbite de A est donc constituée des n sommets du polygone régulier de centre O dont un des sommets est A et par leurs symétriques par rapport à la droite D.

Notons que ces $2n$ points ne sont plus que n points quand la droite passe par un des sommets ou est la médiatrice d'un des côtés du polygone. C'est en effet par exemple le cas dans la situation suivante :



n = 4 et s symétrie par rapport à l'axe des ordonnées

Exercice 247

Soit $n \geq 3$ un entier. Considérons les matrices suivantes de $\mathrm{GL}(2,\mathbb{R})$

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \tau = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

Notons G le sous-groupe de $\mathrm{GL}(2,\mathbb{R})$ engendré par σ et τ ; désignons par H le sous-groupe de G engendré par σ et K le sous-groupe de G engendré par τ :

$$\mathrm{G} = \langle \sigma, \tau \rangle, \qquad \mathrm{H} = \langle \sigma \rangle, \qquad \mathrm{K} = \langle \tau \rangle.$$

1. Donner l'ordre de σ.
2. Donner une interprétation géométrique de τ et donner son ordre.
3. Si G est d'ordre fini, que peut-on dire sur son ordre ?
4. Montrer que $\sigma\tau = \tau^{n-1}\sigma$.
5. Donner tous les éléments de H, K et G.
6. Combien y a-t-il de classes à gauche de G modulo H ?
7. Décrire l'ensemble quotient G/H.
8. A-t-on $\mathrm{H} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient G/H.
9. A-t-on $\mathrm{K} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient G/K.
10. Le sous-ensemble $\mathrm{K}' = \{g \in \mathrm{G} \mid \det g = 1\}$ de G est-il un sous-groupe de G ? Si oui, a-t-on $\mathrm{K}' \triangleleft \mathrm{G}$?
11. Comparer K et K′.
12. Existe-t-il un sous-groupe de G isomorphe à G/K ?

13. Calculer $D(\mathrm{G})$. À quel groupe est isomorphe $\mathrm{G}/D(\mathrm{G})$?
14. Montrer que la multiplication des matrices définit une action

$$\mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX$$

15. L'action est-elle transitive ?
16. L'action est-elle fidèle ?
17. Quels sont les points fixes de l'action ?
18. Quel est le stabilisateur G_{v_0} du vecteur $v_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$?
19. Décrire l'orbite du vecteur $v_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
20. Définissons les vecteurs v_0 et Y_0 de $\mathbb{R}^2$ par

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad Y_0 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

Quel est le stabilisateur G_S du segment $S = [v_0, Y_0]$?

Éléments de réponse 247

1. Donnons l'ordre de σ.

   Nous avons $\sigma \neq \mathrm{id}$ mais $\sigma^2 = \mathrm{id}$ donc σ est d'ordre 2.

2. On voit que τ est la rotation de centre $O = (0, 0)$ et d'angle $\frac{2\pi}{n}$. En particulier τ est d'ordre n. On peut de plus déterminer τ^k :

$$\tau^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$

3. Supposons que G est d'ordre fini. Le groupe $\mathrm{H} = \langle\sigma\rangle$ est un sous-groupe d'ordre 2 (rappelons que σ est d'après la question 1. d'ordre 2) de G.

   Le groupe $\mathrm{K} = \langle\tau\rangle$ est un sous-groupe d'ordre n (rappelons que τ est d'après la question 2. d'ordre n) de G.

   D'après le Théorème de Lagrange, l'ordre de G est divisible d'une part par 2 et d'autre part par n, donc par $\mathrm{ppcm}(2, n)$.

4. Montrons que $\sigma\tau = \tau^{n-1}\sigma$. Un calcul direct assure que $\tau\sigma\tau = \sigma$:

$$\begin{aligned}
\tau\sigma\tau &= \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & -\cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\left(\frac{2\pi}{n}\right) + \sin^2\left(\frac{2\pi}{n}\right) & 0 \\ 0 & -\left(\cos^2\left(\frac{2\pi}{n}\right) + \sin^2\left(\frac{2\pi}{n}\right)\right) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
&= \sigma
\end{aligned}$$

   On en déduit, en multipliant à gauche par τ^{n-1} que $\sigma\tau = \tau^{n-1}\sigma$ (rappelons que τ est d'ordre n).

5. Donnons tous les éléments de G, H et K.

   Puisque σ est d'ordre 2, nous avons $\mathrm{H} = \{\mathrm{id}, \sigma\}$.

   Comme τ est d'ordre n, nous avons $\mathrm{K} = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}\}$.

   Nous avons $\mathrm{G} = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}, \sigma, \tau\sigma, \tau^2\sigma, \ldots, \tau^{n-1}\sigma\}$. En effet, remarquons qu'un élément de G s'écrit

$$\sigma^{j_1}\tau^{i_1}\sigma^{j_2}\tau^{i_2}\sigma\ldots\sigma^{j_k}\tau^{i_k}$$

   avec j_ℓ, i_ℓ dans $\mathbb{Z}$. Effectuons la division euclidienne de j_ℓ par 2 : il existe q_ℓ, r_ℓ tels que $j_\ell = 2q_\ell + r_\ell$ avec $0 \leq r_\ell \leq 1$. Alors $\sigma^{j_\ell} = \sigma^{2q_\ell + r_\ell} = (\sigma^2)^{q_\ell}\sigma^{r_\ell} = \sigma^{r_\ell}$. De même effectuons la division euclidienne de i_ℓ par n : il existe q'_ℓ, r'_ℓ tels que $i_\ell = nq'_\ell + r'_\ell$ avec $0 \leq r'_\ell \leq n-1$. Alors $\tau^{i_\ell} = \tau^{nq'_\ell + r'_\ell} = (\tau^n)^{q'_\ell}\tau^{r'_\ell} = \tau^{r'_\ell}$. Ainsi un élément de G s'écrit

$$\sigma^{r_1}\tau^{r'_1}\sigma^{r_2}\tau^{r'_2}\sigma\ldots\sigma^{r_k}\tau^{r'_k}$$

   avec $r'_\ell \in \{0, 1, \ldots, n-1\}$ et $r_\ell \in \{0, 1\}$. Si $r_\ell = 0$, alors on remplace $\tau^{r'_\ell}\tau^{r'_{\ell+1}}$ par τ_{k_ℓ}. Autrement dit un élément de G est de l'une des quatre formes suivantes :

$$\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}, \qquad \tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$$
$$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}, \qquad \sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma$$

   Montrons par exemple par récurrence qu'un élément de la forme $(\sigma)\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}(\sigma)$ avec k pair est de la forme τ^ℓ ou $\tau^\ell\sigma$:

   a) commençons par considérer un élément de la forme $\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair. Montrons par récurrence sur k qu'il s'écrit aussi τ^κ pour un certain κ. C'est vrai pour $k = 2$, en effet

$$\underbrace{\sigma\tau^{i_1}}_{\tau^{i_1(n-1)}\sigma}\ \sigma\tau^{i_2} = \tau^{i_1(n-1)}\sigma\sigma\tau^{i_2} = \tau^{i_1(n-1)}\tau^{i_2} = \tau^{i_1(n-1)+i_2}$$

Soit k un entier pair. Supposons que la propriété soit vraie pour tout $j \leq k$ pair et montrons qu'alors elle est vraie pour $k+2$:

$$\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa_1}}\underbrace{\sigma\tau^{i_{k+1}}\sigma\tau^{i_{k+2}}}_{\tau^{\kappa_2}} = \tau^{\kappa_1}\tau^{\kappa_2} = \tau^{\kappa_1+\kappa_2}.$$

La propriété est donc vraie pour tout k pair.

b) considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair, alors d'après a) il s'écrit $\tau^{\ell}\sigma$ pour un certain ℓ

$$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k} = \underbrace{\sigma\sigma}_{\mathrm{id}}\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k} = \sigma\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa}} = \sigma\tau^{\kappa} = \tau^{\kappa(n-1)}\sigma.$$

c) considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma$ avec k pair ; d'après b) il s'écrit $\tau^{\kappa}\sigma$ pour un certain κ :

$$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma = \underbrace{\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa}\sigma}\sigma = \tau^{\kappa}\sigma\sigma = \tau^{\kappa}\underbrace{\sigma\sigma}_{\mathrm{id}} = \tau^{\kappa}.$$

d) finalement considérons un élément de la forme $\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma$ avec k pair ; d'après a) il s'écrit $\tau^{\kappa}\sigma$ pour un certain κ :

$$\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma = \underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa}}\sigma = \tau^{\kappa}\sigma$$

Un raisonnement analogue permet de conclure lorsque k est impair.

6. Déterminons le nombre de classes à gauche de G modulo H.

L'ensemble des classes à gauche de G modulo H est l'ensemble ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Son cardinal est $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| = [\mathrm{G} : \mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|}$. D'après la question précédente nous avons $|\mathrm{G}| = 2n$, $|\mathrm{H}| = 2$ et donc $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| = \frac{|\mathrm{G}|}{|\mathrm{H}|} = n$.

7. Décrivons l'ensemble quotient ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Les descriptions de G et H nous permettent d'affirmer que

$$\begin{aligned} {}^{\mathrm{G}}\!/_{\mathrm{H}} &= \{g\mathrm{H} \,|\, g \in \mathrm{G}\} \\ &= \{\mathrm{id}\mathrm{H},\, \tau\mathrm{H},\, \tau^2\mathrm{H},\, \ldots,\, \tau^{n-1}\mathrm{H},\, \sigma\mathrm{H},\, \tau\sigma\mathrm{H},\, \ldots, \tau^{n-1}\sigma\mathrm{H}\} \end{aligned}$$

Or $\mathrm{id}\mathrm{H} = \mathrm{H}$, $\sigma\mathrm{H} = \mathrm{H}$ (car σ appartient à H), $\tau^{\ell}\sigma\mathrm{H} = \tau^{\ell}\mathrm{H}$ (car σ appartient à H) pour tout $1 \leq \ell \leq n-1$. Il en résulte que

$${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\mathrm{id}\mathrm{H},\, \tau\mathrm{H},\, \tau^2\mathrm{H},\, \ldots,\, \tau^{n-1}\mathrm{H}\} = \{\overline{\mathrm{id}},\, \overline{\tau},\, \ldots,\, \overline{\tau^{n-1}}\}.$$

8. Le sous-groupe H de G n'est pas distingué dans G ; en effet

$\tau^{-1}\sigma\tau = \tau^{-1}\tau^{n-1}\sigma = \tau^{n-2}\sigma \notin \mathrm{H}$ (car par hypothèse $n \geq 3$ donc $n-2 \geq 1$).

9. Nous avons $[\mathrm{G} : \mathrm{K}] = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{2n}{2} = 2$. Ainsi K est un sous-groupe d'indice 2 de G ; il est donc distingué dans G et G/K a une structure de groupe.

   Le groupe quotient G/K est d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Nous avons $\mathrm{G}/\mathrm{K} = \{g\mathrm{K} \,|\, g \in \mathrm{G}\}$. Comme $g\mathrm{K} = \mathrm{K}$ pour tout $g \in \mathrm{K}$, nous avons

$$\begin{aligned} \mathrm{G}/\mathrm{K} &= \{g\mathrm{K} \,|\, g \in \mathrm{G} \smallsetminus \mathrm{K}\} \\ &= \{\mathrm{id}\mathrm{K},\, \sigma\mathrm{K},\, \tau\sigma\mathrm{K}, \ldots,\, \tau^{n-1}\sigma\mathrm{K}\}. \end{aligned}$$

   Mais $\tau^\ell\sigma\mathrm{K} = \sigma\tau^{\ell(n-1)}\mathrm{K}$ d'après 4. et $\sigma\tau^{\ell(n-1)}\mathrm{K} = \sigma\tau^{\ell(n-1)}\mathrm{K}$ puisque $\tau^{\ell(n-1)}$ appartient à K. Finalement

$$\mathrm{G}/\mathrm{K} = \{\mathrm{id}\mathrm{K},\, \sigma\mathrm{K}\} = \{\overline{\mathrm{id}},\, \overline{\sigma}\}.$$

10. L'application $\det\colon \mathrm{G} \to \mathbb{R}^*$ est un morphisme de groupes et K′ est son noyau. Ainsi K′ est un sous-groupe distingué de G.

11. Comparons K et K′.

    Soit g un élément de K ; il s'écrit sous la forme τ^ℓ. Remarquons que $\det\tau^\ell = (\det\tau)^\ell = \left(\cos^2\left(\frac{2\pi}{n}\right) + \sin^2\left(\frac{2\pi}{n}\right)\right)^\ell = 1^\ell = 1$ donc τ^ℓ appartient à K′. Ainsi $\mathrm{K} = \langle\tau\rangle \subset \mathrm{K}'$.

    Soit $g \in \mathrm{G} \smallsetminus \mathrm{K}$, alors g s'écrit $\tau^\ell\sigma$ avec $0 \leq \ell \leq n-1$ (cf 5.) d'où

$$\det g = \det(\tau^\ell\sigma) = \det(\tau^\ell)\det\sigma = (\det\tau)^\ell \times (-1) = 1^\ell \times (-1) = 1 \times (-1) = -1.$$

    Par suite g n'appartient pas à K′. Nous venons de montrer que si g n'appartient pas à K, alors g n'appartient pas à K′, autrement dit que si g appartient à K′, alors g appartient à K, *i.e.* $\mathrm{K}' \subset \mathrm{K}$.

12. Les groupes H et G/K sont d'ordre 2, donc sont isomorphes. Il en résulte qu'il existe un sous-groupe de G (le sous-groupe H) isomorphe à G/K.

13. Calculons $D(\mathrm{G})$.

    Le groupe G n'est pas abélien : $\sigma\tau = \tau^{n-1}\sigma \neq \tau\sigma$ car $n \neq 2$. Par conséquent $D(\mathrm{G}) \neq \{\mathrm{id}\}$.

    De plus G/K est abélien (en effet d'après 9. le groupe G/K est isomorphe au groupe abélien $\mathbb{Z}/2\mathbb{Z}$) ; $\mathrm{G}/D(\mathrm{G})$ étant le plus grand quotient abélien $D(\mathrm{G}) \subset \mathrm{K}$.

    Calculons $[\sigma, \tau]$:

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \tau^{-1}\tau^{-1} = \tau^{-2}$$

    ainsi τ^{-2} appartient à $D(\mathrm{G})$ et τ^2 appartient à $D(\mathrm{G})$. Finalement $\langle\tau^2\rangle \subset D(\mathrm{G})$. Nous avons donc les inclusions

$$\langle\tau^2\rangle \subset D(\mathrm{G}) \subset \mathrm{K}.$$

    Supposons que n soit impair ; l'ordre de τ^2 est $\frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{1} = n$ donc $\langle\tau^2\rangle = \langle\tau\rangle$ et $\mathrm{K} = \langle\tau\rangle \subset D(\mathrm{G})$. Finalement $D(\mathrm{G}) = \mathrm{K} = \langle\tau\rangle = \langle\tau^2\rangle$. Dans ce cas nous avons $\mathrm{G}/D(\mathrm{G}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Si $n = 2m$ est pair, montrons que

$$D(\mathrm{G}) = \langle\tau^2\rangle = \{\mathrm{id},\, \tau^2,\, \tau^4,\, \ldots,\, \tau^{n-2}\} = \{\mathrm{id},\, \tau^2,\, \tau^4,\, \ldots,\, \tau^{2(m-1)}\}.$$

Nous avons vu que $\langle\tau^2\rangle \subset D(\mathrm{G})$. Montrons que $\langle\tau^2\rangle \lhd \mathrm{G}$. Soit $y = \tau^{2a} \in \langle\tau^2\rangle$ et $x \in \mathrm{G}$; nous avons $x = \tau^k$ ou $x = \tau^k\sigma$. Dans le premier cas nous obtenons

$$xyx^{-1} = \tau^k\tau^{2a}\tau^{-k} = \tau^{k+2a-k} = \tau^{2a} = y \in \langle\tau^2\rangle$$

et dans le second cas

$$\begin{aligned} xyx^{-1} &= \tau^k\sigma\tau^{2a}(\tau^k\sigma)^{-1} = \tau^k \underbrace{\sigma\tau^{2a}}_{\tau^{2a(n-1)}\sigma} \sigma^{-1}\tau^{-k} \\ &= \tau^k\tau^{2a(n-1)}\sigma\sigma^{-1}\tau^{-k} = \tau^k\tau^{2a(n-1)}\tau^{-k} \\ &= \tau^{k+2a(n-1)-k} = \tau^{2a(n-1)} \in \langle\tau^2\rangle \end{aligned}$$

Ainsi $\langle\tau^2\rangle \lhd \mathrm{G}$.

De plus τ^2 est d'ordre $\frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{2} = m$ donc $|\langle\tau^2\rangle| = m$. Ainsi le quotient $\mathrm{G}/\langle\tau^2\rangle$ est d'ordre $\frac{2n}{m} = 4$. Mais un groupe d'ordre 4

- ◇ ou bien a un élément d'ordre 4 et est alors isomorphe à $\mathbb{Z}/4\mathbb{Z}$,
- ◇ ou bien n'a que des éléments d'ordre 2 et est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

En particulier, un groupe d'ordre 4 est abélien donc $\mathrm{G}/\langle\tau^2\rangle$ est abélien. Comme $\mathrm{G}/D(\mathrm{G})$ est le plus grand quotient abélien de G nous avons l'inclusion $\mathrm{G}/\langle\tau^2\rangle \subset \mathrm{G}/D(\mathrm{G})$ et l'inclusion $D(\mathrm{G}) \subset \langle\tau^2\rangle$. À partir de $\langle\tau^2\rangle \subset D(\mathrm{G})$ et $D(\mathrm{G}) \subset \langle\tau^2\rangle$ on obtient $D(\mathrm{G}) = \langle\tau^2\rangle$.

Il reste à déterminer $\mathrm{G}/D(\mathrm{G}) = \mathrm{G}/\langle\tau^2\rangle$ qui est d'ordre 4. On peut décrire $\mathrm{G}/D(\mathrm{G})$:

$$\begin{aligned} \mathrm{G}/D(\mathrm{G}) &= \mathrm{G}/\langle\tau^2\rangle \\ &= \{g\langle\tau^2\rangle \,|\, g \in \mathrm{G}\} \\ &= \{\langle\tau^2\rangle,\, \tau\langle\tau^2\rangle,\, \tau^2\langle\tau^2\rangle,\, \ldots,\, \tau^{2m-1}\langle\tau^2\rangle,\, \sigma\langle\tau^2\rangle,\, \tau\sigma\langle\tau^2\rangle,\, \tau^2\sigma\langle\tau^2\rangle,\, \ldots,\, \tau^{2m-1}\sigma\langle\tau^2\rangle\} \end{aligned}$$

On peut vérifier que si $2 \leq k \leq n-1$ est pair, alors $\tau^k\langle\tau^2\rangle = \langle\tau^2\rangle$ et que si $2 \leq k \leq n-1$ est impair, alors $\tau^k\langle\tau^2\rangle = \tau\langle\tau^2\rangle$.

On peut vérifier que si $2 \leq k \leq n-1$ est pair, alors $\tau^k\sigma\langle\tau^2\rangle = \sigma\langle\tau^2\rangle$ et que si $2 \leq k \leq n-1$ est impair, alors $\tau^k\sigma\langle\tau^2\rangle = \tau\sigma\langle\tau^2\rangle$.

Ainsi

$$\begin{aligned} \mathrm{G}/D(\mathrm{G}) &= \{\langle\tau^2\rangle,\, \tau\langle\tau^2\rangle,\, \sigma\langle\tau^2\rangle,\, \tau\sigma\langle\tau^2\rangle\} \\ &= \{\overline{\mathrm{id}},\, \overline{\sigma},\, \overline{\tau},\, \overline{\tau\sigma}\}. \end{aligned}$$

Mais $\overline{\tau}^2 = \overline{\tau^2} = \mathrm{id}$ (car on quotiente par τ^2), $\overline{\sigma}^2 = \overline{\sigma^2} = \overline{\mathrm{id}}$ (car σ est d'ordre 2) et $\overline{\tau\sigma}^2 = \overline{\tau}^2\overline{\sigma}^2 = \overline{\mathrm{id}}$ (car le groupe est abélien). Ainsi tous les éléments de $\mathrm{G}/D(\mathrm{G})$ sont d'ordre 2 et $\mathrm{G}/D(\mathrm{G})$ est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

14. Montrons que la multiplication des matrices définit une action

$$\mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX$$

D'une part $\mathrm{id} \cdot X = X$; d'autre part pour M, M' dans G nous avons

$$(MM') \cdot X = MM'X = M \cdot (M' \cdot X)$$

par l'associativité du produit matriciel. Nous avons donc bien une action de G sur $\mathbb{R}^2$.

15. L'action n'est pas transitive. En effet, d'une part l'orbite d'un vecteur $X \in \mathbb{R}^2$ est l'ensemble

$$\mathcal{O}_X = \{g \cdot X \,|\, g \in \mathrm{G}\} = \{gX \,|\, g \in \mathrm{G}\};$$

d'autre part $|\mathrm{G}| = 2n$. En particulier $\mathcal{O}_X$ compte au plus $2n$ éléments alors que $\mathbb{R}^2$ est infini : aucune orbite ne peut être égale à $\mathbb{R}^2$ tout entier.

16. L'action est fidèle : soit $g \in \mathrm{G}$ tel que $g \cdot X = X$ pour tout $X \in \mathbb{R}^2$, *i.e.* tel que $gX = X$ pour tout $X \in \mathbb{R}^2$, alors $g = \mathrm{Id}$.

17. Déterminons les points fixes de l'action, *i.e.* déterminons

$$\{X \in \mathbb{R}^2 \,|\, g \cdot X = X \quad \forall\, g \in \mathrm{G}\}.$$

Autrement dit nous cherchons les $X \in \mathbb{R}^2$ tels que $g \cdot X = X$ pour tout $g \in \mathrm{G}$. Remarquons que $X = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ est un point fixe. Montrons que c'est le seul. En effet si $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est un point fixe, alors en particulier $\sigma \cdot X = X$, c'est-à-dire $(x, -y) = (x, y)$ d'où $y = 0$. De plus nous avons $\tau \cdot X = X$ soit $\tau \cdot \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$ qui se réécrit $\begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) x \\ \sin\left(\frac{2\pi}{n}\right) x \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$. En particulier $\sin\left(\frac{2\pi}{n}\right) x = 0$; mais pour $n \geq 3$, nous avons $\sin\left(\frac{2\pi}{n}\right) \neq 0$ donc $x = 0$ et $X = (0, 0)$. Finalement $(0, 0)$ est l'unique point fixe de l'action.

18. Déterminons le stabilisateur

$$\mathrm{G}_{v_0} = \{g \in \mathrm{G} \,|\, g \cdot v_0 = v_0\} = \{g \in \mathrm{G} \,|\, gv_0 = v_0\}$$

du vecteur $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Remarquons que $\sigma \cdot v_0 = \sigma v_0 = v_0$, *i.e.* σ appartient à G_{v_0}.

Par ailleurs, soit $1 \leq k \leq n-1$, alors $\tau^k \cdot v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$; ainsi $\tau^k \cdot v_0 = v_0$ si et seulement si $\cos\left(\frac{2k\pi}{n}\right) = 1$ et $\sin\left(\frac{2k\pi}{n}\right) = 0$, c'est-à-dire si et seulement si $\frac{2k\pi}{n} \equiv 0 \pmod{}$

2π), *i.e.* si et seulement si k est un multiple de n : contradiction avec $1 \leq k \leq n-1$. Ainsi aucun τ^k, $1 \leq k \leq n-1$, ne fixe v_0.

De même nous avons $\tau^k\sigma \cdot v_0 = v_0$ si et seulement si $\tau^k \cdot v_0 = v_0$ si et seulement si $\tau^k = \mathrm{id}$; ainsi aucun $\tau^k\sigma$, $1 \leq k \leq n-1$, fixe v_0.

Il en résulte que $\mathrm{G}_{v_0} = \{\mathrm{id}, \sigma\} = \mathrm{H}$.

19. Décrivons l'orbite du vecteur v_0.

Puisque $\mathcal{O}_{v_0}$ et $\mathrm{G}/\mathrm{G}_{v_0}$ sont en bijection nous avons

$$|\mathcal{O}_{v_0}| = \left|\mathrm{G}/\mathrm{G}_{v_0}\right|.$$

Or

$$\left|\mathrm{G}/\mathrm{G}_{v_0}\right| = [\mathrm{G} : \mathrm{G}_{v_0}] = [\mathrm{G} : \mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|} = \frac{2n}{2} = n.$$

Ainsi l'orbite du vecteur v_0 compte n éléments.

Les éléments $\tau^k \cdot v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$, $0 \leq k \leq n-1$, sont 2 à 2 distincts. Ils forment donc l'orbite de v_0.

20. Quel est le stabilisateur G_S du segment $S = [v_0, Y_0]$?

Comme $Y_0 = -v_0$ nous voyons que

$$\sigma \cdot Y_0 = \sigma \cdot (-v_0) = \sigma(-v_0) = -\sigma(v_0) = -v_0 = Y_0$$

donc $\sigma[v_0, Y_0] = [v_0, Y_0]$ et σ appartient à G_S.

Si g appartient à G_S, alors comme g est linéaire, g doit envoyer v_0 sur un élément de la droite $\langle v_0 \rangle = (v_0, Y_0)$. Cherchons de tels $g \in \mathrm{G}$. On a ou bien $g = \tau^k$, ou bien $g = \tau^k\sigma$ avec dans les deux cas $0 \leq k \leq n-1$. Dans les deux éventualités

$$g \cdot v_0 = \tau^k v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}.$$

Mais $\langle v_0 \rangle = \{(x, y) \in \mathbb{R}^2 \,|\, y = 0\}$ donc on souhaite que $\sin\left(\frac{2k\pi}{n}\right) \equiv 0 \pmod{\pi}$ c'est-à-dire $\frac{2k\pi}{n} \equiv 0 \pmod{\pi}$.

Si n est impair, alors la seule possibilité est $k = 0$ et $\mathrm{G}_S = \{\mathrm{id}, \sigma\} = \mathrm{H}$.

Si $n = 2m$ est pair, alors nous avons deux possibilités : $k = 0$ et $k = m$. Pour $k = m$ nous avons

$$\tau^m = \begin{pmatrix} \cos\left(\frac{2m\pi}{n}\right) & -\sin\left(\frac{2m\pi}{n}\right) \\ \sin\left(\frac{2m\pi}{n}\right) & \cos\left(\frac{2m\pi}{n}\right) \end{pmatrix}$$

Ainsi $\tau^m \cdot v_0 = Y_0$ et $\tau^m \cdot Y_0 = v_0$. Par suite $\tau^m \cdot S = S$. Finalement $\mathrm{G}_S = \{\mathrm{id}, \sigma, \tau^m, \tau^m\sigma\}$.

Exercice 248

Soit E un espace vectoriel de dimension finie n.

1. Montrer que le groupe $\mathrm{GL}(E)$ agit naturellement sur l'ensemble X des sous-espaces vectoriels de E.
2. Déterminer l'orbite de $F \in X$. Combien existe-t-il d'orbites ?
3. Déterminer le stabilisateur de $F \in X$.

Éléments de réponse 248

1. Le groupe $\mathrm{GL}(E)$ est un sous-groupe du groupe $\mathfrak{S}_E$ des bijections de E. Il agit à gauche sur E et donc sur $\mathcal{P}(E)$

$$\forall\, g \in \mathrm{G} \quad \forall\, X \in \mathcal{P}(E) \quad g \cdot X = \{g \cdot x \,|\, x \in X\}.$$

   Soient $g \in \mathrm{GL}(E)$ et $F \in X$. Alors $g(F)$ est un sous-espace vectoriel de E. Donc X est une partie stable $\mathcal{P}(E)$ et $(g, F) \mapsto g(F)$ est une action de $\mathrm{GL}(E)$ sur X.

2. Soit $F \in X$ de dimension k. Pour tout $g \in \mathrm{GL}(E)$ nous avons $\dim g(F) = k$.

   Réciproquement soit $F' \in X$ tel que $\dim F' = k$. Choisissons des bases $(e_1, e_2, \ldots, e_k)$ de F et $(e'_1, e'_2, \ldots, e'_k)$ de F'. On peut compléter ces familles libres de E et obtenir des bases $(e_1, e_2, \ldots, e_k, e_{k+1}, e_{k+2}, \ldots, e_n)$ et $(e'_1, e'_2, \ldots, e'_k, e'_{k+1}, e'_{k+2}, \ldots, e'_n)$ de E. Il existe g une unique forme linéaire de E dans E telle que $g(e_i) = e'_i$ pour $1 \leq i \leq n$. Puisque le rang de g est n et puisque $g(F) = F'$ nous avons : $g \in \mathrm{GL}(E)$. Ainsi F' appartient l'orbite de F. L'orbite de F est donc l'ensemble des sous-espaces vectoriels de E de même dimension que F. Il existe donc $n + 1$ orbites pour cette action.

3. Le stabilisateur de F est l'ensemble des $g \in \mathrm{GL}(E)$ qui laissent F invariant. C'est l'ensemble des $g \in \mathcal{L}(E)$ qui ont, dans la base $(e_1, e_2, \ldots, e_k, e_{k+1}, e_{k+2}, \ldots, e_n)$ précédente, une matrice de la forme $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ avec $A \in \mathrm{M}_{k,k}$, $B \in \mathrm{M}_{k,n-k}$, $C \in \mathrm{M}_{n-k,n-k}$ et avec A et C inversibles car $\det A \det C = \det M \neq 0$.

Exercice 249

Soient $n \geq 2$ un entier et $d \geq 1$ un diviseur de n. Montrer que le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ contient un unique sous-groupe d'ordre d. Est-il vrai que $\mathbb{Z}/n\mathbb{Z}$ contient un unique élément d'ordre d ? (Commencer par expliciter les réponses dans le cas particulier $n = 6$, $d = 3$).

Éléments de réponse 249

- ◇ Si $d = 1$, le seul sous-groupe d'ordre 1 de $\mathbb{Z}/n\mathbb{Z}$ est $\{\overline{0}\}$.
- ◇ Supposons maintenant $d \geq 2$.

  Existence : soit q le quotient de n par d, c'est-à-dire $n = dq$. Alors le sous-groupe engendré par $\overline{q}$ est d'ordre d :

$$\langle q \rangle = \{\overline{0}, \overline{q}, \overline{2q}, \ldots, \overline{(d-1)q}\}.$$

Unicité : Soit $\mathrm{H} \subset {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ un sous-groupe d'ordre $d \geq 2$. Soit $k > 0$ le plus petit entier positif tel que $\overline{k} \in \mathrm{H}$. Si $\overline{a}$ appartient à H pour un certain a dans $\mathbb{N}$, montrons que a est un multiple de k. En effet écrivons la division euclidienne de a par q : $a = qk + r$, $0 \leq r \leq k-1$, on obtient alors $\overline{a} = \underbrace{\overline{k} + \overline{k} + \ldots + \overline{k}}_{q \text{ fois}} + \overline{r}$ d'où $\overline{r} \in \mathrm{H}$ et donc $r = 0$ par minimalité de k. En particulier puisque $\overline{d} = \overline{0} \in \mathrm{H}$, d est un multiple de k et donc $\mathrm{H} = \langle \overline{k} \rangle$ avec $n = kd$.

Exemple : dans ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$, l'unique sous-groupe d'ordre 3 est $\{\overline{0}, \overline{2}, \overline{4}\}$, qui contient deux éléments d'ordre 3.

Exercice 250

On se propose de montrer que le groupe alterné $\mathcal{A}_4$ ne contient aucun sous-groupe d'ordre 6.

(1) En général, montrer que si $\mathrm{H} \subset \mathrm{G}$ est un sous-groupe d'indice 2, alors H est distingué dans G.

(2) Rappeler la liste des classes de conjugaison de $\mathcal{A}_4$ et leurs cardinaux.

(3) Conclure.

Éléments de réponse 250

(1) Soit $\mathrm{H} \subset \mathrm{G}$ d'indice 2. Si g appartient à H, alors $g\mathrm{H} = \mathrm{H}g = \mathrm{H}$ (l'hypothèse indice 2 est inutile ici). Si g n'appartient pas à H, alors puisque H est d'indice 2 nous avons

$$\mathrm{G} = \mathrm{H} \cup g\mathrm{H} = \mathrm{H} \cup \mathrm{H}g.$$

On voit que $g\mathrm{H} = \mathrm{H}g = \mathrm{G} \setminus \mathrm{H}$; en particulier $g\mathrm{H} = \mathrm{H}g$, autrement dit H est distingué dans G.

(2) Le groupe $\mathcal{A}_4$ compte quatre classes de conjugaison, qui sont :

- ◇ la classe de l'identité, de cardinal 1,
- ◇ la classe des doubles transposition, de cardinal 3,
- ◇ une première classe de 3-cycles, de cardinal 4,
- ◇ une deuxième classe de 3-cycles, de cardinal 4.

Notons que dans $\mathfrak{S}_4$ la réponse serait différente : les 3-cycles forment une seule classe de conjugaison dans $\mathfrak{S}_4$, de cardinal 8.

(3) Supposons que $\mathrm{H} \subset \mathcal{A}_4$ soit un sous-groupe d'ordre 6 ; il est ainsi d'indice 2 dans $\mathcal{A}_4$. La question (1) assure que H est donc distingué dans $\mathcal{A}_4$. Alors H devrait être union de classes de conjugaison, dont celle du neutre, mais il n'est pas possible d'obtenir 6 en sommant des nombres parmi $\{1, 3, 4, 4\}$: contradiction.

Remarque : d'après (2) les cardinaux possibles pour un sous-groupe distingué de $\mathcal{A}_4$ sont

- ◇ 1 (sous-groupe trivial),
- ◇ $4 = 1 + 3$ (c'est le groupe de Klein engendré par les double-transpositions),
- ◇ $5 = 1 + 4$ (en fait impossible par Lagrange),
- ◇ $8 = 1 + 3 + 4$ (en fait impossible par Lagrange),
- ◇ $9 = 1 + 4 + 4$ (en fait impossible par Lagrange),
- ◇ $12 = 1 + 3 + 4 + 4$ (groupe $\mathcal{A}_4$ entier).

Exercice 251

Soit $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ le groupe des matrices inversibles 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Quel est l'ordre de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$?
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définir une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.
3. En déduire que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathfrak{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

Éléments de réponse 251

1. Les éléments de $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$. Se donner un élément de G c'est se donner une colonne c_1 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ non nulle et une colonne c_2 non colinéaire à c_1. Il y a $2^2 - 1$ choix possibles pour c_1 (il y a deux choix pour chacun des coefficients de la colonne et on retire la colonne nulle) et $2^2 - 2$ choix possibles pour c_2 (il y a deux choix pour chacun des coefficients de la colonne et on retire λc_1 avec $\lambda \in \{0, 1\}$). Finalement il y a donc $(2^2 - 1)(2^2 - 2) = 3 \times 2$ choix possibles, c'est-à-dire $|\mathrm{G}| = 6$.

   Les éléments de G sont :

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$$

2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définissons une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.

   À chaque base (v, w) de l'espace vectoriel E correspond une action de G sur E : pour $M \in \mathrm{G}$ et $u \in E$ on définit $M \cdot u \in E$ comme l'image du vecteur u par la matrice M dans la base (v, w) :

$$\begin{aligned} \mathrm{G} \times E &\to E \\ (M, u) &\mapsto M \cdot u = Mu \end{aligned}$$

   Notons que si M et M' appartiennent à G et u à E, alors $M \cdot (M' \cdot u) = (MM') \cdot u$ et que $\mathrm{id} \cdot u = u$ pour tout $u \in E$.

3. Montrons que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathfrak{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

   Première méthode. Le groupe $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est d'ordre 6 ; il n'est pas abélien

   $$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \neq \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}$$

   Par suite $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe à $\mathfrak{S}_3$.

   Seconde méthode.

   Remarquons que $\#E = 4$ (en effet E est constitué des quatre vecteurs $(0,0)$, $(1,0)$, $(0,1)$ et $(1,1)$).

   Se donner l'action de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E :

   $$\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right) \times E \to E, \qquad (M, v) \mapsto M \cdot v = Mv$$

   revient à se donner le morphisme de groupes φ de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ dans $\mathfrak{S}_E \simeq \mathfrak{S}_4$ donné par

   $$\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right) \to \mathfrak{S}_E \simeq \mathfrak{S}_4, \qquad M \to \varphi(M)\colon E \to E$$
   $$v \mapsto \varphi(M)(v) = M \cdot v = Mv$$

   Remarquons que φ est injectif. De plus, $\operatorname{im}\varphi \simeq \mathfrak{S}_3$; en effet tout élément $\varphi(M)$ fixe $(0,0)$ (rappelons que $\varphi(M)$ est la matrice d'une application linéaire) et permute les vecteurs $(1,0)$, $(0,1)$ et $(1,1)$. Il en résulte que $\varphi\colon \mathrm{G} \to \mathfrak{S}_3$ est un isomorphisme.

Exercice 252

Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrer que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$. Indication : faire agir G par conjugaison sur H.
2. Montrer que l'ordre de $Z(\mathrm{G})$ est > 1. Indication : faire agir G par conjugaison sur G.

Éléments de réponse 252

Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrons que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$. Faisons agir G par conjugaison sur H (notons que c'est possible car H étant distingué dans G nous avons $\forall\, g \in \mathrm{G}$, $g\mathrm{H}g^{-1} \subset \mathrm{H}$) :

   $$\mathrm{G} \times \mathrm{H} \to \mathrm{H}$$
   $$(g, h) \mapsto g \cdot h = ghg^{-1}$$

   L'ordre de H est une puissance de p soit p^β car, d'après le théorème de Lagrange, $|\mathrm{H}|$ divise $|\mathrm{G}|$ qui est une puissance de p. L'ordre de H est aussi somme des cardinaux des

orbites pour l'action de G par conjugaison sur H (les orbites forment une partition de G) ; chacune de ces orbites a pour cardinal un diviseur de |G|, c'est-à-dire de p^n donc une puissance de p.

Raisonnons par l'absurde : supposons que $Z(\mathrm{G}) \cap \mathrm{H} = \{e\}$; alors une seule des orbites est réduite à un seul élément : l'orbite de e. Ainsi nous avons d'une part $|\mathrm{H}| = p^\beta$, d'autre part $|\mathrm{H}| = 1 +$ somme de puissances de p d'où

$$p^\beta = 1 + \text{ somme de puissances de } p$$

contradiction. Par suite $Z(\mathrm{G}) \cap \mathrm{H} \neq \{e\}$.

2. Montrons que l'ordre de $Z(\mathrm{G})$ est > 1. Faisons agir G par conjugaison sur lui-même

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, h) \mapsto g \cdot h = ghg^{-1}$$

Remarquons que les orbites de G pour l'action de G par conjugaison sur lui-même ont pour cardinal des puissances de p ; en effet ces cardinaux sont des diviseurs de $|\mathrm{G}| = p^n$.

Raisonnons par l'absurde : supposons que $|Z(\mathrm{G})| = 1$, alors d'une part $|\mathrm{G}| = p^n$, d'autre part (les orbites formant une partition de G) nous avons $|\mathrm{G}| = 1 +$ somme de puissances de p. Par suite $p^n = 1+$ somme de puissances de p : contradiction. Il en résulte que $|Z(\mathrm{G})| > 1$.

Exercice 253

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \setminus Z(\mathrm{G})$; notons $\mathrm{St}(g)$ le stabilisateur de g.

   Montrer que $Z(\mathrm{G}) \subset \mathrm{St}(g) \subset \mathrm{G}$ (les inclusions sont strictes).

2. En déduire que si G n'est pas abélien, alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier divisant l'ordre |G| de G.

3. Soit p un nombre premier. Soit n un entier.

   Quelles sont les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n ?

   Quel est le centre d'un groupe d'ordre p^2 ?

   Quel est le centre d'un groupe non abélien d'ordre p^3 ?

4. Donner un exemple de groupe d'ordre p^3 non abélien.

5. Montrer que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Éléments de réponse 253

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \smallsetminus Z(\mathrm{G})$; notons $\mathrm{St}(g)$ le stabilisateur de g.

   Montrons que $Z(\mathrm{G}) \subset \mathrm{St}(g) \subset \mathrm{G}$ (les inclusions sont strictes).

   L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{St}(g)$ est claire.

   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{St}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{St}(g)$.

   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Puisque $g \notin Z(\mathrm{G})$ il existe un élément $h \in \mathrm{G}$ qui ne commute pas avec g donc qui n'appartient pas à $\mathrm{St}(g)$. Il en résulte que $\mathrm{St}(g)$ est un sous-groupe propre de G.

2. Supposons que G ne soit pas abélien, montrons qu'alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier p divisant l'ordre $|\mathrm{G}|$ de G.

   D'après 1. si G n'est pas abélien et si g appartient à $\mathrm{G} \smallsetminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{St}(g)|$. Mais $|\mathrm{G} : \mathrm{St}(g)| \geq p$ car $|\mathrm{G} : \mathrm{St}(g)|$ divise $|\mathrm{G}|$. Par suite $|\mathrm{G} : Z(\mathrm{G})| > p$.

3. Soit p un nombre premier. Soit n un entier.

   Donnons les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n.

   Si G est abélien, alors $|Z(\mathrm{G})| = p^n$.

   Si G n'est pas abélien, alors $|\mathrm{G} : Z(\mathrm{G})| > p$ donc $|Z(\mathrm{G})| < p^{n-1}$. L'exercice précédent assure que $Z(\mathrm{G})$ n'est pas réduit à l'élément neutre donc $|Z(\mathrm{G})| \geq p$. Finalement lorsque G n'est pas abélien, nous avons

   $$|Z(\mathrm{G})| \in \{p, p^2, \ldots, p^{n-2}\}$$

   Si $n = 2$, le groupe G est nécessairement abélien.

   Déterminons le centre d'un groupe d'ordre p^2. Le centre d'un groupe G d'ordre p^2 est donc G tout entier.

   Déterminons le centre d'un groupe non abélien d'ordre p^3. Le centre d'un groupe non abélien d'ordre p^3 est d'ordre p.

4. Donnons un exemple de groupe d'ordre p^3 non abélien.

   Le groupe des quaternions est un groupe d'ordre 2^3 (ici $p = 2$) et n'est pas abélien.

5. Montrons que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

   Soit G un groupe d'ordre p^2. Il est abélien. Nous avons l'alternative suivante :

   — ou bien G contient un élément d'ordre p^2 auquel cas G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;

   — ou bien tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \smallsetminus \{e\}$ tels que $y \notin \langle x \rangle$. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$. En effet le sous-groupe $\langle x \rangle \cap \langle y \rangle$ est d'ordre strictement inférieur à p et d'ordre divisant p donc d'ordre 1. Puisque

tout sous-groupe du groupe abélien G est distingué G est isomorphe à $\langle x\rangle \times \langle y\rangle$. Or $\langle x\rangle \simeq \langle y\rangle \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Ainsi $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

Exercice 254

Soient E un ensemble et G un groupe agissant sur E. Soient g et h des éléments de E appartenant à la même orbite.

Montrer que les stabilisateurs St_g et St_h sont des sous-groupes conjugués de G.

En déduire que St_g et St_h ont même ordre.

Éléments de réponse 254

Soient E un ensemble et G un groupe agissant sur E. Soient g et h des éléments de E appartenant à la même orbite. Alors il existe x dans G tel que $h = x \cdot g$.

Soit $y \in \mathrm{St}_g$. Alors $y \cdot g = g$. De plus d'une part $y \cdot g = y \cdot (x^{-1}h)$ et d'autre part $g = x^{-1}h$. Par conséquent $y \cdot (x^{-1}h) = x^{-1}h$, soit $xyx^{-1} \cdot h = h$ c'est-à-dire xyx^{-1} appartient à St_h. Autrement dit $x\mathrm{St}_g x^{-1} \subset \mathrm{St}_h$.

Un raisonnement similaire conduit à $\mathrm{St}_h \subset x\mathrm{St}_g x^{-1}$.

Il s'en suit que $\mathrm{St}_h = x\mathrm{St}_g x^{-1}$.

L'application $y \mapsto xyx^{-1}$ est un automorphisme de G. C'est donc une bijection et l'image de St_g par cet automorphisme est St_h. Ces deux ensembles ont donc même cardinal.

Exercice 255

Soit E un ensemble fini. Soit G un groupe fini qui opère sur E. Pour tout g dans G on définit

$$E^g = \{s \in E \,|\, g \cdot s = s\}.$$

Autrement dit E^g est l'ensemble des points fixes de E sous l'action de g. Pour $s \in E$, on note G_s le fixateur de s pour l'action de G sur E.

1. Construire la table de l'opération

   $$\varphi\colon \mathrm{G} \times E \to \{\text{ vrai=V, faux=F }\}$$

   définie par

   $$\begin{cases} \varphi(g,s) = V \text{ si } g \cdot s = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

   dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.
2. Démontrer que $\displaystyle\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.
3. i) Soit $x \in E$. Soit $y \in \mathcal{O}_x$. Montrer qu'il existe $z \in \mathrm{G}$ tel que $\mathrm{G}_y = z^{-1}\mathrm{G}_x z$.

   ii) Montrer que pour tout $x \in E$ nous avons $|\mathrm{G}| = \displaystyle\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y|$.

iii) En déduire la formule de Burnside

$$|\mathrm{G}| \times |\Omega| = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g)$$

où $\Omega = \{\mathcal{O}_x \,|\, x \in E\}$ désigne l'ensemble des orbites de E sous l'action de G.

Éléments de réponse 255

1. Construisons la table de l'opération

$$\varphi\colon \mathrm{G} \times E \to \{\text{ vrai=V, faux=F }\}$$

définie par

$$\begin{cases} \varphi(g,s) = V \text{ si } g \cdot s = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.

Désignons par O le centre de gravité du triangle équilatéral ABC et par ρ la rotation de centre O et d'angle $\frac{2\pi}{3}$. Soient s_A, s_B et s_C les symétries d'axes respectifs AO, BO et CO.

Nous obtenons la table suivante

	A	B	C
id	V	V	V
ρ	F	F	F
ρ^2	F	F	F
s_A	V	F	F
s_B	F	V	F
s_C	F	F	V

En effet

(a) $\mathrm{id}(A) = A$, $\mathrm{id}(B) = B$ et $\mathrm{id}(C) = C$;

(b) $\rho(A) \in \{B, C\}$, $\rho(B) \in \{A, C\}$ et $\rho(C) \in \{A, B\}$;

(c) $\rho^2(A) \in \{B, C\}$, $\rho^2(B) \in \{A, C\}$ et $\rho^2(C) \in \{A, B\}$;

(d) $s_A(A) = A$, $s_A(B) = C$ et $s_A(C) = B$;

(e) $s_B(B) = B$, $s_B(A) = C$ et $s_B(C) = A$;

(f) $s_C(C) = C$, $s_C(A) = B$ et $s_C(B) = A$.

2. Montrons que $\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.

Rappelons que $\mathrm{G}_s = \{g \in \mathrm{G} \,|\, g\cdot s = s\}$. Posons $p = |\mathrm{G}|$. Notons g_1, g_2, …, g_p les éléments de G. Posons $q = \mathrm{card}(E)$. Notons s_1, s_2, …, s_q les éléments de E.

D'une part

$$\begin{aligned}\varphi^{-1}(V) &= \{(g,s) \in \mathrm{G}\times E \,|\, g\cdot s = s\}\\ &= \{(g,s) \in \mathrm{G}\times E \,|\, s \in E^g\}\\ &= \{g_1\}\times E^{g_1} \cup \{g_2\}\times E^{g_2} \cup \ldots \cup \{g_p\}\times E^{g_p}\end{aligned}$$

ce qui conduit à

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$$

D'autre part

$$\begin{aligned}\varphi^{-1}(V) &= \{(g,s) \in \mathrm{G}\times E \,|\, g\cdot s = s\}\\ &= \{(g,s) \in \mathrm{G}\times E \,|\, g \in \mathrm{G}_s\}\\ &= \mathrm{G}_{s_1}\times \{s_1\} \cup \mathrm{G}_{s_2}\times \{s_2\} \cup \ldots \cup \mathrm{G}_{s_q}\times \{s_q\}\end{aligned}$$

ce qui entraîne

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{s\in E} |\mathrm{G}_s|.$$

Il en résulte que

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = \sum_{s\in E} |\mathrm{G}_s|. \tag{1.6.2}$$

3. ◇ Soient $x \in E$ et $y \in \mathcal{O}_x$. Trouvons $z \in \mathrm{G}$ tel que

$$\mathrm{G}_y = z^{-1}\mathrm{G}_x z.$$

Soient $x \in E$ et $y \in \mathcal{O}_x$. Il existe $g \in \mathrm{G}$ tel que $y = g\cdot x$. Soit $w \in \mathrm{G}_x$, alors $w\cdot x = x$. D'une part $w\cdot x = w\cdot(g^{-1}y)$, d'autre part $x = g^{-1}y$. Par conséquent $w\cdot x = x$ se réécrit $w\cdot(g^{-1}y) = g^{-1}y$ ou encore $(gwg^{-1})\cdot y = y$; autrement dit gwg^{-1} appartient à G_y et $g\mathrm{G}_x g^{-1} \subset \mathrm{G}_y$. Un raisonnement analogue conduit à $\mathrm{G}_y \subset g\mathrm{G}_x g^{-1}$. Il s'en suit que $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ et que $z = g^{-1}$ convient.

◇ Montrons que pour tout $x \in E$

$$|\mathrm{G}| = \sum_{y\in \mathcal{O}_x} |\mathrm{G}_y|.$$

D'après le ◇ précédent $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ donc $|\mathrm{G}_y| = |\mathrm{G}_x|$ et

$$\sum_{y\in \mathcal{O}_x} |\mathrm{G}_y| = \sum_{y\in \mathcal{O}_x} |\mathrm{G}_x| = |\mathrm{G}_x| \sum_{y\in \mathcal{O}_x} 1 = |\mathrm{G}_x|\,|\mathcal{O}_x|.$$

Or l'application

$$\mathrm{G}/\mathrm{G}_x \to \mathcal{O}_x, \qquad \overline{g} \mapsto g \cdot x$$

est bien définie et est une bijection ; par suite $\left|\mathrm{G}/\mathrm{G}_x\right| = |\mathcal{O}_x|$, *i.e.* $|\mathrm{G}| = |\mathcal{O}_x|\,|\mathrm{G}_x|$. Ainsi $\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.

◇ Déduisons-en la formule

$$|\Omega| = \frac{1}{|\mathrm{G}|}\sum_{x\in E} |\mathrm{G}_x|$$

où $\Omega = \{\mathcal{O}_x \,|\, x \in E\}$ est l'ensemble des orbites de E sous l'action de G.

Nous avons

$$\sum_{x\in E} |\mathrm{G}_x| = \sum_{\mathcal{O}_x\subset\Omega}\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y|.$$

D'après le ◇ précédent $\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$ d'où

$$\sum_{x\in E} |\mathrm{G}_x| = \sum_{\mathcal{O}_x\subset\Omega} |\mathrm{G}| = |\mathrm{G}| \sum_{\mathcal{O}_x\subset\Omega} 1 = |\mathrm{G}|\,|\Omega|.$$

Finalement

$$|\Omega| = \frac{1}{|\mathrm{G}|}\sum_{x\in X} |\mathrm{G}_x|.$$

et

$$\sum_{x\in E} |\mathrm{G}_x| = |\Omega|\,|\mathrm{G}| \tag{1.6.3}$$

Les égalités (3.6.2) et (1.16.4) entraînent la formule de Burnside.

Exercice 256

Combien $(\mathbb{F}_2)^n$ admet-il de sous-espaces vectoriels de dimension k ?

Éléments de réponse 256

Soit $0 \le k \le n$. Le groupe $\mathrm{GL}(n, \mathbb{F}_2)$ agit transitivement sur l'ensemble Λ_k des sous-espaces vectoriels de dimension k de $(\mathbb{F}_2)^n$. L'ordre du groupe $\mathrm{GL}(n, \mathbb{F}_2)$ est

$$\begin{aligned}
&(2^n-1)\times(2^n-2)\times\ldots\times(2^n-2^{n-1})\\
&\quad= (2^n-1)\times 2\times(2^{n-1}-1)\times\ldots\times 2^{n-1}\times(2-1)\\
&\quad= 2\times 2^2\times\ldots\times 2^{n-1}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)\\
&\quad= 2^{1+2+\ldots+(n-1)}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)\\
&\quad= 2^{\frac{n(n-1)}{2}}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)
\end{aligned}$$

Le stabilisateur de $(\mathbb{F}_2)^k \times \{0_{n-k}\}$ sous l'action de $\mathrm{GL}(n,\mathbb{F}_2)$ sur Λ_k est d'ordre [3]

$$\underbrace{(2^k-1)(2^k-2)\dots(2^k-2^{k-1})}_{|\mathrm{GL}(k,\mathbb{F}_2)|}\times(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1}).$$

Simplifions cette expression :

$$\begin{aligned}
&(2^k-1)(2^k-2)\dots(2^k-2^{k-1})(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\\
&\quad=\Big((2^k-1)(2^k-2)\dots(2^k-2^{k-1})\Big)\Big((2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\Big)\\
&\quad=\Big((2^k-1)\times 2\times(2^{k-1}-1)\times\dots\times 2^{k-1}\times(2-1)\Big)\\
&\qquad\Big(2^k\times(2^{n-k}-1)\times 2^{k+1}\times(2^{n-k-1}-1)\times\dots\times 2^{n-1}\times(2-1)\Big)\\
&\quad=2\times 2^2\times\dots 2^k\times 2^{k+1}\times\dots\times 2^{n-1}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times(2-1)\\
&\quad=2^{1+2+\dots+(n-1)}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)\\
&\quad=2^{\frac{n(n-1)}{2}}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)
\end{aligned}$$

Le ratio de ces deux quantités donne le cardinal recherché soit

$$\frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-k+1}-1)}{(2^k-1)(2^{k-1}-1)\dots(2-1)}.$$

Exercice 257

Soit G un groupe. Soient H et K deux sous-groupes distingués de G.

Montrer que le sous-groupe de G engendré par $\mathrm{H}\cup\mathrm{K}$ est aussi distingué dans G.

Éléments de réponse 257

Soient $g\in\mathrm{G}$ et $x\in\langle\mathrm{H}\cup\mathrm{K}\rangle$. Il existe donc y_1, y_2, …, y_m dans $\mathrm{H}\cup\mathrm{K}$ tels que $x=y_1y_2\dots y_m$ et

$$gxg^{-1}=gy_1y_2\dots y_mg^{-1}.$$

Si y_1 appartient à H alors puisque H est distingué dans G il existe $y_1'\in\mathrm{H}$ tel que $gy_1=y_1'g$. Si y_1 appartient à K alors puisque K est distingué dans G il existe $y_1''\in\mathrm{K}$ tel que $gy_1=y_1''g$. Ainsi il existe $z_1\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_1=z_1g$.

En fait pour tout $1\leq i\leq m$ il existe $z_i\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_i=z_ig$.

3. cela revient à choisir une matrice de $\mathrm{GL}(k,\mathbb{F}_2)$ puis à choisir un vecteur non nul linéairement indépendant avec les k premiers puis un vecteur non nul linéairement indépendant avec les $k+1$ premiers...

Nous obtenons donc

$$\begin{aligned} gxg^{-1} &= gy_1y_2\dots y_mg^{-1} \\ &= z_1gy_2\dots y_mg^{-1} \\ &= z_1z_2g\dots y_mg^{-1} \\ &= \dots \\ &= z_1z_2\dots z_mgg^{-1} \\ &= z_1z_2\dots z_m \end{aligned}$$

Or $z_1z_2\dots z_m$ appartient à $\mathrm{H}\cup\mathrm{K}$ donc gxg^{-1} appartient à $\mathrm{H}\cup\mathrm{K}$. Ainsi $\langle \mathrm{H}\cup\mathrm{K}\rangle$ est distingué dans G.

Exercice 258

Soit G un groupe. Rappelons que le centralisateur d'un élément de G est l'ensemble des éléments de G qui commutent avec lui.

1. Montrer que le centralisateur d'un élément de G est un sous-groupe de G.
2. Dans $\mathfrak{S}_4$ quel est le centralisateur de (1 2) ? Est-ce un sous-groupe distingué de $\mathfrak{S}_4$?

Éléments de réponse 258

1. Soit G un groupe. Montrons que le centralisateur C_g d'un élément g de G est un sous-groupe de G.

   Notons que e appartient à C_g.

   Soit x dans C_g. Alors $gx = xg$ d'où $x^{-1}gxx^{-1} = x^{-1}xgx^{-1}$ c'est-à-dire $x^{-1}g = gx^{-1}$, autrement dit x^{-1} appartient à C_g.

   Soient x et y dans C_g. Alors

   $$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

   i.e. xy appartient à C_g.

   Il en résulte que C_g est un sous-groupe de G.

2. Déterminons le centralisateur de (1 2) dans $\mathfrak{S}_4$.

   Soit σ un élément de $\mathfrak{S}_n$. Si $(i\ j)$ est une transposition quelconque alors $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$. En effet soit $y \in \{1, 2, \dots, n\}$;

   - si $y = \sigma(i)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(j)$;
   - si $y = \sigma(j)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(i)$;
   - si $y \notin \{\sigma(i), \sigma(j)\}$, alors $\big((i\ j)\sigma^{-1}\big)(y) = \sigma^{-1}(y)$ et $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = y$.

   Ainsi le centralisateur de $(i\ j)$ est constitué des permutations $\sigma \in \mathfrak{S}_n$ qui laisse l'ensemble $\{i, j\}$ invariant, *i.e.* des permutations $\sigma \in \mathfrak{S}_n$ telles que $\sigma(i) = i$ ou j et $\sigma(j) = j$ ou i. En particulier le centralisateur de (1 2) dans $\mathfrak{S}_4$ est $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.

Considérons la permutation (3 4) qui appartient au centralisateur de (1 2) dans $\mathfrak{S}_4$. Conjuguons là par la transposition (2 3). Nous obtenons (2 4), *i.e.* (2 3)(1 2)(2 3) = (2 4). En particulier (2 3)(1 2)(2 3) n'appartient pas au centralisateur de (1 2) dans $\mathfrak{S}_4$. Le centralisateur de (1 2) dans $\mathfrak{S}_4$ n'est donc pas un sous-groupe distingué de $\mathfrak{S}_4$.

Exercice 259

Soit G un groupe. Soient H et K deux groupes de G. Considérons un sous-groupe L de $\mathrm{H}\cap\mathrm{K}$ qui est distingué dans H et dans K.

Montrer que L est distingué dans le sous-groupe de G engendré par $\mathrm{H}\cup\mathrm{K}$.

Éléments de réponse 259

Le sous-groupe L est un sous-groupe de $\langle \mathrm{H}\cup\mathrm{K}\rangle$. Soit z un élément de $\langle \mathrm{H}\cup\mathrm{K}\rangle$. Nous pouvons écrire z sous la forme $z_1 z_2 \dots z_m$ les z_i, $1 \leq i \leq m$, appartenant à $\mathrm{H}\cup\mathrm{K}$.

Soit $\ell \in \mathrm{L}$; alors

$$z\ell z^{-1} = z_1 z_2 \dots (z_m \ell z_m^{-1}) \dots z_2^{-1} z_1^{-1}.$$

L'élément $z_m \ell z_m^{-1}$ appartient à L ; en effet si z_m appartient à H (respectivement K), nous utilisons le fait que L est distingué dans H (respectivement K).

Nous en déduisons de la même façon que $z_{m-1} z_m \ell z_m^{-1} z_{m-1}^{-1}$ appartient à L. Par récurrence $z\ell z^{-1}$ appartient à L ce qui prouve que L est distingué dans $\langle \mathrm{H}\cup\mathrm{K}\rangle$.

Exercice 260

Montrer que dans un groupe tout sous-groupe d'indice 2 est distingué.

Éléments de réponse 260

Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Nous avons donc ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\mathrm{H},\, x\mathrm{H}\}$ où $x \neq \mathrm{H}$ et $\mathrm{G} = \mathrm{H}\cup x\mathrm{H}$ avec $\mathrm{H}\cap x\mathrm{H} = \emptyset$.

Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons

$$ghg^{-1} = xh_0 h h_0^{-1} x^{-1} = xh'x^{-1}$$

où $h' = h_0 h h_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à $x\mathrm{H}$, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

Exercice 261

Soit G un groupe. Soient H et K des sous-groupes de G. Supposons que

- H et K sont des sous-groupes distingués de G ;
- $\mathrm{H}\cap\mathrm{K} = \{e\}$;
- $\mathrm{HK} = \mathrm{G}$.

Considérons l'application

$$\varphi\colon \mathrm{H}\times\mathrm{K}\to\mathrm{G} \qquad\qquad \varphi(h,k)=hk.$$

1. Montrer que φ est une application injective.
2. Montrer que φ est un isomorphisme de groupes.

Éléments de réponse 261

1. Montrons que φ est une application injective.

   Soient h et h' dans H, soient k et k' dans K. Supposons que $\varphi(h,k)=\varphi(h',k')$, *i.e.* $hk=h'k'$ ce que nous pouvons réécrire $h^{'-1}h=k'k^{-1}$. D'une part $h^{'-1}h$ appartient à H, d'autre part $k^{'-1}k$ appartient à K. Il en résulte que $h^{'-1}h=k'k^{-1}$ appartient à $\mathrm{H}\cap\mathrm{K}=\{e\}$. Ainsi $h=h'$, $k=k'$ et φ est injective.

2. Montrons que φ est un isomorphisme de groupes.

   Par hypothèse $\mathrm{HK}=\mathrm{G}$ donc φ est surjective.

   Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk=k_1h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1h=h_1k_1$ pour un certain h_1 dans H. Or φ est injective donc $h=h_1$, $k=k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$ d'où

   - HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK ;
   - φ est un morphisme de groupes.

   Par suite φ est un isomorphisme de groupes.

Exercice 262

Soit G un groupe. Soient H et K deux sous-groupes propres de G. Supposons que

- H et K sont des sous-groupes d'indice 2 dans G ;
- $\mathrm{H}\cap\mathrm{K}=\{e\}$.

Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 262

Les groupes H et K sont d'indice 2 dans G ils sont donc distingués dans G.
De plus $\mathrm{H}\cap\mathrm{K}=\{e\}$ donc HK est un sous-groupe distingué de G. En effet

- Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk=k_1h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1h=h_1k_1$ pour un certain h_1 dans H. Or φ est injective donc $h=h_1$, $k=k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$. Ainsi HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK.

- Le groupe HK est distingué dans G ; en effet soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Comme H est distingué dans G l'élémeent $ghkg^{-1}$ s'écrit aussi h_1gkg^{-1} avec h_1 dans H. Par ailleurs $h_1gkg^{-1} = h_1k_1gg^{-1} = h_1k_1$ avec k_1 dans K car K est distingué dans G. Il s'en suit que $ghkg^{-1}$ appartient à HK.
- Montrons que H et K sont d'ordre 2. Nous avons $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $x \notin \mathrm{H}$. Comme K est d'indice 2 il est d'ordre au moins 2 et contient donc au moins un élément k qui n'est pas dans H (en particulier $k \neq e$). Nous pouvons donc prendre pour x cet élément k. Ainsi $\mathrm{G} = \mathrm{H} \cup k\mathrm{H}$ avec $\mathrm{H} \cap k\mathrm{H} = \emptyset$. Soit $k' \in \mathrm{K} \setminus \{e\}$. Ainsi k' n'appartient pas à H et $k' \in k\mathrm{H}$. Il existe donc $h \in \mathrm{H}$ tel que $k' = kh$. Par suite $h = k^{-1}k'$ est aussi dans K donc $h = e$ et $k = k'$. Le groupe K contient donc seulement deux éléments : e et k.

  De même nous obtenons que H est d'ordre 2.

  Ainsi H et K sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.
- Montrons que $\mathrm{G} = \mathrm{KH}$. Soit $g \in \mathrm{G}$. Alors ou bien g appartient à H et donc g appartient à HK, ou bien g appartient à kH, *i.e.* $g = kh$ avec $h \in \mathrm{H}$. Or $\mathrm{HK} = \mathrm{KH}$ donc g appartient à HK.

Finalement G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 263

Pour a et b réels on définit l'application

$$\tau_{a,b} \colon \mathbb{R} \to \mathbb{R} \qquad\qquad x \mapsto ax + b.$$

1. Soit $\mathrm{G} = \{\tau_{a,b} \mid a \neq 0\}$.

   Montrer que G est un groupe pour la composition des applications.
2. Soit $\mathrm{H} = \{\tau_{a,b} \mid a \neq 0,\ a \in \mathbb{Q}\}$.

   Montrer que H est un sous-groupe de G.
3. Décrire les classes à droite de H dans G.

   Montrer que toute classe à gauche (modulo H) est classe à droite (modulo H). (Indication : considérer l'application qui à l'élément $\tau_{a,b}$ de G associe la classe de a dans $\mathbb{R}^*/\mathbb{Q}^*$).
4. Donner un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.
5. Soit $\mathrm{N} = \{\tau_{a,b} \mid a = 1\}$.

   Montrer que N est un sous-groupe distingué de G.

Éléments de réponse 263

1. Soit $\mathrm{G} = \{\tau_{a,b} \mid a \neq 0\}$.

   Montrons que G est un groupe pour la composition des applications.

Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de G. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite G est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.

2. Soit $\mathrm{H} = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.

   Montrons que H est un sous-groupe de G.

   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de H. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite H est un sous-groupe de G.

3. Décrivons les classes à droite de H dans G et montrons que toute classe à gauche (mod H) est classe à droite (modulo H).

   La classe à droite de l'élément $\tau_{\alpha,\beta}$ de G est l'ensemble des $\tau_{\alpha a,\alpha b+\beta}$ où $a \in \mathbb{Q}$.

   Pour montrer que toute classe à gauche est une classe à droite il suffit de montrer que H est distingué dans G. Considérons le morphisme de groupes

   $$\varphi\colon \mathrm{G} \to {}^{\mathbb{R}^*}\!/_{\mathbb{Q}^*} \qquad\qquad \tau_{a,b} \mapsto \text{ la classe de } a \text{ dans } {}^{\mathbb{R}^*}\!/_{\mathbb{Q}^*}$$

   Son noyau est H qui est donc distingué dans G.

4. Donnons un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.

   Soit K le sous-groupe de G des éléments $\tau_{a,b}$ où a et b sont rationnels. Les classes à gauche et à droite de K dans G ne coïncident pas.

5. Soit $\mathrm{N} = \{\tau_{a,b} \,|\, a = 1\}$.

   Montrons que N est un sous-groupe distingué de G.

   L'identité appartient à N. Soient $\tau_{1,b}$ et $\tau_{1,b'}$ deux éléments de N. Nous avons $\tau_{1,b} \circ \tau_{1,b'}^{-1} = \tau_{1,b-b'}$; en particulier $\tau_{1,b} \circ \tau_{1,b'}^{-1}$ appartient à N. Ainsi N est un sous-groupe de G.

   Soit $\tau_{\alpha,\beta}$ un élément quelconque de G et soit $\tau_{1,b}$ un élément quelconque de N. Alors

   $$\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1} = \tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{1/\alpha,-\beta/\alpha} = \tau_{1,\alpha b};$$

   ainsi $\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1}$ appartient à N ce qui prouve que N est un sous-groupe distingué de G.

Exercice 264

Soit H un sous-groupe d'un groupe G tel que toute classe à gauche modulo H soit classe à droite modulo H. Le sous-groupe H est-il distingué ?

Éléments de réponse 264

Supposons que H ne soit pas distingué dans G. Cela signifie qu'il existe $g \in \mathrm{G} \setminus \{e\}$ tel que $g\mathrm{H} \neq \mathrm{H}g$ ou encore qu'il existe $h \in \mathrm{H}$ tel que gh n'appartient pas à $\mathrm{H}g$.

Ainsi gh appartient à une autre classe à droite que nous noterons $\mathrm{H}g'$ ($\mathrm{H}g' \neq \mathrm{H}g$). Puisque toute classe à gauche est une classe à droite et que les classes à droite forment une partition de G la classe à droite qui est égale à $g\mathrm{H}$ est nécessairement $\mathrm{H}g'$.

Donc g appartient à $g\mathrm{H}$ et $\mathrm{H}g$. Comme $g\mathrm{H} = \mathrm{H}g'$ l'élément g appartient aussi à $\mathrm{H}g'$. Autrement dit g appartient à $\mathrm{H}g \cap \mathrm{H}g'$. Ceci n'est possible que si $g = e$ ou $\mathrm{H}g = \mathrm{H}g'$. Mais par hypothèse $g \neq e$ et $\mathrm{H}g \neq \mathrm{H}g'$.

Il en résulte que H est distingué dans G.

Exercice 265

Soit G un groupe fini. Soit H un sous-groupe de G. Soit N un sous-groupe distingué de G.

Montrer que si $|\mathrm{H}|$ et $[\mathrm{G} : \mathrm{N}]$ sont premiers entre eux, alors H est un sous-groupe de N.

Éléments de réponse 265

Raisonnons par l'absurde : supposons que H ne soit pas un sous-groupe de N. Alors il existe $h \in \mathrm{H}$ qui n'est pas un élément de N. Il s'en suit que $h\mathrm{N}$ est un élément différent de l'élément neutre N de G/N.

Soit q l'ordre de $h\mathrm{N}$ dans G/N. On sait que $q \neq 1$ et que q divise $|\mathrm{G}/\mathrm{N}| = [\mathrm{G} : \mathrm{N}]$. Par ailleurs $h^{|\mathrm{H}|} = e$ donc $(h\mathrm{N})^{|\mathrm{H}|} = \mathrm{N}$. Par suite q divise $|\mathrm{H}|$. Ainsi $q \neq 1$ est un diviseur commun à $[\mathrm{G} : \mathrm{N}]$ et $|\mathrm{H}|$ qui sont premiers entre eux : contradiction. Il en résulte que H est un sous-groupe de N.

Exercice 266

Soit G un groupe qui ne contient qu'un seul sous-groupe H d'ordre n.

Montrer que H est distingué dans G.

Éléments de réponse 266

Nous allons montrer que H est un sous-groupe caractérisque de G. Soit φ un automorphisme de G et $\varphi_{|\mathrm{H}} : \mathrm{H} \to \varphi(\mathrm{H})$ la restriction de φ à H et à son image. Comme φ est un automorphisme de G, $\varphi_{|\mathrm{H}}$ est bijective. C'est donc un isomorphisme de groupes. Étant donné que H est fini d'ordre n, $\varphi(\mathrm{H})$ est fini d'ordre n. Or H est l'unique sous-groupe de G d'ordre n donc $\varphi(\mathrm{H}) = \mathrm{H}$.

Puisque H est un sous-groupe caractéristique de G c'est un sous-groupe distingué de G.

Exercice 267

Soit H un sous-groupe de G tel que le produit de deux classes à gauche modulo H soit une classe à gauche modulo H.

Le sous-groupe H est-il distingué dans G ?

Éléments de réponse 267

Comme le produit de deux classes à gauche est une classe à gauche pour tout couple (g, g') d'éléments de G il existe $g'' \in \mathrm{G}$ tel que $g\mathrm{H}g'\mathrm{H} = g''\mathrm{H}$. En particulier il existe g'' tel que $g\mathrm{H}g^{-1}\mathrm{H} = g''\mathrm{H}$. Et pour tout élément h de H il existe h' et h'' dans H tels que $ghg^{-1}h' = g''h''$. En particulier puisque e appartient à H il existe h'' dans H tel que $geg^{-1}e = g''h''$ ce qui se réécrit $e = g''h''$. Ainsi $g'' = h''^{-1} \in \mathrm{H}$ et $g\mathrm{H}g^{-1}\mathrm{H} = \mathrm{H}$, c'est-à-dire $g\mathrm{H}g^{-1} = \mathrm{H}$. Le sous-groupe H est donc distingué dans G.

Exercice 268

Soit G un groupe. Soit H un sous-groupe distingué de G.

Montrer que si H est cyclique tout sous-groupe de H est distingué dans G.

Éléments de réponse 268

Soit h un générateur de H. Soit K un sous-groupe du groupe cyclique distingué H. Alors tous les éléments de K sont égaux à une puissance de h et K est lui-même cyclique engendré par une puissance de h : posons $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$. Soit h^p un élément de K. Nous avons $p = qp_0 + r$ avec $0 \leq r < p_0$. Par suite $h^p = (h^{p_0})^q h^r$ et $h^r = h^p (h^{-p_0})^q$ appartient à K. Puisque $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$ nous avons nécessairement $r = 0$ et $\mathrm{K} = \langle h^{p_0} \rangle$.

Puisque H est distingué dans G pour tout $g \in \mathrm{G}$ il existe q tel que $ghg^{-1} = h^q$. Par conséquent $gh^{p_0}g^{-1} = h^{qp_0}$ et K est distingué dans G.

Exercice 269

Soient A un groupe et C un sous-groupe distingué de A. Soient B un groupe et D un sous-groupe distingué de B.

Montrer que ${}^{\mathrm{A} \times \mathrm{B}}\!/_{\mathrm{C} \times \mathrm{D}} \simeq {}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Éléments de réponse 269

Considérons le morphisme de groupes entre $\mathrm{A} \times \mathrm{B}$ et ${}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$ donné par

$$\varphi((a,b)) = (a\mathrm{C}, b\mathrm{D}).$$

Le noyau de φ est égal à

$$\begin{aligned} \ker\varphi &= \{(a,b) \in \mathrm{A} \times \mathrm{B} \,|\, a\mathrm{C} = \mathrm{C} \text{ et } b\mathrm{D} = \mathrm{D}\} \\ &= \{(a,b) \in \mathrm{A} \times \mathrm{B} \,|\, a \in \mathrm{C} \text{ et } b \in \mathrm{D}\} \\ &= \mathrm{C} \times \mathrm{D}. \end{aligned}$$

Par ailleurs $(a\mathrm{C}, b\mathrm{D})$ est l'image de (a,b) par φ donc φ est surjectif. Il en résulte que φ induit un isomorphisme entre ${}^{\mathrm{A} \times \mathrm{B}}\!/_{\mathrm{C} \times \mathrm{D}}$ et ${}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Exercice 270

Soient G_1 et G_2 deux groupes non isomorphes.

1. Montrer que $Z(\mathrm{G}_1) \times Z(\mathrm{G}_2)$ est isomorphe à $Z(\mathrm{G}_1 \times \mathrm{G}_2)$.
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrer que $\mathrm{G}_1 \times \mathrm{G}_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   (b) Montrer que si H est un sous-groupe distingué de $\mathrm{G}_1 \times \mathrm{G}_2$, alors $\mathrm{H} \cap \mathrm{H}_1$ est distingué dans H_1 et $\mathrm{H} \cap \mathrm{H}_2$ est distingué dans H_2.
   (c) En déduire que H_1 et H_2 sont les seuls sous-groupes distingués de $\mathrm{G}_1 \times \mathrm{G}_2$.

Éléments de réponse 270

1. Montrons que $Z(\mathrm{G}_1) \times Z(\mathrm{G}_2)$ est isomorphe à $Z(\mathrm{G}_1 \times \mathrm{G}_2)$.
   Soit $(x_1, x_2) \in \mathrm{G}_1 \times \mathrm{G}_2$; alors (x_1, x_2) appartient à $Z(\mathrm{G}_1 \times \mathrm{G}_2)$ si et seulement si
   $$\forall\, (y_1, y_2) \in \mathrm{G}_1 \times \mathrm{G}_2 \qquad (x_1, x_2)(y_1, y_2) = (y_1, y_2)(x_1, x_2)$$
   si et seulement si
   $$\forall\, (y_1, y_2) \in \mathrm{G}_1 \times \mathrm{G}_2 \qquad (x_1 y_1, x_2 y_2) = (y_1 x_1, y_2 x_2)$$
   si et seulement si
   $$\forall\, (y_1, y_2) \in \mathrm{G}_1 \times \mathrm{G}_2 \qquad x_1 y_1 = y_1 x_1 \text{ et } x_2 y_2 = y_2 x_2.$$
   Par conséquent (x_1, x_2) appartient à $Z(\mathrm{G}_1 \times \mathrm{G}_2)$ si et seulement si x_1 appartient à $Z(\mathrm{G}_1)$ et x_2 appartient à $Z(\mathrm{G}_2)$. Ainsi
   $$Z(\mathrm{G}_1 \times \mathrm{G}_2) \simeq Z(\mathrm{G}_1) \times Z(\mathrm{G}_2).$$
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrons que $\mathrm{G}_1 \times \mathrm{G}_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   Soit $\mathrm{H}_1 = \mathrm{G}_1 \times \{e_2\}$ où e_2 est l'élément neutre de G_2. Le groupe H_1 est un sous-groupe de $\mathrm{G}_1 \times \mathrm{G}_2$ isomorphe à G_1. De plus H_1 est distingué dans $\mathrm{G}_1 \times \mathrm{G}_2$ car pour tout $(x_1, x_2) \in \mathrm{G}_1 \times \mathrm{G}_2$, pour tout $(x, e_2) \in \mathrm{H}_1$ nous avons
   $$(x_1, x_2)(x, e_2)(x_1, x_2)^{-1} = (x_1, x_2)(x, e_2)(x_1^{-1}, x_2^{-1}) = (x_1 x x_1^{-1}, x_2 x_2^{-1}) = (x_1 x x_1^{-1}, e_2)$$
   et $(x_1, x_2)(x, e_2)(x_1, x_2)^{-1}$ appartient à H_1.
   De même $\mathrm{H}_2 = \{e_1\} \times \mathrm{G}_2$ est un sous-groupe distingué de $\mathrm{G}_1 \times \mathrm{G}_2$.
   (b) Montrons que si H est un sous-groupe distingué de $\mathrm{G}_1 \times \mathrm{G}_2$, alors $\mathrm{H} \cap \mathrm{H}_1$ est distingué dans H_1 et $\mathrm{H} \cap \mathrm{H}_2$ est distingué dans H_2.
   Soit $(x_1, e_2) \in \mathrm{H}_1$ et soit $(x, e_2) \in \mathrm{H} \cap \mathrm{H}_1$; nous avons
   $$(x_1, e_2)(x, e_2)(x_1, e_2)^{-1} = (x_1, e_2)(x, e_2)(x_1^{-1}, e_2) = (x_1 x x_1^{-1}, e_2)$$
   donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H_1. Par ailleurs H est un sous-groupe distingué de $\mathrm{G}_1 \times \mathrm{G}_2$ donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H. Finalement $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à $\mathrm{H} \cap \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_1$ est un sous-groupe distingué de H_1.
   De même $\mathrm{H} \cap \mathrm{H}_2$ est un sous-groupe distingué de H_2.
   (c) Les sous-groupes H_1 et H_2 sont isomorphes à G_1 et G_2 respectivement. Les groupes G_1 et G_2 étant simples les groupes H_1 et H_2 sont aussi simples. Il y a donc quatre cas possibles qui sont les suivants :
      i) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{G}_1 \times \mathrm{G}_2$.
      ii) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \mathrm{H}_1$.
      iii) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{H}_2$.

iv) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \{(e_1, e_2)\}$. En effet $\mathrm{HH}_1/\mathrm{H}_1$ (qui est isomorphe à H) est distingué dans G/H_1, groupe qui est lui-même isomorphe à G_2.

De la même façon nous obtenons que si H n'est pas trivial il est isomorphe à G_1.

Ainsi si H n'est pas trivial, il est isomorphe à G_1 et à G_2 et G_1 et G_2 sont isomorphes : contradiction. Par conséquent $\mathrm{H} = \{(e_1, e_2)\}$.

Ainsi les seuls sous-groupes distingués propres de $\mathrm{G}_1 \times \mathrm{G}_2$ sont H_1 et H_2.

Exercice 271

Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'en posant $g \cdot a\mathrm{H} = (ga)\mathrm{H}$, où a, $g \in \mathrm{G}$, on définit une action de G sur l'ensemble G/H des classes à gauche modulo H.

(b) Montrer que cette action est transitive.

Déterminer le stabilisateur de aH.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Éléments de réponse 271

(a) Posons $X = \mathrm{G}/\mathrm{H}$. Soient g dans G et x dans X. Désignons par a, a' deux représentants de la classe à gauche x. On a $a\mathrm{H} = a'\mathrm{H} = x$ ou encore $a^{-1}a' \in \mathrm{H}$. Or

$$(ga)^{-1}ga' = a^{-1}g^{-1}ga' = a^{-1}a' \in \mathrm{H}$$

donc $ga\mathrm{H} = ga'\mathrm{H}$.

Si on remplace a par un autre représentant a' de la classe $x = a\mathrm{H}$, alors $ga'\mathrm{H} = ga\mathrm{H}$. La formule a donc bien un sens et définit une application de $\mathrm{G} \times X \to X$.

C'est bien une action de G sur X puisque

- $\forall\, x = a\mathrm{H} \in X$ nous avons $e \cdot x = ea\mathrm{H} = a\mathrm{H} = x$,
- $\forall\, x = a\mathrm{H} \in X$, $\forall\, g \in \mathrm{G}$, $\forall\, g' \in \mathrm{G}$ nous avons

$$g \cdot (g' \cdot x) = g \cdot (g'a\mathrm{H}) = g(g'a)\mathrm{H} = (gg')a\mathrm{H} = gg' \cdot x$$

(b) Pour tous $x = a\mathrm{H} \in X$ et $y = b\mathrm{H} \in X$ il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.

Le stabilisateur de $x = a\mathrm{H}$ est $a\mathrm{H}a^{-1}$ car :

$$g \in \mathrm{G}_x \iff ga\mathrm{H} = a\mathrm{H} \iff a^{-1}ga\mathrm{H} = \mathrm{H} \iff a^{-1}ga \in \mathrm{H} \iff g \in a\mathrm{H}a^{-1}.$$

(c) Comme $\mathrm{G}_x = a\mathrm{H}a^{-1} = \mathrm{Ad}_a(\mathrm{H}) \simeq \mathrm{H}$, on retrouve le théorème de Lagrange

$$[\mathrm{G} : \mathrm{H}] = \mathrm{card}\left(\mathrm{G}/\mathrm{H}\right) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[\mathrm{G} : 1]}{[\mathrm{G}_x : 1]} = \frac{[\mathrm{G} : 1]}{[\mathrm{H} : 1]}.$$

Exercice 272

Soient p un nombre premier et $a > 1$. En utilisant une action de groupe que l'on précisera montrer que tout groupe G d'ordre p^a admet un élément central (*i.e.* qui commute avec tout élément de G) d'ordre p.

Éléments de réponse 272

Faisons agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites on a donc $|Z(\mathrm{G})| \equiv 0 \bmod p$, ce qui interdit à $Z(\mathrm{G})$ d'être trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{e\}$, alors g est d'ordre p^b pour un certain $1 \leq b \leq a$. Alors $g^{p^{b-1}}$ appartient à $Z(\mathrm{G})$ et est d'ordre p.

Exercice 273

Soit G un groupe. Soient H et K deux sous-groupes de G tels que $\mathrm{K} \subset \mathrm{H} \subset \mathrm{G}$.

a) Supposons que G soit fini. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

b) On ne suppose plus que G est fini. On suppose par contre que H et K sont distingués dans G. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

Éléments de réponse 273

a) Comme G est fini, on a

$$|\mathrm{G}| = |\mathrm{G} : \mathrm{H}|\,|\mathrm{H}| \qquad |\mathrm{H}| = |\mathrm{H} : \mathrm{K}|\,|\mathrm{K}| \qquad |\mathrm{G}| = |\mathrm{G} : \mathrm{K}|\,|\mathrm{K}|$$

L'ordre d'un groupe n'est jamais nul donc $|\mathrm{K}| \neq 0$ et

$$|\mathrm{G} : \mathrm{K}| = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{|\mathrm{G} : \mathrm{H}|\,|\mathrm{H}|}{|\mathrm{K}|} = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

b) Les groupes G/H et $\mathrm{G}/\mathrm{K}/\mathrm{H}/\mathrm{K}$ sont isomorphes donc $\left|\mathrm{G}/\mathrm{H}\right| = \left|\mathrm{G}/\mathrm{K}/\mathrm{H}/\mathrm{K}\right|$ soit $|\mathrm{G} : \mathrm{H}| = \left|\mathrm{G}/\mathrm{K} : \mathrm{H}/\mathrm{K}\right|$ d'où $|\mathrm{G} : \mathrm{H}| \left|\mathrm{H}/\mathrm{K}\right| = \left|\mathrm{G}/\mathrm{K}\right|$, *i.e.*

$$|\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| = |\mathrm{G} : \mathrm{K}| .$$

Exercice 274

Soit G un groupe. Les assertions suivantes sont-elles vraies ou fausses ? Justifier.

a) Si tout sous-groupe H de G est distingué dans G, alors G est abélien.

b) Si $\mathrm{H} \triangleleft \mathrm{G}$ et $\mathrm{K} \triangleleft \mathrm{H}$, alors $\mathrm{K} \triangleleft \mathrm{G}$.

c) Soient g et h dans G d'ordre fini. Alors gh est d'ordre fini.

d) Si G a un nombre fini de sous-groupes, alors G est fini.

e) Si H et K sont des sous-groupes de G, alors $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

Éléments de réponse 274

a) Faux. Considérons le groupe $\mathbb{H}_8$ des quaternions. Rappelons qu'il est défini de la façon suivante : $\mathbb{H}_8$ est l'ensemble

$$\mathbb{H}_8 = \{ \pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k} \}$$

et la loi de groupe est définie par

$$(-1)^2 = 1,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$
$$(-1)\cdot\mathbf{i} = \mathbf{i}\cdot(-1) = -\mathbf{i},\ (-1)\cdot\mathbf{j} = \mathbf{j}\cdot(-1) = -\mathbf{j},\ (-1)\cdot\mathbf{k} = \mathbf{k}\cdot(-1) = -\mathbf{k}$$
$$\mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i} = \mathbf{k}.$$

Les sous-groupes de $\mathbb{H}_8$ sont

— le sous-groupe trivial $\{\mathrm{id}\}$ qui est distingué dans $\mathbb{H}_8$,

— le sous-groupe d'ordre 2 engendré par -1 qui est distingué dans $\mathbb{H}_8$ car contenu dans le centre de $\mathbb{H}_8$,

— les sous-groupes d'ordre 4 sont d'indice 2 dans $\mathbb{H}_8$ donc distingués dans $\mathbb{H}_8$,

— le sous-groupe $\mathbb{H}_8$ entier qui est distingué dans $\mathbb{H}_8$.

Les sous-groupes de $\mathbb{H}_8$ sont donc tous distingués dans $\mathbb{H}_8$ mais $\mathbb{H}_8$ n'est pas abélien.

b) Faux. Considérons par exemple $\mathrm{G} = \mathfrak{S}_4$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 2)(3\ 4)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple il faut que le groupe G soit infini et non abélien. Prenons par exemple $\mathrm{G} = \mathrm{GL}(2,\mathbb{Q})$, $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'élément g est d'ordre 2, l'élément h est d'ordre 3 mais $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

d) Vrai. Tout élément de G est d'ordre fini : si g est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$ et contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques notés $\langle g_1 \rangle, \ldots, \langle g_n \rangle$. Donc pour tout g dans G il existe i tel que $\langle g \rangle = \langle g_i \rangle$, autrement dit g est une puissance de g_i. Ceci assure que le cardinal de G est borné par la somme des ordres des g_i. Il s'en suit que G est fini.

e) Faux. L'inclusion $\mathrm{HK} \subset \langle \mathrm{H} \cup \mathrm{K} \rangle$ est toujours vérifiée. En revanche le sous-ensemble HK n'est en général pas un sous-groupe de G contrairement à $\langle \mathrm{H} \cup \mathrm{K} \rangle$. En effet prenons par exemple $\mathrm{G} = \mathfrak{S}_3$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 3)\}$. Alors $\langle \mathrm{H} \cup \mathrm{K} \rangle$ coïncide avec G et $\mathrm{HK} = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$ n'est pas un sous-groupe de G.

La réponse est vraie si l'on suppose que H ou K est distingué dans G (exercice).

Exercice 275

Soit S un sous-ensemble non vide d'un groupe fini G. Soit $N(S) = \{g \in \mathrm{G} \,|\, gSg^{-1} = S\}$ le normalisateur de S dans G. Soit $C(S) = \{g \in \mathrm{G} \,|\, \forall\, s \in S,\, gsg^{-1} = s\}$ le centralisateur de S dans G.

Montrer que

a) $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$.

b) $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

c) Si $\mathrm{H} \lhd \mathrm{G}$, alors $C(\mathrm{H}) \lhd \mathrm{G}$.

d) Si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Éléments de réponse 275

a) Montrons que $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$. Bien sûr e appartient à $N(S)$. Soient g et h dans $N(S)$. Alors

$$(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$$

donc gh appartient à $N(S)$. Si g appartient à $N(S)$ on a $gSg^{-1} = S$ donc en multipliant à gauche et à droite par g^{-1} et g respectivement on a $S = g^{-1}Sg$, autrement dit g^{-1} appartient à $N(S)$. Ainsi $N(S)$ est un sous-groupe de G.

De même $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons que $C(S)$ est distingué dans $N(S)$. Soient $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors

$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}$$

et comme h appartient à $N(S)$, on a $h^{-1}sh$ appartient à S. Donc puisque g appartient à $C(S)$

$$g(h^{-1}sh)g^{-1} = h^{-1}sh$$

et finalement

$$(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s.$$

Ainsi hgh^{-1} appartient à $C(S)$ et $C(S) \lhd N(S)$.

b) Montrons que $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

Supposons que $N(S) = \mathrm{G}$. Alors pour tout $g \in \mathrm{G}$, on a $gSg^{-1} = S$ donc $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

Réciproquement supposons que $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$. Pour tout $g \in \mathrm{G}$ nous avons $g^{-1}Sg \subset S$ donc en multipliant par g et g^{-1} à gauche et à droite respectivement nous avons $S \subset gSg^{-1} \subset S$ d'où $S = gSg^{-1}$. Ainsi g appartient à $N(S)$ et $\mathrm{G} = N(S)$.

c) Montrons que si $\mathrm{H} \triangleleft \mathrm{G}$, alors $C(\mathrm{H}) \triangleleft \mathrm{G}$. Supposons que H soit distingué dans G. Soient g dans G, c dans $C(\mathrm{H})$ et h dans H. Nous avons

$$(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$$

puisque H est distingué dans G nous savons que $g^{-1}hg$ appartient à H. Or c appartient à $C(\mathrm{H})$ donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$ et finalement

$$(gcg^{-1})h(gcg^{-1})^{-1}$$

ce qui assure que gcg^{-1} appartient à $C(\mathrm{H})$. Le groupe $C(\mathrm{H})$ est donc distingué dans G.

d) Montrons que si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Par définition et a) $N(\mathrm{H})$ est un sous-groupe de G contenant H et H est distingué dans $N(\mathrm{H})$. Considérons un sous-groupe K de G contenant H tel que $\mathrm{H} \triangleleft \mathrm{K}$. Par définition nous avons $k\mathrm{H}k^{-1} = \mathrm{H}$ pour tout $k \in \mathrm{K}$. Par conséquent k appartient à $N(\mathrm{H})$ donc $\mathrm{K} \subset N(\mathrm{H})$ ce qui assure la maximalité de $N(\mathrm{H})$ parmi les sous-groupes de G concernés.

Exercice 276

Soit G un groupe. Désignons par Aut(G) le groupe des automorphismes de G. Si a appartient à G, notons $\varphi(a)$ l'application

$$\varphi(a)\colon \mathrm{G} \to \mathrm{G} \qquad\qquad g \mapsto aga^{-1}.$$

a) Montrer que pour tout a dans G l'application $\varphi(a)$ est un automorphisme de G (appelé automorphisme intérieur de G).

b) Montrer que $\varphi\colon \mathrm{G} \to \mathrm{Aut(G)}$, $g \mapsto \varphi(g)$ est un morphisme de groupes de G dans Aut(G).

c) Notons Int(G) l'ensemble des automorphismes intérieurs de G. Montrer que Int(G) est un sous-groupe distingué de Aut(G).

d) Notons $Z(\mathrm{G})$ le centre de G. Montrer que $\mathrm{Int(G)} \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Éléments de réponse 276

a) Il faut montrer que $\varphi(a)$ est un morphisme de G dans G ; bien sûr $\varphi(a)(e) = e$. Il reste donc à montrer que $\varphi(a)(gg') = \varphi(a)(g)\varphi(a)(g')$. Or

$$\varphi(a)(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \varphi(a)(g)\varphi(a)(g').$$

Montrons que $\ker \varphi(a) = \{e\}$. Soit $g \in \ker \varphi(a)$, alors $\varphi(a)(g) = e$, autrement dit $aga^{-1} = e$ d'où $g = a^{-1}a = e$. Ainsi $\varphi(a)$ est un morphisme injectif.

Soit g dans G. On a $g = a(a^{-1}ga)a^{-1} = \varphi(a)(a^{-1}ga)$. Autrement dit $\varphi(a)$ est surjectif.

Il en résulte que $\varphi(a)$ est un automorphisme de G et $(\varphi(a))^{-1} = \varphi(a^{-1})$.

b) D'une part $\varphi(e)(g) = ege^{-1} = g$, *i.e.* $\varphi(e) = \mathrm{id}$. D'autre part
$$\varphi(a) \circ \varphi(a')(g) = a(a'ga'^{-1})a^{-1} = (aa')g(aa')^{-1} = \varphi(aa')(g)$$
c'est-à-dire $\varphi(a) \circ \varphi(a') = \varphi(aa')$. Par suite φ est un morphisme de groupes de G dans Aut(G).

c) Int(G) est l'image de G par le morphisme de groupes φ ; c'est donc un sous-groupe de Aut(G).

Soit τ un automorphisme de G ; alors
$$\tau \circ \varphi(a) \circ \tau^{-1}(g) = \tau(a\tau^{-1}(g)a^{-1}) = \tau(a)\tau(\tau^{-1}(g))\tau(a^{-1}) = \tau(a)g\tau(a^{-1})$$
Ainsi $\tau \circ \varphi(a) \circ \tau^{-1} = \varphi(\tau(a))$ appartient à $\operatorname{Im}\varphi$. Le groupe Int(G) est distingué dans Aut(G).

d) D'une part $\ker\varphi$ est le centre $Z(\mathrm{G})$ de G [4], d'autre part $\operatorname{Im}\varphi = \mathrm{Int}(\mathrm{G})$ (voir c)). Le théorème d'isomorphisme assure que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Exercice 277

Soit G un groupe et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ en fonction de ceux de G.

b) Soit K un sous-groupe de G.

i) Si K est distingué dans G et contient H, montrer que
$${}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{K}}\!/_{\mathrm{H}} \simeq {}^{\mathrm{G}}\!/_{\mathrm{K}}$$

ii) Montrer que HK est un sous-groupe de G égal à KH.

iii) Montrer que H est distingué dans HK.

iv) Montrer que
$${}^{\mathrm{K}}\!/_{(\mathrm{K} \cap \mathrm{H})} \simeq {}^{\mathrm{HK}}\!/_{\mathrm{H}}.$$

Éléments de réponse 277

Soit G un groupe et soit $H \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrivons les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ en fonction de ceux de G. On note $\pi : \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. La correspondance $K \mapsto \pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ donc la réciproque est donnée par $\overline{K} \mapsto \pi^{-1}(\overline{K})$. Cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

b) Soit K un sous-groupe de G.

4. $\ker\varphi = \{g \in \mathrm{G} \mid \varphi(g) = \mathrm{id}\} = \{g \in \mathrm{G} \mid \forall h \in \mathrm{G},\ \varphi(g)(h) = h\} = \{g \in \mathrm{G} \mid \forall h \in \mathrm{G},\ ghg^{-1} = h\} = \{g \in \mathrm{G} \mid \forall h \in \mathrm{G},\ gh = hg\} = Z(\mathrm{G})$

i) Supposons que K soit distingué dans G et que K contienne H. Montrons que

$$\mathrm{G}/\mathrm{H}^{\mathrm{K}}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$$

Le morphisme $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ composé avec la projection $\pi'\colon \mathrm{G}/\mathrm{H} \to (\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$ induit un morphisme surjectif $q\colon \mathrm{G} \to (\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$. Par construction un élément g de G appartient à $\ker q$ si et seulement si $\pi(g)$ appartient à $\ker \pi' = \mathrm{K}/\mathrm{H}$ si et seulement si g appartient à K. Ainsi $\ker q = \mathrm{K}$. Le théorème de factorisation assure alors que q induit un isomorphisme entre $\mathrm{G}/\ker q = \mathrm{G}/\mathrm{K}$ et $(\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$.

ii) Montrons que HK est un sous-groupe de G égal à KH.

Soient h, h' dans H et k, k' dans K. Le groupe H étant distingué dans G il existe h'' dans H tel que $k \cdot h' = h'' \cdot k$. Par suite

$$(h \cdot k) \cdot (h' \cdot k') = (h \cdot h'') \cdot (k \cdot k')$$

appartient à HK et HK est un sous-groupe de G.

iv) Montrons que $\mathrm{K}/(\mathrm{K} \cap \mathrm{H})$ et $(\mathrm{HK})/\mathrm{H}$ sont isomorphes. L'inclusion $\mathrm{K} \to \mathrm{HK}$ induit un morphisme $p\colon \mathrm{K} \to (\mathrm{HK})/\mathrm{H}$. Montrons que p est surjectif : si h est dans H et k dans K, alors la classe $(h \cdot k)\mathrm{H} = k\mathrm{H}$ est l'image de k par p, donc p est surjectif. De plus un élément $k \in \mathrm{K}$ appartient à $\ker p$ si et seulement si il est dans H. Autrement dit $\ker p = \mathrm{K} \cap \mathrm{H}$. On conclut à l'aide du théorème de factorisation.

Exercice 278

Soit G un groupe fini. Soient H et K des sous-groupes de G. Supposons que

— H et K sont des sous-groupes distingués de G ;

— $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que HK est un sous-groupe distingué de G d'ordre $|\mathrm{H}||\mathrm{K}|$.

Éléments de réponse 278

Montrons tout d'abord que HK est un sous-groupe de G. On définit l'application φ par

$$\varphi\colon \mathrm{H} \times \mathrm{K} \to \mathrm{HK} \qquad\qquad (h,k) \mapsto hk.$$

Cette application est injective. En effet soient h, h' dans H et k, k' dans K tels que $f(h,k) = f(h',k')$, *i.e.* $hk = h'k'$. On en déduit que $hh'^{-1} = k'k^{-1}$; de plus $hh'^{-1} = k'k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e\}$. Donc $hh'^{-1} = e$ et $kk'^{-1} = e$ c'est-à-dire $(h,k) = (h',k')$. Cette application est par définition surjective. Soient h, h' dans H et soient k, k' dans K. Puisque K est distingué il existe k_1 dans K tel que $hk = k_1 h$. Comme H est distingué il existe h_1 dans H tel que $k_1 h = h_1 k_1$. Ainsi $hk = h_1 k_1$. Mais φ est injective d'où $h = h_1$, $k = k_1$ et h et k commutent ($hk = kh$). Donc $hkh'k' = hh'kk'$. On en déduit que

— HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et si $g \in \mathrm{HK}$, alors $g^{-1} \in \mathrm{HK}$;

— φ est un morphisme de groupes.

En particulier φ est un isomorphisme de groupes.

Montrons que HK est distingué dans G. Soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Alors

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h_1(gkg^{-1})$$

avec h_1 dans H car H est distingué dans G. Par ailleurs $h_1gkg^{-1} = h_1k_1$ avec k_1 dans K car K est distingué dans G. Donc $ghkg^{-1}$ appartient à HK et HK est distingué dans G.

Montrons que HK est d'ordre |H||K|. Comme φ est un isomorphisme de groupes l'ordre de HK est celui de $\mathrm{H} \times \mathrm{K}$, *i.e.* |H||K|.

Exercice 279

Soit G un groupe de centre $Z(\mathrm{G})$.

a) Montrer que $Z(\mathrm{G})$ est un sous-groupe distingué de G.

b) Montrer que si ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène (*i.e.* ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est engendré par un seul élément), alors G est abélien.

Éléments de réponse 279

a) Le centre de G est un sous-groupe de G. En effet si $x \in Z(\mathrm{G})$ et $y \in Z(\mathrm{G})$, alors $y^{-1} \in Z(\mathrm{G})$ et pour tout élément g de G on a $xy^{-1}g = xgy^{-1} = gxy^{-1}$ ce qui implique que xy^{-1} appartient à $Z(\mathrm{G})$.

Par ailleurs soit $g \in \mathrm{G}$ et soit $c \in Z(\mathrm{G})$. Comme c commute avec tous les éléments de G nous avons

$$gcg^{-1} = cgg^{-1} = c.$$

Donc $gZ(\mathrm{G})g^{-1} = Z(\mathrm{G})$ et $Z(\mathrm{G})$ est un sous-groupe distingué dans G.

b) Si $\mathrm{G} = Z(\mathrm{G})$, alors G est abélien. Si $\mathrm{G} \neq Z(\mathrm{G})$ et si ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène non trivial, alors il existe un élément x de G tel que $x \notin Z(\mathrm{G})$ et ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} = \langle xZ(\mathrm{G})\rangle$. Soit y dans G. Ou bien $y \in Z(\mathrm{G})$ et $xy = yx$. Ou bien $y \notin Z(\mathrm{G})$ et il existe $n \in \mathbb{N}$ tel que $y \in (xZ(\mathrm{G}))^n = x^nZ(\mathrm{G})$, autrement dit $y = x^nc$ avec $c \in Z(\mathrm{G})$. Dans ce cas $xy = xx^nc = x^ncx = yx$. Ainsi x commute avec tous les éléments de G, *i.e.* $x \in Z(\mathrm{G})$: contradiction. Ainsi $\mathrm{G} = Z(\mathrm{G})$ et G est abélien.

Exercice 280

On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}(2,\mathbb{C})$, appelé *groupe des quaternions* engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad K = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

1. Calculer l'ordre de $\mathbb{H}_8$.

2. Exhiber les sous-groupes de $\mathbb{H}_8$.
3. Exhiber les sous-groupes distingués de $\mathbb{H}_8$.
4. Est-il isomorphe au groupe diédral D_8 ?

Éléments de réponse 280

1. On vérifie que

$$I^2 = J^2 = K^2 = -\mathrm{id}, \quad IJ = K, \quad IK = -J, \quad JK = I, \quad JI = -K, \quad KI = J, \quad KJ = -I.$$

Par conséquent le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id}, -\mathrm{id}, I, -I, J, -J, K, -K\}.$$

En particulier il est d'ordre 8.

2. Commençons par rappeler le théorème de Lagrange

Soit G un groupe fini. Soit H un sous-groupe fini de G. Alors |H| et |[G : H]| divisent |G|.

D'après le théorème de Lagrange les sous-groupes propres de $\mathbb{H}_8$ sont d'ordre 2 ou 4. Il y a un seul sous-groupe d'ordre 2 : $\langle -\mathrm{id}\rangle$ et trois sous-groupes d'ordre 4 : $\langle I\rangle$, $\langle J\rangle$, $\langle K\rangle$.

3. Commençons par :

Rappel : Soit G un groupe. Soit H un sous-groupe de G. Le groupe H est un sous-groupe distingué de G s'il est invariant par automorphisme intérieur, *i.e.* si $$\forall\, a \in \mathrm{G} \quad \forall\, h \in \mathrm{H} \quad aha^{-1} \in \mathrm{H}.$$ Si H est distingué dans G, on note $\mathrm{H} \triangleleft \mathrm{G}$. Remarque : la condition ci-dessus équivaut à dire que pour tout $a \in \mathrm{G}$ $a\mathrm{H} = \mathrm{H}a$ *i.e.* égalité des classes à gauche et à droite modulo H.

Tous les sous-groupes de $\mathbb{H}_8$ sont distingués.

En effet, $\langle \mathrm{id}\rangle$ et $\mathbb{H}_8$ sont bien entendu distingués dans $\mathbb{H}_8$.

Vérifions que $\langle -\mathrm{id}\rangle$ est distingué dans $\mathbb{H}_8$: d'une part

$$\forall\, A \in \mathbb{H}_8 \quad A\mathrm{id}A^{-1} = AA^{-1} = \mathrm{id} \in \langle -\mathrm{id}\rangle$$

d'autre part comme $-\mathrm{id}$ commute à tout élément de $\mathbb{H}_8$ nous avons

$$\forall\, A \in \mathbb{H}_8 \quad A(-\mathrm{id})A^{-1} = (-\mathrm{id})AA^{-1} = -\mathrm{id} \in \langle -\mathrm{id}\rangle.$$

Vérifions par exemple que $\langle J\rangle = \{\mathrm{id}, -\mathrm{id}, J, -J\}$ est distingué dans $\mathbb{H}_8$:

- ◇ Pour tout g dans $\mathbb{H}_8$ nous avons $g\mathrm{id}g^{-1} = gg^{-1} = \mathrm{id} \in \langle J\rangle$.

◇ Pour tout g dans $\mathbb{H}_8$ nous avons $g(-\mathrm{id})g^{-1} = -gg^{-1}$ car $-\mathrm{id}$ commute à tout élément de $\mathbb{H}_8$; il s'en suit que pour tout g dans $\mathbb{H}_8$ nous avons $g(-\mathrm{id})g^{-1} = -\mathrm{id} \in \langle J\rangle$.

◇ Montrons que pour tout $g \in \mathbb{H}_8$ gJg^{-1} appartient à $\langle J\rangle$:

- $\mathrm{id}J\mathrm{id}^{-1} = \mathrm{id}J\mathrm{id} = J \in \langle J\rangle$
- $(-\mathrm{id})J(-\mathrm{id})^{-1} = (-\mathrm{id})J(-\mathrm{id}) = J \in \langle J\rangle$
- $IJ\underbrace{I^{-1}}_{-I} = IJ(-I) = \underbrace{(IJ)}_{K}(-I) = K(-I) = -KI = -J \in \langle J\rangle$
- $(-I)J(-I)^{-1} = (-\mathrm{id}I)J(-\mathrm{id}I)^{-1} = -\mathrm{id}IJI^{-1}(-\mathrm{id})^{-1} = -\mathrm{id}IJI^{-1}(-\mathrm{id}) = IJI^{-1} = -J \in \langle J\rangle$
- $JJJ^{-1} = (JJ)J^{-1} = J^2J^{-1} = (-\mathrm{id})J^{-1} = -J^{-1} = J \in \langle J\rangle$
- $(-J)J(-J)^{-1} = JJJ^{-1} = J \in \langle J\rangle$
- $KJ\underbrace{K^{-1}}_{-K} = \underbrace{KJ}_{-I}(-K) = (-I)(-K) = IK = -J \in \langle J\rangle$
- $(-K)J(-K)^{-1} = KJK^{-1} = -J \in \langle J\rangle$

◇ Il reste à montrer pour tout $g \in \mathbb{H}_8$ $g(-J)g^{-1}$ appartient à $\langle J\rangle$. Pour tout $g \in \mathbb{H}_8$ nous avons $g(-J)g^{-1} = g(-\mathrm{id})Jg^{-1} = -\mathrm{id}gJg^{-1}$ car $-\mathrm{id}$ commute à tout élément de $\mathbb{H}_8$. Autrement dit pour tout $g \in \mathbb{H}_8$ nous avons $g(-J)g^{-1} = g(-\mathrm{id})Jg^{-1} = -gJg^{-1}$. Or d'une part d'après ce qui précède gJg^{-1} appartient à $\langle J\rangle$ pour tout $g \in \mathbb{H}_8$ et d'autre part si h appartient à $\langle J\rangle$, alors $-h$ appartient à $\langle J\rangle$. Ainsi $g(-J)g^{-1}$ appartient à $\langle J\rangle$ pour tout $g \in \mathbb{H}_8$.

Un raisonnement analogue montre que $\langle I\rangle$ et $\langle K\rangle$ sont distingués dans $\mathbb{H}_8$.

4. Soit $n \geq 3$. Le groupe diédral D_{2n} d'ordre $2n$ est le sous-groupe de $\mathrm{O}(2,\mathbb{R})$ engendré par la rotation r d'angle $\frac{2\pi}{n}$ et la symétrie σ autour de l'axe des abscisses dans $\mathbb{R}^2$. Autrement dit il s'agit du groupe engendré par les matrices

$$r = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

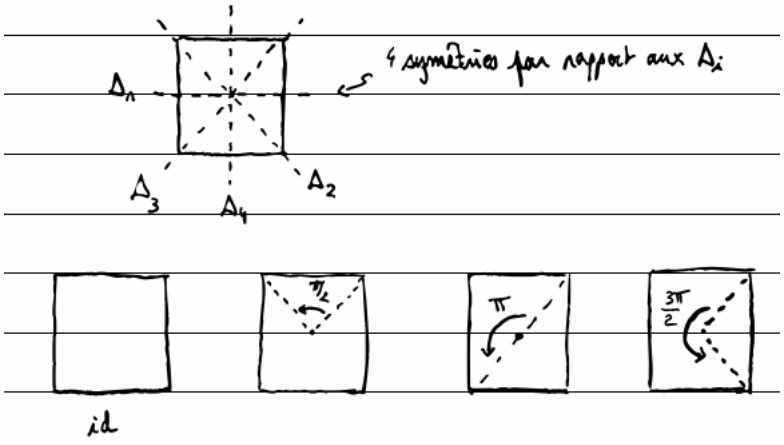
Puisque r et σ laissent invariant l'ensemble des sommets du polyèdre régulier à n côtés, noté P_n, le groupe D_{2n} laisse invariant P_n.

La rotation r engendre le groupe des rotations d'angle $\frac{2k\pi}{n}$ avec $0 \leq k \leq n-1$ et donc $\langle r\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. De plus $\sigma^2 = \mathrm{id}$ ainsi $\langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Un calcul montre que $\sigma r\sigma^{-1} = \sigma r\sigma = r^{-1}$ et par récurrence nous obtenons $\sigma r^k\sigma^{-1} = r^{-k}$. Par suite tous les éléments de $\langle r, \sigma\rangle$ sont de la forme r^k ou $r^k\sigma$. Par conséquent

$$\mathrm{D}_{2n} = \{r^k,\, r^k\sigma \,|\, 0 \leq k \leq n-1\}.$$

Le groupe D_8 est donc le groupe des isométries du plan euclidien préservant un carré :



Rappelons aussi que si $f\colon \mathrm{G} \to \mathrm{H}$ est un morphisme de groupes et si g est un élément de G, alors pour tout entier relatif k nous avons $f(g^k) = (f(g))^k$. En particulier, l'ordre de $f(g)$ divise l'ordre de g. En effet, si g est d'ordre ℓ, alors $g^\ell = e_\mathrm{G}$ et $f(g^\ell) = f(e_\mathrm{G})$. Comme f est un morphisme $f(g^\ell) = (f(g))^\ell$ et $f(e_\mathrm{G}) = e_\mathrm{H}$ donc $f(g^\ell) = f(e_\mathrm{G})$ se réécrit $(f(g))^\ell = e_\mathrm{H}$: l'ordre de $f(g)$ divise ℓ qui est l'ordre de g. Si de plus f est un isomorphisme de groupes, alors g est d'ordre k si et seulement $f(g)$ est d'ordre k. En effet, f étant un morphisme l'ordre de $f(g)$ divise l'ordre de g et f^{-1} étant un morphisme l'ordre de g divise l'ordre de $f(g)$; par conséquent l'ordre de g coïncide avec l'ordre de $f(g)$. En particulier, deux groupes isomorphes ont le même nombre d'éléments d'ordre d.

Le groupe diédral D_8 compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.

Exercice 281

Soit Q_8 le groupe des matrices 2×2 inversibles engendré par $\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$ et $\begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$. Ce groupe est appelé le groupe des quaternions.

a) Quel est l'ordre de Q_8 ?

b) Montrer que Q_8 n'a qu'un élément d'ordre 2.

c) Quel est le centre de Q_8 ?

d) Montrer que tous les sous-groupes de Q_8 sont distingués.

e) Peut-on trouver un isomorphisme entre Q_8 et un produit semi-direct de $\mathbb{Z}/4\mathbb{Z}$ avec $\mathbb{Z}/2\mathbb{Z}$?

Éléments de réponse 281

Posons $\mathcal{I} = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$, $\mathcal{J} = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$, $\mathcal{K} = \mathcal{I}\mathcal{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a) On vérifie que Id est l'élément neutre,

$$-\mathrm{Id}M = -M \quad \forall\, M \in \{\mathcal{I}, \mathcal{J}, \mathcal{K}\} \qquad \mathcal{I}^2 = \mathcal{J}^2 = \mathcal{K}^2 = -\mathrm{Id}$$
$$\mathcal{I}\mathcal{J} = \mathcal{K},\ \mathcal{J}\mathcal{K} = \mathcal{I},\ \mathcal{K}\mathcal{I} = \mathcal{J} \qquad \mathcal{J}\mathcal{I} = -\mathcal{K},\ \mathcal{K}\mathcal{J} = -\mathcal{I},\ \mathcal{I}\mathcal{K} = -\mathcal{J}$$

Il en résulte que Q_8 contient 8 élements.

b) D'après ce qui précède l'unique élément d'ordre 2 est $-\mathrm{Id}$.

c) D'après ce qui précède le centre de Q_8 est $\{\mathrm{Id}, -\mathrm{Id}\}$.

d) Les sous-groupes de Q_8 sont le groupe trivial, le centre de Q_8 et

$$\langle\mathcal{I}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{I}, -\mathcal{I}\} \qquad \langle\mathcal{J}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{J}, -\mathcal{J}\} \qquad \langle\mathcal{K}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{K}, -\mathcal{K}\}$$

e) Les groupes $\langle\mathcal{I}\rangle$, $\langle\mathcal{J}\rangle$ et $\langle\mathcal{K}\rangle$ sont tous trois cycliques d'ordre 4 donc isomorphes à $\mathbb{Z}/4\mathbb{Z}$ mais aucun d'entre eux ne peut être un facteur semi-direct de Q_8 car l'autre facteur serait d'ordre 2 et d'intersection réduite à $\{\mathrm{Id}\}$ avec le facteur d'ordre 4. Or tous ces sous-groupes d'ordre 4 contiennent le sous-groupe d'ordre 2. Par conséquent Q_8 ne peut s'obtenir comme produit semi-direct de deux de ses sous-groupes propres.

Exercice 282

Soit G un groupe d'ordre 55 possédant deux sous-groupes distingués d'ordre 5 et 11 respectivement. Montrer que G est isomorphe à $\mathbb{Z}/55\mathbb{Z}$.

Éléments de réponse 282

Si H et K sont d'ordre respectif 5 et 11, alors $\mathrm{H} \cap \mathrm{K} = \{e\}$ (en effet tous les éléments de $\mathrm{H} \setminus \{e\}$ sont d'ordre 5 et tous les éléments de $\mathrm{K} \setminus \{e\}$ sont d'ordre 11.

L'exercice **??** assure que HK est un sous-groupe de G d'ordre $5 \times 11 = 55$ qui est l'ordre de G. Il en résulte que $\mathrm{G} = \mathrm{HK}$. Alors HK est isomorphe à $\mathrm{H} \times \mathrm{K}$. Par suite G est isomorphe à $\mathrm{H} \times \mathrm{K}$. Or H est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et K est isomorphe à $\mathbb{Z}/11\mathbb{Z}$ donc G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} = \mathbb{Z}/55\mathbb{Z}$ (théorème chinois).

Exercice 283

Soit G un groupe agissant sur un ensemble X. Soit $\phi\colon \mathrm{G} \to \mathfrak{S}_X$ le morphisme de groupes associé.

1. Montrer que le stabilisateur d'un élément de X est toujours un sous-groupe de G.
2. Décrire le noyau d'une action à l'aide des stabilisateurs.
3. Montrer que si une action n'est pas fidèle, alors on peut définir une action de $\mathrm{G}/\ker\phi$ qui l'est.

Éléments de réponse 283

1. Soit x un élément de X. Alors son stabilisateur est
$$\mathrm{St}(x) = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$
Montrons que $\mathrm{St}(x)$ est un sous-groupe de G :
   - ◇ e appartient à $\mathrm{St}(x)$: en effet $g \cdot e = g$.
   - ◇ soient g et g' dans $\mathrm{St}(x)$, alors d'une part $g \cdot x = x$, d'autre part $g' \cdot x = x$. Il en résulte que
   $$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$$
   i.e. gg' appartient à $\mathrm{St}(x)$.
   - ◇ soit g dans $\mathrm{St}(x)$; alors $g \cdot x = x$ et
   $$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
   c'est-à-dire g^{-1} appartient à $\mathrm{St}(x)$.

   Il en résulte que $\mathrm{St}(x)$ est un sous-groupe de G.

2. Le noyau de ϕ, formé de tous les g tels que, pour tout x, $g \cdot x = x$, est l'intersection de tous les stabilisateurs.

3. Soit $\phi\colon \mathrm{G} \to \mathfrak{S}_X$ le morphisme de groupes associé à l'action de G sur X. Montrons que si une action n'est pas fidèle on peut définir une action de $\mathrm{G}/\ker\phi$ qui l'est.

   Si une action n'est pas fidèle, c'est que ϕ n'est pas un morphisme injectif. Le premier théorème d'isomorphisme assure qu'on peut définir un morphisme injectif de $\mathrm{G}/\ker\phi$ dans $\mathfrak{S}_X$ le groupe symétrique de X.

Exercice 284 [Formule de Burnside et coloriage de polyèdres]

1. Soit G un groupe fini agissant sur un ensemble fini X. Pour tout $x \in X$ on désigne par $\mathcal{O}_x$ l'orbite de x par l'action de G et par G_x son stabilisateur.
   a) Soient $x \in X$ et $y \in \mathcal{O}_x$. Trouvez $z \in \mathrm{G}$ tel que
   $$\mathrm{G}_y = z^{-1}\mathrm{G}_x z.$$
   b) Montrer que pour tout $x \in X$
   $$|\mathrm{G}| = \sum_{y \in \mathcal{O}_x} |\mathrm{G}_y|.$$
   c) En déduire que
   $$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{x \in X} |\mathrm{G}_x|$$
   où $\Omega = \{\mathcal{O}_x \,|\, x \in X\}$ est l'ensemble des orbites dans X par l'action de G.

d) En décomposant de deux façons différentes l'ensemble $F = \{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\}$ déduire de la question précédente la formule de Burnside

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

où $\mathrm{Fix}(g)$ est l'ensemble des points $x \in X$ tels que $g \cdot x = x$.

2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où k couleurs sont disponibles, à chaque face et à chaque arête étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel $\mathbb{R}^3$ et on le suppose centré en 0.

Nous identifions deux coloriages du tétraèdre s'il existe une rotation R de l'espace euclidien $\mathbb{R}^3$ qui préserve le tétraèdre, *i.e.* $R(T) = T$, et qui envoie le premier coloriage sur le second.

a) Soit X l'ensemble des coloriages où on interdit cette identification. Quel est le cardinal de X ?

b) Montrer que l'ensemble des rotations préservant T, muni de la loi de composition, est un groupe.

Notons G ce groupe. On admet qu'il est fini et plus précisément que $|\mathrm{G}| = 12$:

- l'identité $\mathrm{id}_{\mathbb{R}^3}$;
- 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
- 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.

c) Le groupe G agit naturellement sur X, et chaque coloriage du tétraèdre correspond à une orbite $\mathcal{O}_x$ dans X par l'action de G. Exprimer le nombre de coloriages du tétraèdre en fonction de k.

Éléments de réponse 284

1. a) Soient $x \in X$ et $y \in \mathcal{O}_x$. Il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$. Soit $w \in \mathrm{G}_x$, alors $w \cdot x = x$. D'une part $w \cdot x = w \cdot (g^{-1}y)$, d'autre part $x = g^{-1}y$. Par conséquent $w \cdot x = x$ se réécrit $w \cdot (g^{-1}y) = g^{-1}y$ ou encore $(gwg^{-1}) \cdot y = y$; autrement dit gwg^{-1} appartient à G_y et $g\mathrm{G}_x g^{-1} \subset \mathrm{G}_y$. Un raisonnement analogue conduit à $\mathrm{G}_y \subset g\mathrm{G}_x g^{-1}$. Il s'en suit que $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ et que $z = g^{-1}$ convient.

b) D'après a) $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ donc $|\mathrm{G}_y| = |\mathrm{G}_x|$ et

$$\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = \sum_{y \in \mathcal{O}_x} |\mathrm{G}_x| = |\mathrm{G}_x| \sum_{y \in \mathcal{O}_x} 1 = |\mathrm{G}_x|\,|\mathcal{O}_x|.$$

Or l'application

$$\mathrm{G}/\mathrm{G}_x \to \mathcal{O}_x, \qquad \overline{g} \mapsto g \cdot x$$

est bien définie et est une bijection ; par smeuite $\left|\mathrm{G}/\mathrm{G}_x\right| = |\mathcal{O}_x|$, *i.e.* $|\mathrm{G}| = |\mathcal{O}_x|\,|\mathrm{G}_x|$. Ainsi $\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.

c) Nous avons

$$\sum_{x\in X} |\mathrm{G}_x| = \sum_{\mathcal{O}_x\subset\Omega} \sum_{y\in\mathcal{O}_x} |\mathrm{G}_y|.$$

D'après b) $\sum_{y\in\mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$ d'où

$$\sum_{x\in X} |\mathrm{G}_x| = \sum_{\mathcal{O}_x\subset\Omega} |\mathrm{G}| = |\mathrm{G}| \sum_{\mathcal{O}_x\subset\Omega} 1 = |\mathrm{G}|\,|\Omega|.$$

Finalement

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{x\in X} |\mathrm{G}_x|.$$

d) Le groupe G est fini ; désignons par g_1, g_2, …, g_p ses éléments. L'ensemble X est fini ; désignons par x_1, x_2, …, x_q ses éléments. D'une part

$$\begin{aligned} F &= \{(g,x) \in \mathrm{G}\times X \,|\, g\cdot x = x\} \\ &= \{(g,x) \in \mathrm{G}\times X \,|\, x \in \mathrm{Fix}(g)\} \\ &= \Big(\{g_1\}\times \mathrm{Fix}(g_1)\Big) \cup \Big(\{g_2\}\times \mathrm{Fix}(g_2)\Big) \cup \ldots \cup \Big(\{g_p\}\times \mathrm{Fix}(g_p)\Big) \end{aligned}$$

d'où $|F| = \sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)|$.

D'autre part

$$\begin{aligned} F &= \{(g,x) \in \mathrm{G}\times X \,|\, g\cdot x = x\} \\ &= \{(g,x) \in \mathrm{G}\times X \,|\, g \in \mathrm{G}_x\} \\ &= \Big(\mathrm{G}_{x_1}\times \{x_1\}\Big) \cup \Big(\mathrm{G}_{x_2}\times \{x_2\}\Big) \cup \ldots \cup \Big(\mathrm{G}_{x_q}\times \{x_q\}\Big) \end{aligned}$$

d'où $|F| = \sum_{x\in X} |\mathrm{G}_x|$. Par conséquent $\sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)| = \sum_{x\in X} |\mathrm{G}_x|$. Mais c) assure que $|\Omega|\,|\mathrm{G}| = \sum_{x\in X} |\mathrm{G}_x|$. donc

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)|$$

2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où k couleurs sont disponibles, à chaque face et à chaque arête

étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel $\mathbb{R}^3$ et on le suppose centré en 0.

Nous identifions deux coloriages du tétraèdre s'il existe une rotation R de l'espace euclidien $\mathbb{R}^3$ qui préserve le tétraèdre, *i.e.* $R(T) = T$, et qui envoie le premier coloriage sur le second.

a) Soit X l'ensemble des coloriages où on interdit cette identification. Quel est le cardinal de X ?

Un tétraèdre régulier a quatre faces S_1, S_2, S_3, S_4 et six arêtes A_1, A_2, …, A_6. En particulier il y a dix objets à colorier. On a donc $|X| = k^{10}$.

b) Montrons que l'ensemble des rotations préservant T, muni de la loi de composition, est un groupe.

Voir cours.

Notons G ce groupe. On admet qu'il est fini et plus précisément que $|\mathrm{G}| = 12$:

- l'identité $\mathrm{id}_{\mathbb{R}^3}$;
- 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
- 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.

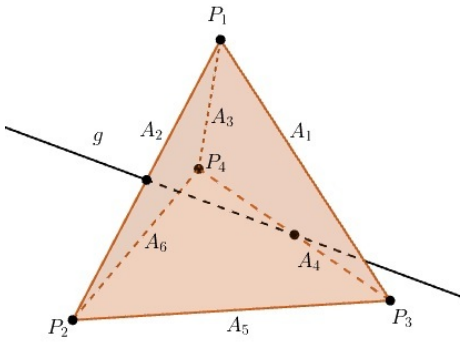
c) Le groupe G agit naturellement sur X, et chaque coloriage du tétraèdre correspond à une orbite $\mathcal{O}_x$ dans X par l'action de G. Exprimons le nombre de coloriages du tétraèdre en fonction de k.

Appliquons la formule de Burnside : soit n le nombre de coloriages, ou de manière équivalente le nombre d'orbites de G sur X. Alors

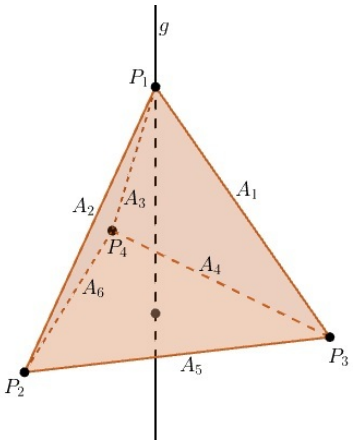
$$n = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

Trois cas sont à distinguer :

- Si $g = \mathrm{id}$, alors $\mathrm{Fix}(g) = X$; par suite $|\mathrm{Fix}(g)| = |X| = k^{10}$.
- Si g est l'une des trois rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π. Alors $|\mathrm{Fix}(g)| = k^6$.



- Si g est l'une des huit rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm\frac{2\pi}{3}$. Par conséquent $|\mathrm{Fix}(g)| = k^4$.



Finalement

$$n = \frac{1}{12}\left(k^{10} + 3 \cdot k^6 + 8 \cdot k^4\right)$$

Exercice 285

1. Soit G un groupe fini qui opère sur un ensemble fini non vide E. Supposons que G soit d'ordre p^m avec p premier et $m \in \mathbb{N}^*$. Posons

   $$E^{\mathrm{G}} = \{x \in E \,|\, \forall\, g \in \mathrm{G},\, g \cdot x = x\}.$$

   Montrer que $|E^{\mathrm{G}}| = |E| \bmod p$.

2. Soit H un groupe fini d'ordre n. Soit p un diviseur premier de n. Montrer que H contient un élément d'ordre p (lemme de Cauchy). Indication : on introduit l'ensemble

   $$E = \{(x_1, x_2, \ldots, x_p) \in \mathrm{H}^p \,|\, x_1 x_2 \ldots x_p = e\}.$$

i) Calculer le cardinal de E.

ii) Montrer que $\mathbb{Z}/p\mathbb{Z}$ agit naturellement sur E et que chaque orbite a un ou p éléments. À quoi correspondent les orbites à un élément ?

iii) En déduire le résultat.

3. Soit H un groupe fini d'ordre n. Soit $m \in \mathbb{N}^*$ tel que pour tout $x \in \mathrm{H}$ on ait $x^m = e$. Montrer que n divise une puissance de m.

Éléments de réponse 285

1. Si x appartient à E, nous notons $\mathcal{O}_x$ l'orbite de x sous l'action de G. Les éléments de E^{G} sont exactement les éléments x de E tels que $\mathcal{O}_x = \{x\}$. Notons ω_1, ω_2, …, ω_r les orbites de E de cardinal strictement supérieur à 1. Rappelons que $|\omega_i|$ divise $|\mathrm{G}|$, par suite $|\omega_i|$ est une puissance de p différente de 1. Il résulte de l'équation aux classes que

$$|E| = |E^{\mathrm{G}}| + \sum_{i=1}^{r} |\omega_i| \equiv |E^{\mathrm{G}}| \mod p$$

2. i) L'ensemble E est de cardinal n^{p-1} car les $p-1$ premiers éléments de la liste $(x_1, x_2, \ldots, x_p)$ déterminent le dernier, $x_p = (x_1 x_2 \ldots x_{p-1})^{-1}$.

ii) Le groupe $\mathbb{Z}/p\mathbb{Z}$ agit sur E par

$$k \cdot (x_1, x_2, \ldots, x_p) = (x_{k+1}, x_{k+2}, \ldots, x_{k+p})$$

avec la convention que les indices sont pris modulo p. C'est l'action naturelle de $\langle\sigma\rangle$ où $\sigma = (1\ 2\ \ldots\ p)$ est une permutation circulaire. Il faut néanmoins vérifier que nous avons encore $x_{k+1}x_{k+2}\ldots x_{k+p} = e$. Cela se voit facilement par récurrence : soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$.

Soit $x = (x_1, x_2, \ldots, x_p) \in E$. L'orbite de x est réduite à un point lorsque $x_1 = x_2 = \ldots = x_p = \zeta$; un tel élément ζ vérifie $\zeta^p = e$; soit $\zeta = e$, soit ζ est d'ordre p puisque p est premier.

iii) Appliquons alors le résultat obtenu à la question 1. ; nous avons $|E| \equiv |E^{\mathbb{Z}/p\mathbb{Z}}| \mod p$. Comme p divise n, $|E^{\mathbb{Z}/p\mathbb{Z}}|$ est nul modulo p. Or $E^{\mathbb{Z}/p\mathbb{Z}}$ est formé des éléments dont l'orbite est réduite à 1 ; donc $E^{\mathbb{Z}/p\mathbb{Z}}$ contient le p-uplet $(e, e, \ldots, e)$, $E^{\mathbb{Z}/p\mathbb{Z}}$ est non vide et $E^{\mathbb{Z}/p\mathbb{Z}}$ a un cardinal supérieur à p. Il y a donc au moins $(p-1)$ éléments d'ordre p dans H.

3. Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m. Soit p un premier divisant n. Le lemme de Cauchy garantit l'existence d'un élément $h \in \mathrm{H}$ d'ordre p. Or par hypothèse $h^m = e$ donc p divise m.

Exercice 286

Soit G un groupe fini. Soit p le plus petit nombre premier divisant $|\mathrm{G}|$. Soit H un sous-groupe de G d'indice p. On se propose de montrer que H est distingué dans G.

a) Montrer que H opère sur l'ensemble des classes à gauche ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ pour tout $h \in \mathrm{H}$ et pour tout $a \in \mathrm{G}$.

Quel est le stabilisateur de $a\mathrm{H}$?

Quelle est l'orbite de la classe H ?

b) Montrer que si H n'était pas distingué dans G, alors au moins une des orbites aurait un cardinal $\geq p$.

c) Conclure.

Éléments de réponse 286

a) Commençons par rappeler

Soit G un groupe. Soit X un ensemble. On dit que G opère sur X si on s'est donné une application

$$\mathrm{G} \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

vérifiant les axiomes suivants :

1) $\forall\, g,\, g' \in \mathrm{G},\, \forall\, x \in X,\, g \cdot (g' \cdot x) = (gg') \cdot x$

2) $\forall\, x \in X,\, 1 \cdot x = x$.

Remarque : il revient au même de se donner un morphisme de groupes $\varphi\colon \mathrm{G} \to \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ désigne le groupe des bijections de X, on pose alors : $g \cdot x = \varphi(g)(x)$.

On peut vérifier que $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ est bien définie : si $a\mathrm{H} = b\mathrm{H}$, alors $(ha)\mathrm{H} = (hb)\mathrm{H}$ donc $h \cdot (a\mathrm{H})$ ne dépend pas du représentant a choisi dans une même classe à gauche, et que ceci définit une action de groupe :

- ◇ pour tous $g,\, g' \in \mathrm{H}$ nous avons $g \cdot (g' \cdot a\mathrm{H}) = g \cdot ((g'a)\mathrm{H}) = (gg'a)\mathrm{H}$ et $(gg') \cdot (a\mathrm{H}) = (gg'a)\mathrm{H}$;
- ◇ $e \cdot (a\mathrm{H}) = (ea)\mathrm{H} = a\mathrm{H}$ pour tout $a\mathrm{H} \in {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Soit G un groupe agissant sur un ensemble X. Si x appartient à X, nous définissons

$$\mathrm{Stab}(x) = \{g \in \mathrm{G} \mid g \cdot x = x\}$$

C'est un sous-groupe de G (non distingué en général) appelé le stabilisateur de x.

Le stabilisateur de $a\mathrm{H}$ est

$$\begin{aligned}\mathrm{Stab}(a\mathrm{H}) &= \{h \in \mathrm{H} \,|\, h \cdot (a\mathrm{H}) = a\mathrm{H}\} \\ &= \{h \in \mathrm{H} \,|\, (ha)\mathrm{H} = a\mathrm{H}\} \\ &= \{h \in \mathrm{H} \,|\, a^{-1}ha \in \mathrm{H}\} \\ &= \{h \in \mathrm{H} \,|\, h \in a\mathrm{H}a^{-1}\} \\ &= \mathrm{H} \cap a\mathrm{H}a^{-1}.\end{aligned}$$

Soit G un groupe agissant sur un ensemble X. L'orbite d'un élément $x \in X$ sous l'action de G est

$$\mathcal{O}_x = \{g \cdot x \,|\, g \in \mathrm{G}\}.$$

L'orbite de H est réduite à H :

$$\mathcal{O}_\mathrm{H} = \{h \cdot \mathrm{H} \,|\, h \in \mathrm{H}\} = \{h\mathrm{H} \,|\, h \in \mathrm{H}\} = \mathrm{H}.$$

b) Si H n'est pas distingué dans G, alors il y a au moins une orbite dont le cardinal n'est pas 1 puisque cela signifie qu'il existe $a \in \mathrm{G}$ et $h \in \mathrm{H}$ tel que $a^{-1}(ha)$ n'appartient pas à H. Puisque le cardinal de cette orbite divise celui de H (donc aussi celui de G par le théorème de Lagrange) ce cardinal est au moins p étant donné que p est le plus petit diviseur premier de $|\mathrm{G}|$.

c) Si H n'est pas distingué dans G, alors il y a au moins une orbite de cardinal au moins p mais il y a aussi une orbite de cardinal 1 : celle de H.

Rappel : soit K un groupe agissant sur un ensemble X ; X est réunion disjointe des orbites de X sous l'action de K, *i.e.* $|X| = \sum_{i=1}^{p} |\mathcal{O}_i|$ où les $\mathcal{O}_i$ sont les orbites de X sous l'action de K.

Puisque H opère sur l'ensemble des classes à gauche, nous avons $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| \geq p+1$: contradiction avec le fait que $\underbrace{[\mathrm{G} : \mathrm{H}]}_{\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right|} = p$.

Exercice 287

Soit E un espace vectoriel de dimension finie n sur un corps $\Bbbk$.

a) Faisons agir le groupe linéaire $\mathrm{G} = \mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par $g \cdot F := g(F)$ pour tout $g \in \mathrm{G}$ et tout sous-espace F de E. Quelles sont les orbites pour cette action ?

b) On prend $\Bbbk = {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

Éléments de réponse 287

a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement, si F et G sont des sous-espaces de dimension d, on choisit une base $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0$, $1, \ldots, n$.

b) Fixons un sous-espace F de dimension 3 (on sait qu'il y en a au moins 1). D'après a) le nombre cherché est le cardinal de l'orbite de F sous l'action de $\mathrm{GL}(E)$ ou encore l'ordre de $\mathrm{GL}(E)$ divisé par celui du stabilisateur S de F. Le cardinal de $\mathrm{GL}(E)$ est obtenu en comptant le nombre de bases de E, il vaut

$$(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4).$$

En prenant une base de F que l'on complète en une base de E on voit que S est isomorphe au groupe des matrices-bloc de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où $A \in \mathrm{GL}(3, \mathbb{F}_7)$, $B \in \mathrm{M}_{3,2}(\mathbb{F}_7)$ et $C \in \mathrm{GL}(2, \mathbb{F}_7)$. Ainsi

$$|S| = (7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6.$$

Par suite le cardinal cherché est

$$\begin{aligned} &\frac{(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4)}{(7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6}\mathbb{N}onumber \\ &\quad = \frac{7\times 7^2\times 7^3\times 7^4\times (7^5-1)(7^4-1)(7^3-1)(7^2-1)(7-1)}{7\times 7^2\times 7\times 7^6\times (7^3-1)(7^2-1)(7-1)(7^2-1)(7-1)} \\ &\quad = \frac{(7^5-1)(7^4-1)}{(7^2-1)(7-1)} \\ &\quad = 140050 \end{aligned}$$

Exercice 288

a) Combien y a-t-il d'actions du groupe $\mathbb{Z}/4\mathbb{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?

b) Soient G et X deux groupes. On dit que G *opère par automorphismes sur* X si on s'est donné une action $(g, x) \mapsto g\cdot x$ de G sur X telle que pour tout $g \in$ G l'application $x \mapsto g\cdot x$ soit un automorphisme de X.

L'action de G sur lui-même par translation est-elle une action par automorphismes ?

L'action de G sur lui-même par conjugaison est-elle une action par automorphismes ?

c) Si $G = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathbb{Z}/13\mathbb{Z}, +\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

d) Si $G = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathfrak{S}_3, \circ\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

Éléments de réponse 288

a) On cherche le nombre de morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans le groupe des permutations $\mathfrak{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\overline{1})$) dans $\mathfrak{S}_5$. Or $\mathfrak{S}_5$ contient
   - un élément d'ordre 1 (l'identité),
   - $\binom{5}{2} = 10$ transpositions,
   - $5 \cdot 3 = 15$ doubles transpositions (cinq façons de choisir le point fixe puis trois double transpositions avec les quatre éléments restants),
   - $5 \cdot 6 = 30$ 4-cycles (cinq façons de choisir le point fixe et six 4-cycles dans le groupe des permutations des quatre éléments restants).

   Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.

b) L'action de G sur lui-même par translation n'est pas une action par automorphismes.

   L'action de G sur lui-même par conjugaison est une action par automorphismes.

c) Le groupe des automorphismes de X est isomorphe au groupe multiplicatif de l'anneau $\mathbb{Z}/13\mathbb{Z}$ (en effet, si on pose $\varphi_a(x) = ax$ on peut vérifier que $a \mapsto \varphi_a$ est un isomorphisme de $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ sur $\mathrm{Aut}(X)$) lequel est isomorphe au groupe additif $\mathbb{Z}/12\mathbb{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ou encore le nombre d'éléments de $\mathbb{Z}/12\mathbb{Z}$ d'ordre divisant 3. Il y a ainsi 3 possibilités.

d) Les seuls automorphismes de $\mathfrak{S}_3$ sont intérieurs. Le groupe des automorphismes de $\mathfrak{S}_3$ est donc isomorphe à $\mathfrak{S}_3$ quotienté par son centre, c'est-à-dire à $\mathfrak{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathfrak{S}_3$ et il y a 3 possibilités.

Exercice 289

Soit E un espace euclidien. On fait agir le groupe orthogonal $\mathrm{O}(E)$ de E sur l'ensemble des sous-espaces vectoriels de E.

a) Quelles sont les orbites pour cette action ?

b) Donner un énoncé analogue pour les espaces hermitiens.

c) Y a-t-il un énoncé analogue pour le groupe orthogonal $\mathrm{O}(q)$ d'un espace vectoriel de dimension finie muni d'une forme quadratique non dégénérée q ?

Éléments de réponse 289

a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement si F et G sont des sous-espaces de dimension d, on choisit une base orthonormée $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base orthonormée $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base orthonormée $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base orthonormée $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \ldots, n$.

b) Idem en remplaçant le groupe orthogonal de E par le groupe unitaire de E.

c) Il est clair que si F est un sous-espace une condition nécessaire pour qu'un autre sous-espace G soit dans l'orbite de F est que les restrictions de q à F et G soient des formes quadratiques isomorphes (ce qui entraîne en particulier $\dim F = \dim G$ mais n'est pas équivalent à cette condition). Cette condition est en fait suffisante mais c'est un énoncé difficile, le théorème de Witt.

Exercice 290

Soit G un groupe. Soit g un élément de G. On appelle *centralisateur* de g l'ensemble G_g des éléments h de G tels que $hg = gh$.

a) Montrer que G_g est un sous-groupe de G. Est-il toujours distingué ?

b) Supposons que G soit fini. Soit C_g la classe de conjugaison de g. Trouver une relation entre $|\mathrm{G}|$, $|C_g|$ et $|\mathrm{G}_g|$.

Éléments de réponse 290

a) Il est immédiat que $\mathrm{G}_g = \{h \in \mathrm{G} \,|\, hg = gh\}$ est un sous-groupe de G :

- ◇ e appartient à G_g donc G_g n'est pas vide ;
- ◇ soient h et h' dans G_g alors

$$(hh')g = h(h'g) \overset{h' \in \mathrm{G}_g}{=} h(gh') = (hg)h' \overset{h \in \mathrm{G}_g}{=} (gh)h' = g(hh')$$

- ◇ soit h dans G_g, alors $hg = gh$ d'où $h^{-1}(hg)h^{-1} = h^{-1}(gh)h^{-1}$ soit $(h^{-1}h)gh^{-1} = h^{-1}g(hh^{-1})$ ou encore $gh^{-1} = h^{-1}g$, *i.e.* h^{-1} appartient à G_g.

Mais G_g n'est pas toujours distingué dans G : par exemple le centralisateur d'une transposition τ n'est pas distingué dans $\mathfrak{S}_3$; en effet si $\mathfrak{S}_3 = \mathfrak{S}(\{1, 2, 3\})$, nous notons $\tau_1 = (2\ 3)$ et $\tau_2 = (1\ 3)$; on peut vérifier que

- ◇ $\mathrm{G}_{\tau_1} = \{\tau_1, \mathrm{id}\}$ et
- ◇ G_{τ_1} n'est pas un sous-groupe distingué de $\mathfrak{S}_3$ car $\tau_2\tau_1\tau_2^{-1}$ n'appartient pas à G_{τ_1}.

b) Le groupe G opère par conjugaison sur lui-même. Par définition C_g est l'orbite de g et G_{g_0} son stabilisateur d'où

$$|\mathrm{G}| = |C_g| \cdot |\mathrm{G}_g|.$$

Exercice 291

Soit G un groupe agissant sur un ensemble X. Si (g, x) appartient à $\mathrm{G} \times X$ quelle relation peut-on écrire entre $\mathrm{St}(x)$ et $\mathrm{St}(g \cdot x)$?

Éléments de réponse 291

Nous avons $\mathrm{St}(g \cdot x) = g \cdot \mathrm{St}(x) \cdot g^{-1}$.

Exercice 292

Soit G un groupe d'ordre 33 agissant sur un ensemble X de cardinal 19. Montrer qu'il existe une orbite de cardinal 1.

Éléments de réponse 292

Utiliser la formule des classes.

Exercice 293

Pour chaque polyèdre régulier et convexe $\mathcal{P}$ d'un espace euclidien $\mathcal{E}$ de dimension 3 déterminer le nombre d'isométries de $\mathcal{E}$ préservant $\mathcal{P}$.

Éléments de réponse 293

Le groupe $\mathrm{Isom}(\mathcal{P})$ agit transitivement sur $\mathcal{P}$; il suffit donc de déterminer l'ordre du stabilisateur d'un sommet de $\mathcal{P}$.

Exercice 294

1. Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E = \{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\},$$

calculer le nombre moyen de points fixes d'un élément de G. Que dire en particulier si l'action est transitive ? Que dire de la moyenne du nombre de points fixes d'une permutation aléatoire ?

2. Combien de colliers de 9 perles différents peut-on faire avec 4 perles bleues, 3 perles blanches et 2 perles oranges ?

Éléments de réponse 294

1. Désignons par $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points fixes de g dans X.

◇ Soient $x \in X$ et $y \in \mathcal{O}_x$. Montrons que G_y et G_x sont conjugués.

Il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$. Soit $w \in \mathrm{G}_x$, alors $w \cdot x = x$. D'une part $w \cdot x = w \cdot (g^{-1}y)$, d'autre part $x = g^{-1}y$. Par conséquent $w \cdot x = x$ se réécrit $w \cdot (g^{-1}y) = g^{-1}y$ ou encore $(gwg^{-1}) \cdot y = y$; autrement dit gwg^{-1} appartient à G_y et $g\mathrm{G}_x g^{-1} \subset \mathrm{G}_y$. Un raisonnement analogue conduit à $\mathrm{G}_y \subset g\mathrm{G}_x g^{-1}$. Il s'en suit que $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$.

◇ D'après ce qui précède $\mathrm{G}_y = g\mathrm{G}_x g^{-1}$ donc $|\mathrm{G}_y| = |\mathrm{G}_x|$ et

$$\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = \sum_{y \in \mathcal{O}_x} |\mathrm{G}_x| = |\mathrm{G}_x| \sum_{y \in \mathcal{O}_x} 1 = |\mathrm{G}_x|\,|\mathcal{O}_x|.$$

Or l'application

$$\mathrm{G}/\mathrm{G}_x \to \mathcal{O}_x, \qquad \overline{g} \mapsto g \cdot x$$

est bien définie et est une bijection ; par suite $\left|\mathrm{G}/\mathrm{G}_x\right| = |\mathcal{O}_x|$, *i.e.* $|\mathrm{G}| = |\mathcal{O}_x|\,|\mathrm{G}_x|$. Ainsi $\displaystyle\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.

◇ Nous avons

$$\sum_{x \in X} |\mathrm{G}_x| = \sum_{\mathcal{O}_x \subset \Omega} \sum_{y \in \mathcal{O}_x} |\mathrm{G}_y|$$

où $\Omega = \{\mathcal{O}_x \,|\, x \in X\}$ est l'ensemble des orbites de l'action de G sur X. D'après b) $\displaystyle\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$ d'où

$$\sum_{x \in X} |\mathrm{G}_x| = \sum_{\mathcal{O}_x \subset \Omega} |\mathrm{G}| = |\mathrm{G}| \sum_{\mathcal{O}_x \subset \Omega} 1 = |\mathrm{G}|\,|\Omega|.$$

Finalement

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{x \in X} |\mathrm{G}_x|.$$

◇ D'une part

$$\begin{aligned} E &= \{(g,x) \in \mathrm{G} \times X \,|\, g \cdot x = x\} \\ &= \{(g,x) \in \mathrm{G} \times X \,|\, x \in \mathrm{Fix}(g)\} \\ &= \Big(\{g_1\} \times \mathrm{Fix}(g_1)\Big) \cup \Big(\{g_2\} \times \mathrm{Fix}(g_2)\Big) \cup \ldots \cup \Big(\{g_p\} \times \mathrm{Fix}(g_p)\Big) \end{aligned}$$

d'où $|E| = \displaystyle\sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$.

D'autre part

$$\begin{aligned} E &= \{(g,x) \in \mathrm{G} \times X \,|\, g \cdot x = x\} \\ &= \{(g,x) \in \mathrm{G} \times X \,|\, g \in \mathrm{G}_x\} \\ &= \Big(\mathrm{G}_{x_1} \times \{x_1\}\Big) \cup \Big(\mathrm{G}_{x_2} \times \{x_2\}\Big) \cup \ldots \cup \Big(\mathrm{G}_{x_q} \times \{x_q\}\Big) \end{aligned}$$

d'où $|E| = \sum_{x\in X} |\mathrm{G}_x|$. Par conséquent $\sum_{g\in \mathrm{G}} |\mathrm{Fix}(g)| = \sum_{x\in X} |\mathrm{G}_x|$. Mais d'après ce qui précède $|\Omega|\,|\mathrm{G}| = \sum_{x\in X} |\mathrm{G}_x|$. donc

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{g\in \mathrm{G}} |\mathrm{Fix}(g)|$$

Cela signifie que le nombre moyen de points fixes d'un élément de G est exactement $|\Omega|$, *i.e.* le nombre d'orbites de l'action.

En particulier si l'action est transitive ce nombre vaut 1.

Par exemple si $\mathrm{G} = \mathfrak{S}_n$ agit (via l'action évidente) sur $X = \{1, 2, \ldots, n\}$, alors le nombre moyen de points fixes d'une permutation est exactement 1.

2. On représente un collier par un cercle du plan euclidien orienté $\mathbb{R}^2$ (de centre O et de rayon 1) muni de neuf points A_1, A_2, …, A_9 disposés à intervalles réguliers.

Deux colliers sont dits équivalents si et seulement si on peut obtenir l'un à partir de l'autre en effectuant une rotation plane du collier ou en le retournant (comme une crêpe) dans l'espace de dimension 3.

Autrement dit l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges, est muni d'une action du groupe diédral $\mathrm{G} = \mathrm{D}_{18}$ des isométries d'un polygône régulier à neuf côtés. Ce groupe G est donc un sous-groupe de $\mathrm{SO}(2,\mathbb{R})$, il est d'ordre 18 et ses éléments sont les suivants

$$\mathrm{G} = \{\mathrm{id},\, r,\, r^2,\, r^3,\, r^4,\, r^5,\, r^6,\, r^7,\, r^8,\, s,\, r\circ s,\, r^2\circ s,\, r^3\circ s,\, r^4\circ s,\, r^5\circ s,\, r^6\circ s,\, r^7\circ s,\, r^8\circ s\}$$

où r est la rotation de centre O et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (OA_1)$. En particulier G contient neuf rotations et neuf symétries orthogonales.

Le nombre de colliers est exactement le nombre d'orbites dans l'action de G sur X, *i.e.* $|\Omega|$.

On calcule ce nombre à l'aide de la formule obtenue en 1.

$$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{g\in \mathrm{G}} |\mathrm{Fix}(g)|.$$

Déterminons $\mathrm{Fix}(g)$ pour tout g dans G. Soit $g \in \mathrm{G}$.

- ◇ Si $g = \mathrm{id}$, alors $\mathrm{Fix}(g) = X$.
- ◇ Si $g \in \{r, r^2, r^4, r^5, r^7, r^8\}$, alors le sous-groupe de G engendré par g est constitué des 9 rotations (r^k engendre ce groupe si et seulement si k est premier avec 9). Donc un collier fixe par g est fixe par r ce qui implique que toutes les perles sont de la même couleur. Ceci n'est pas possible. Par suite $\mathrm{Fix}(g) = \emptyset$.
- ◇ Si $g \in \{r^3, r^6\}$, alors dans un collier fixe par g le nombre de perles d'une couleur donnée doit être un multiple de 3, ce qui n'est pas le cas dans l'ensemble X, donc $\mathrm{Fix}(g) = \emptyset$.

◇ Si g est une symétrie, nous pouvons supposer que $g = s$, les autres cas étant identiques. Puisque l'axe Δ de g ne contient que la perle A_1, dans un collier fixe par g, les perles A_i, $i \neq 1$, vont par paire de même couleur. Cela assure que la perle A_1 est nécessairement blanche. Se donner un collier fixe par g revient alors à se donner les couleurs des perles A_2, A_3, A_4, A_5 de sorte que 2 soient bleues, 1 blanche et 1 rouge. Il est clair que le nombre de tels colliers vaut

$$|\mathrm{Fix}(g)| = \binom{4}{2}\binom{2}{1} = 6 \times 2 = 12.$$

Enfin le cardinal de X est

$$|X| = \binom{9}{4}\binom{5}{3} = 126 \times 10 = 1260.$$

On en déduit que

$$|\Omega| = \frac{1}{18}\Big(1260 + 9 \times 12\Big) = 76.$$

Il y a donc 76 colliers distincts (à équivalence près) satisfaisant les contraintes de l'énoncé.

Exercice 295

Montrer que nous avons les isomorphismes suivants

$$\mathrm{PGL}(2, \mathbb{F}_2) \simeq \mathfrak{S}_3, \qquad \mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathfrak{S}_4, \qquad \mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4, \qquad \mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5.$$

Éléments de réponse 295

Le groupe $\mathrm{PGL}(n, \mathbb{F}_q)$ agit fidèlement sur les droites de $\mathbb{F}_q^n$.

Exercice 296

Soit $\Bbbk$ un corps commutatif. Considérons l'action du groupe $\mathrm{GL}(m, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$ sur $\mathrm{M}_{m,n}(\Bbbk)$ définie par $\big((P, Q), M\big) \mapsto PMQ^{-1}$.

Déterminer le nombre d'orbites de cette action.

Éléments de réponse 296

Il s'agit de classer les matrices à équivalence près. On en déduit qu'il y a $\min(m, n) + 1$ orbites.

Exercice 297

Soit $\Bbbk$ un corps commutatif. Considérons l'action de $\mathrm{GL}(n, \Bbbk)$ sur $\mathrm{Sym}(n, \Bbbk)$ définie par

$$(P, S) \mapsto PS{}^{\mathrm{t}}P$$

a) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{C}$.

b) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{R}$.

c) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{F}_p$ lorsque p désigne un nombre premier impair.

Éléments de réponse 297

Il s'agit de classer les formes bilinéaires sur $\Bbbk^n$.

— Si $\Bbbk = \mathbb{C}$, alors il y a $n+1$ orbites.

— Si $\Bbbk = \mathbb{R}$, alors il y a $\frac{(n+2)(n+1)}{2}$ orbites.

— Si $\Bbbk = \mathbb{F}_p$, alors il y a $2n+1$ orbites.

Exercice 298

Soit G un groupe d'ordre $n \in \mathbb{N}^*$ et soit $\Bbbk$ un corps commutatif. Montrer qu'il existe un morphisme de groupes injectif de G dans $\mathrm{GL}(n, \Bbbk)$.

Éléments de réponse 298

Utiliser le théorème de Cayley.

Exercice 299

Soit G un groupe d'ordre $2m$ avec $m \in \mathbb{N}^*$ impair. Montrer que G admet un sous-groupe d'indice 2.

Éléments de réponse 299

Utiliser le théorème de Cayley.

Exercice 300

Déterminer les groupes finis admettant exactement deux classes de conjugaison.

Éléments de réponse 300

Avec la formule des classes on trouve $\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 301

Déterminer les groupes finis admettant exactement trois classes de conjugaison.

Éléments de réponse 301

La formule des classes assure qu'il existe un couple (a, b) dans $\mathbb{N}^2$ tel que $1 \leq b \leq a \leq |\mathrm{G}|$ et

$$1 = \frac{1}{|\mathrm{G}|} + \frac{1}{a} + \frac{1}{b}.$$

Nous en déduisons que $1 \leq b \leq 3$ puis en étudiant les différents cas nous obtenons que $\mathrm{Card}(\mathrm{G}) \leq 6$. Finalement nous obtenons que $\mathrm{G} \simeq \mathbb{Z}/3\mathbb{Z}$ ou $\mathrm{G} \simeq \mathfrak{S}_3$.

Exercice 302

Soit G un groupe d'ordre p^n où n appartient à $\mathbb{N}^*$ et p est un nombre premier. Montrer que le centre de G n'est pas trivial.

Éléments de réponse 302

Faire agir G sur lui-même et utiliser la formule des classes.

Exercice 303

Soit G un groupe d'ordre infini. Supposons que G admette un sous-groupe propre H d'indice fini. Montrer que G n'est pas simple.

Éléments de réponse 303

Faire agir G sur G/H par translation des classes.

Exercice 304

Soit G un groupe fini d'ordre $n \geq 2$. Soit p le plus petit facteur premier de n. Montrer que si H est un sous-groupe de G d'ordre p alors H est central.

Éléments de réponse 304

Faire agir G sur H par conjugaison. Étudier le cardinal de chaque orbite pour obtenir qu'elles sont des singletons.

Exercice 305

1. Soit G un groupe agissant sur un ensemble E. On note pour $g \in \mathrm{G}$ et $x \in E$ l'action de g sur x par : $g \cdot x$. Montrer que pour tout x dans E le stabilisateur
$$\mathrm{St}_{\mathrm{G}}(x) = \mathrm{G}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$
de x est un sous-groupe de G.

   Soit maintenant $n \in \mathbb{N}$, $n \geq 2$. Notons G le groupe orthogonal $(\mathrm{O}(n, \mathbb{R}), \circ)$. Posons
$$\forall\, f \in \mathrm{G},\ \forall\, v \in \mathbb{R}^n \qquad f \cdot v = f(v).$$
   Désignons par $\mathcal{C} = (e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$.

2. Montrer que
$$\mathrm{G} \times \mathbb{R}^n \to \mathbb{R}^n \qquad\qquad (f, v) \mapsto f \cdot v$$
   définit une action du groupe G sur l'ensemble $\mathbb{R}^n$.

3. Déterminer l'orbite
$$\mathcal{O}_v^{\mathrm{G}} = \{f \cdot v \,|\, f \in \mathrm{G}\}$$
   d'un élément v de $\mathbb{R}^n$ sous l'action de G.

4. Montrer que f appartient à G_{e_1} si et seulement si la matrice représentative de f dans $\mathcal{C}$ est du type
$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$
   où P désigne un élément de $\mathrm{O}(n-1, \mathbb{R})$.

5. En déduire que $\mathrm{G}_{e_1} \simeq \mathrm{O}(n-1,\mathbb{R})$ en explicitant un isomorphisme entre $\mathrm{O}(n-1,\mathbb{R})$ et G_{e_1}.
6. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Donner un isomorphisme de groupes $\phi_x \colon \mathrm{G}_x \xrightarrow{\simeq} \mathrm{G}_{e_1}$.
7. Pour quels $x \in \mathbb{R}^n$ a-t-on $\mathrm{G}_x \lhd \mathrm{O}(n,\mathbb{R})$?
8. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Nous restreignons l'action de G sur $\mathbb{R}^n$ à celle de G_x. Donner l'orbite
$$\mathcal{O}_v^{\mathrm{G}_x} = \{f \cdot v \,|\, f \in \mathrm{G}_x\}$$
d'un élément v de $\mathbb{R}^n$ sous cette action (peut-être s'aider d'un dessin).

Éléments de réponse 305

1. Soit x dans E. Par définition d'une action $e \cdot x = x$ ce qui conduit à $e \in \mathrm{G}_x$.
   Si g et g' appartiennent à G_x nous avons
$$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$$
   donc gg' appartient à G_x.
   Enfin si g appartient à G_x, alors $x = g \cdot x$ et en faisant agir g^{-1} de part et d'autre de l'égalité nous obtenons
$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
   ce qui montre que g^{-1} appartient à G_x.
   En conclusion G_x est un sous-groupe de G.
2. Soit v dans $\mathbb{R}^n$. Nous avons
$$\mathrm{id}_{\mathbb{R}^n} \cdot v = \mathrm{id}_{\mathbb{R}^n}(v) = v$$
   et si f, g appartiennent à $\mathrm{O}(n,\mathbb{R})$, alors
$$(f \circ g) \cdot v = (f \circ g)(v) = f(g(v)) = f \cdot g(v) = f \cdot (g \cdot v).$$
   Par suite
$$\mathrm{G} \times \mathbb{R}^n \to \mathbb{R}^n, \qquad (f, v) \mapsto f \cdot v = f(v)$$
   définit une action du groupe G sur $\mathbb{R}^n$.
3. Soit v dans $\mathbb{R}^n$.
   - ◇ Si $v = 0$, quel que soit $f \in \mathrm{O}(n,\mathbb{R})$ nous avons $f(v) = 0$ et
$$\mathcal{O}_0^{\mathrm{G}} = \{f \cdot 0 \,|\, f \in \mathrm{G}\} = \{f(0) \,|\, f \in \mathrm{G}\} = \{0\}.$$
   - ◇ Si $v \neq 0$, alors du fait que les éléments $f \in \mathrm{O}(n,\mathbb{R})$ conservent la norme pour le produit scalaire standard de $\mathbb{R}^n$ nous avons $||f(v)|| = ||v||$ et donc $\mathcal{O}_v^{\mathrm{G}}$ est contenue dans la sphère $S(0, ||v||)$ de centre 0 et de rayon $||v||$. Réciproquement, soit u dans $\mathbb{R}^n$ tel que $||v|| = ||u||$, soient $\mathcal{B}_u = \left(\frac{u}{||u||}, u_2, u_2, \ldots u_n\right)$ et $\mathcal{B}_v = \left(\frac{v}{||v||}, v_2, v_2, \ldots v_n\right)$ deux

bases orthonormées de $\mathbb{R}^n$ (on peut compléter par le procédé de Gram-Schmidt un vecteur de norme 1 en une base orthonormée en dimension finie) et soit f l'application linéaire qui transforme $\mathcal{B}_v$ en $\mathcal{B}_u$. Puisque $\mathcal{B}_v$ et $\mathcal{B}_u$ sont deux bases orthonormées, f appartient à $\mathrm{O}(n,\mathbb{R})$. De plus $f\left(\frac{v}{||v||}\right) = \frac{u}{||u||}$ et $||u|| = ||v||$ entraînent $f(v) = u$. Finalement u appartient à $\mathcal{O}_v^{\mathrm{G}}$ et $\mathcal{O}_v^{\mathrm{G}} = S(0, ||v||)$ si $v \neq 0$.

4. Si f appartient à G_{e_1}, alors $f(e_1) = e_1$ et donc la première colonne de la matrice M représentant f dans la base canonique est : $\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. D'autre part $f(e_1) = e_1$ étant orthogonal à $f(e_2)$, $f(e_3)$, …, $f(e_n)$ puisque f préserve le produit scalaire la première ligne de M est $(1\ 0\ 0\ \ldots\ 0)$. Par suite $M = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$. Puisque ${}^{\mathrm{t}}MM = \mathrm{id}_n$ nécessairement ${}^{\mathrm{t}}PP = \mathrm{id}_{n-1}$; anisi P appartient à $\mathrm{O}(n-1,\mathbb{R})$.

   Réciproquement si

$$M = \mathrm{mat}(f, \mathcal{C}_n) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$

   avec P dans $\mathrm{O}(n-1,\mathbb{R})$ nous avons bien : f appartient à $\mathrm{O}(n,\mathbb{R})$ (car ${}^{\mathrm{t}}MM = \begin{pmatrix} 1 & 0 \\ 0 & {}^{\mathrm{t}}PP \end{pmatrix} = \mathrm{id}_n$) et $f(e_1) = e_1$.

5. D'après 4. l'application $\Psi\colon \mathrm{O}(n-1,\mathbb{R}) \to \mathrm{G}_{e_1}$ définie par $\Psi(g) = f$ où $\mathrm{mat}(f, \mathcal{C}) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$ et $\mathrm{mat}(g, \widetilde{\mathcal{C}}) = P$ est bien à valeurs dans G_{e_1} (où $\widetilde{\mathcal{C}}$ désigne la base canonique de $\mathbb{R}^{n-1}$). L'application Ψ est bien un morphisme de groupes : à la composition des applications correspond le produit des matrices. De plus g appartient à $\ker \Psi$ si et seulement si $\mathrm{mat}(g, \mathcal{C}_{n-1}) = \mathrm{id}_{n-1}$ si et seulement si $g = \mathrm{id}_{\mathbb{R}^{n-1}}$ ce qui prouve que Ψ est injective. La surjectivité de Ψ résulte directement du point 4.

6. Soit x dans $\mathbb{R}^n \setminus \{0\}$. Soit h dans $\mathrm{O}(n-1,\mathbb{R})$ tel que $h(e_1) = \frac{x}{||x||}$ (une telle application existe d'après 3.) Considérons

$$\phi_x\colon \mathrm{G}_x \to \mathrm{G}_{e_1} \qquad\qquad f \mapsto h^{-1} \circ f \circ h.$$

   Notons que $\phi_x(f)$ appartient à $\mathrm{O}(n-1,\mathbb{R})$ puisque f et h appartiennent à $\mathrm{O}(n-1,\mathbb{R})$. D'autre part

$$\phi_x(f)(e_1) = h^{-1}(f(h(e_1))) = h^{-1}\left(f\left(\frac{x}{||x||}\right)\right) = h^{-1}\left(\frac{x}{||x||}\right) = e_1$$

   ainsi ϕ_x est bien à valeurs dans G_{e_1}. Le fait que ϕ_x est un isomorphisme de groupes se vérifie directement.

7. Soit x dans $\mathbb{R}^n$.
   - Si $x = 0$, alors $\mathrm{G}_0 = \mathrm{O}(n, \mathbb{R})$ et $\mathrm{G}_0 \triangleleft \mathrm{O}(n, \mathbb{R})$.
   - Supposons $x \neq 0$. Soit f dans $\mathrm{G}_x \setminus \{\mathrm{id}_{\mathbb{R}^n}\}$ (rappelons que d'après 3. G_x n'est pas réduit à $\mathrm{id}_{\mathbb{R}^n}$). Il existe y dans $\mathbb{R}^n$ tel que $||y|| = ||x||$ et $f(y) \neq y$. D'après 3. on peut alors construire h dans $\mathrm{O}(n, \mathbb{R})$ tel que $h(y) = x$. Alors $h(f(h^{-1}(x))) \neq x$ (en effet $h^{-1}(x) = y$ donc $f(h^{-1}(x)) = f(y) \neq y$). Ainsi G_x n'est pas distingué dans $\mathrm{O}(n, \mathbb{R})$.

   Finalement $\mathrm{G}_x \triangleleft \mathrm{O}(n, \mathbb{R})$ si et seulement si $x = 0$.

8. D'après 4. un élément f de G_x s'identifie à une application orthogonale de $\mathrm{O}(n-1, \mathbb{R})$ qui agit sur $x^\perp$ (en identifiant $\mathbb{R}^{n-1}$ et $x^\perp$) en laissant fixe la direction x. Écrivons v dans une base orthonormée commençant par $\frac{x}{||x||}$; on voit que l'image par f de v appartient à $S(0, ||v||)$ (car f conserve la norme) et aussi à l'hyperplan affine $\mathcal{H}$ de $\mathbb{R}^n$ orthogonal à x et passant par la projection orthogonale π de v sur la droite x (car f préserve la coordonnée suivant $\frac{x}{||x||}$). L'intersection de $S(0, ||v||)$ et de $\mathcal{H}$ est la sphère $S_{\mathcal{H}}$ de $\mathcal{H}$ centrée en $\pi(v)$ et de rayon $\mathrm{dist}(v, \mathrm{vect}(x))$. Réciproquement, si u appartient à $S_{\mathcal{H}}$ la projection orthogonale $p(u)$ de u sur $x^\perp$ est de même norme que la projection orthogonale $p(v)$ de v sur $x^\perp$. Il existe donc une application orthogonale f de $\mathrm{O}(n-1, \mathbb{R})$ qui envoie $p(u)$ sur $p(v)$ (nous avons identifié $\mathbb{R}^{n-1}$ et $x^\perp$). Nous étendons alors f à $\widetilde{f}$ sur $\mathbb{R}^n$ tout entier en imposant que $\widetilde{f}$ laisse fixe la direction x. L'application $\widetilde{f}$ appartient à G_x et envoie u sur v. Il s'en suit que $\mathcal{O}_v^{\mathrm{G}_x} = S_{\mathcal{H}}$.

Exercice 306

Soient G un p-groupe et H un sous-groupe non trivial distingué de G.
Montrer que $\mathrm{H} \cap Z(\mathrm{G})$ n'est pas réduit à l'élément neutre.

Éléments de réponse 306

Le sous-groupe H de G étant distingué, G agit par conjugaison sur H. Puisque G est un p-groupe H l'est aussi et les orbites non triviales de cette action sont de cardinal divisible par p. On en déduit que la réunion des orbites triviales, c'est-à-dire l'ensemble $\mathrm{H} \cap Z(\mathrm{G})$ des points fixes, est aussi de cardinal divisible par p. Comme il contient l'élément neutre il contient au moins p éléments et n'est donc pas réduit à l'élément neutre.

Exercice 307

1. Soit G un groupe fini. Soit H un sous-groupe strict de G. Montrer qu'il existe $x \in \mathrm{G}$ tel que la classe de conjugaison de x ne rencontre pas H.
2. Donner un contre-exemple si G n'est pas fini.

Éléments de réponse 307

1. Soient x et g dans G. Nous avons $gxg^{-1} \in \mathrm{H} \iff x \in g^{-1}\mathrm{H}g$. On est donc ramené à montrer que la réunion $\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ des conjugués de H n'est pas égale à G. Pour cela on va majorer le cardinal de $\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ et montrer que cette réunion contient strictement moins d'éléments que G. Notons que si g_1 et g_2 sont dans la même classe à gauche modulo H, *i.e.* s'il existe $h \in \mathrm{H}$ tel que $g_2 = g_1 h$, alors
$$g_2\mathrm{H}g_2^{-1} = g_1(h\mathrm{H}h^{-1})g_1^{-1} = g_1\mathrm{H}g_1^{-1}.$$
Dans la réunion ci-dessus on peut donc prendre un système de représentants des classes à gauche modulo H. Soit g_1, g_2, …, g_k un tel système de représentants, $k = \frac{|\mathrm{G}|}{|\mathrm{H}|}$ étant l'indice de H dans G. Les conjugués de H ayant au moins l'élément neutre en commun il vient
$$\left|\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}\right| = \left|\bigcup_{i=1}^{k} g_i\mathrm{H}g_i^{-1}\right| \leq 1 + (|\mathrm{H}|-1)k = |\mathrm{G}| + 1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < |\mathrm{G}|$$
car par hypothèse $|\mathrm{H}| < |\mathrm{G}|$ donc $1 < \frac{|\mathrm{G}|}{|\mathrm{H}|}$ et $1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < 0$.
2. Le résultat précédent ne s'étend pas à un groupe infini. Prenons par exemple $\mathrm{G} = \mathrm{GL}(n, \mathbb{C})$ et H le sous-groupe de G formé des matrices triangulaires supérieures inversibles. Toute matrice de G étant trigonalisable la classe de conjugaison de toute matrice de G rencontre H.

Exercice 308

Soit $\Bbbk = \mathbb{F}_q$ un corps fini de cardinal q. Considérons le groupe linéaire $\mathrm{GL}(n, \Bbbk)$ et son sous-groupe $\mathrm{SL}(n, \Bbbk)$.

a) Montrer que le centre de $\mathrm{GL}(n, \Bbbk)$ (respectivement de $\mathrm{SL}(n, \Bbbk)$) est constitué des matrices scalaires de ce groupe.

b) Notons $\mathrm{PGL}(n, \Bbbk)$ (respectivement $\mathrm{PSL}(n, \Bbbk)$) le quotient de $\mathrm{GL}(n, \Bbbk)$ (respectivement $\mathrm{SL}(n, \Bbbk)$) par son centre. Calculer les ordres de $\mathrm{SL}(n, \Bbbk)$, $\mathrm{PGL}(n, \Bbbk)$ et $\mathrm{PSL}(n, \Bbbk)$.

Soit n un entier. Soit E le $\Bbbk$-espace vectoriel $\Bbbk^n$. Désignons par $\mathbb{P}(E)$ l'ensemble des droites vectorielles de $\Bbbk^n$ (espace projectif de dimension $n-1$).

c) Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}(n, \Bbbk)$ dans le groupe symétrique $\mathfrak{S}_{\mathbb{P}(E)}$.

Dans la suite on suppose que $n = 2$.

d) Montrer que $\mathbb{P}(E)$ est de cardinal $q+1$; on identifie Φ à un morphisme de $\mathrm{PGL}(2, \Bbbk)$ dans $\mathfrak{S}_{q+1}$.

e) Supposons que $q = 2$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2, \mathbb{F}_2)$ et $\mathrm{PSL}(2, \mathbb{F}_2)$ sur $\mathfrak{S}_3$.

f) Supposons que $q = 3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2, \mathbb{F}_3)$ sur $\mathfrak{S}_4$ et de $\mathrm{PSL}(2, \mathbb{F}_3)$ sur $\mathcal{A}_4$. Les groupes $\mathrm{PGL}(2, \mathbb{F}_3)$ et $\mathrm{SL}(2, \mathbb{F}_3)$ sont-ils isomorphes ?

g) Supposons que $q = 4$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2, \mathbb{F}_4)$ et $\mathrm{PSL}(2, \mathbb{F}_4)$ sur $\mathcal{A}_5$.

h) Supposons que $q = 5$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2, \mathbb{F}_5)$ sur $\mathfrak{S}_5$ et de $\mathrm{PSL}(2, \mathbb{F}_5)$ sur $\mathcal{A}_5$ (rappelons une conséquence non triviale de la simplicité des groupes alternés : tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ pour $n \geq 5$).

Éléments de réponse 308

a) Montrons plus généralement (sur un corps $\Bbbk$ quelconque) que si un endomorphisme f de $\Bbbk^n$ commute avec tous les endomorphismes de déterminant 1, alors f est une homothétie. Pour cela montrons que tout vecteur $v \neq 0$ de $\Bbbk^n$ est vecteur propre pour f. Complétons v en une base $(v, e_1, e_2, \ldots, e_{n-1})$ de $\Bbbk^n$. Soit M la matrice de f dans cette base. Alors M commute avec la matrice de Jordan J_n donc laisse stable le noyau de J_n qui est $\Bbbk \cdot v$. Ainsi v est bien vecteur propre pour f.

b) Nous avons
$$|\mathrm{GL}(n, \Bbbk)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$
Par définition $\mathrm{SL}(n, \Bbbk)$ est le noyau du morphisme de groupes surjectif
$$\det \colon \mathrm{GL}(n, \Bbbk) \to \Bbbk^*;$$
son cardinal est celui de $\mathrm{GL}(n, \Bbbk)$ divisé par $q - 1$, soit
$$|\mathrm{SL}(n, \Bbbk)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})q^{n-1}.$$
De plus $\mathrm{PGL}(n, \Bbbk)$ est le quotient de $\mathrm{GL}(n, \Bbbk)$ par un groupe isomorphe à $\Bbbk^*$ (les matrices scalaires non nulles) donc $|\mathrm{PGL}(n, \Bbbk)| = |\mathrm{SL}(n, \Bbbk)|$.

Pour finir $|\mathrm{PSL}(n, \Bbbk)| = \frac{|\mathrm{SL}(n,\Bbbk)|}{|Z(\mathrm{SL}(n,\Bbbk))|}$ et $Z(\mathrm{SL}(n, \Bbbk)) = \{\lambda \mathrm{Id} \mid \lambda^n = 1\}$. Or il y a $\mathrm{pgcd}(n, q-1)$ racines $n$ièmes de l'unité dans un corps $\Bbbk$ de cardinal q [5] donc
$$|\mathrm{PSL}(n, \Bbbk)| = \frac{(q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})q^{n-1}}{\mathrm{pgcd}(n, q - 1)}.$$

c) Faisons agir $\mathrm{PGL}(n, \Bbbk)$ sur l'ensemble $\mathbb{P}(E)$ des droites vectorielles de E par $\overline{g} \cdot D = g(D)$ où g appartient à $\mathrm{GL}(n, \Bbbk)$ et $\overline{g}$ est son image dans $\mathrm{PGL}(n, \Bbbk)$. Ceci est bien défini car si $\overline{g_1} = \overline{g_2}$, alors g_1 et g_2 sont proportionnels et $g_1(D) = g_2(D)$. L'action est fidèle car les seuls éléments g de $\mathrm{GL}(n, \Bbbk)$ qui stabilisent toutes les droites sont les homothéties. Nous obtenons donc un morphisme injectif Φ de $\mathrm{PGL}(n, \Bbbk)$ dans $\mathfrak{S}_{\mathbb{P}(E)}$.

d) Les droites vectorielles de E sont données par une équation $y = ax$ dans le plan, avec $a \neq 0$, ou par l'équation $x = 0$. Il y a donc $q + 1$ droites, *i.e.* $|\mathbb{P}(E)| = q + 1$.

5. En effet $\Bbbk^*$ est un groupe cyclique d'ordre $q - 1$. Nous sommes donc ramenés à compter le nombre de solutions x de $nx = 0$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$ ce qui donne le résultat.

e) D'après c) les groupes $\mathrm{PGL}(2,\mathbb{F}_2)$ et $\mathrm{PSL}(2,\mathbb{F}_2)$ coïncident et sont d'ordre 6. De plus $\mathfrak{S}_3$ est d'ordre 6. Ainsi le morphisme injectif Φ est aussi surjectif d'où le résultat.

f) D'une part $|\mathrm{PGL}(2,\mathbb{F}_3)| = (3^2-1)\times 3 = 24$ d'autre part $|\mathfrak{S}_4| = 24$. Ainsi Φ réalise un isomorphisme entre entre $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathfrak{S}_4$. Comme $\mathrm{pgcd}(2,3-1) = 2$ le groupe $\mathrm{PSL}(2,\mathbb{F}_3)$ est, d'après c), un sous-groupe d'indice 2 de $\mathrm{PGL}(2,\mathbb{F}_3)$. Puisque le seul sous-groupe d'indice 2 de $\mathfrak{S}_4$ est $\mathcal{A}_4$ [6] nous obtenons que Φ induit un isomorphisme entre $\mathrm{PSL}(2,\mathbb{F}_3)$ et $\mathcal{A}_4$.

Les groupes $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathrm{SL}(2,\mathbb{F}_3)$ ne sont pas isomorphes. En effet $Z(\mathrm{SL}(2,\mathbb{F}_3))$ est d'ordre 2 alors que le centre de $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathfrak{S}_4$ est trivial.

g) D'une part $|\mathrm{PGL}(2,\mathbb{F}_4)| = (4^2-1)\times 4 = 60$, d'autre part comme $\mathrm{pgcd}(2,4-1) = 1$ nous avons $\mathrm{PGL}(2,\mathbb{F}_4) = \mathrm{PSL}(2,\mathbb{F}_4)$. Par suite Φ induit un des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_4)$ et $\mathrm{PSL}(2,\mathbb{F}_4)$ sur un sous-groupe d'indice 2 de $\mathfrak{S}_5$ qui ne peut être que $\mathcal{A}_5$ [7].

h) L'ordre de $\mathrm{PGL}(2,\mathbb{F}_5)$ est $(5^2-1)\times 5 = 120$ donc Φ induit un isomorphisme de $\mathrm{PGL}(2,\mathbb{F}_5)$ sur un sous-groupe d'indice 6 de $\mathfrak{S}_6$ lequel est isomorphe à $\mathfrak{S}_5$ d'après le résultat rappelé. Étant donné que $\mathrm{pgcd}(2,5-1) = 2$, le groupe $\mathrm{PSL}(2,\mathbb{F}_5)$ est un sous-groupe d'indice 2 de $\mathrm{PGL}(2,\mathbb{F}_5) \simeq \mathfrak{S}_5$ et est donc isomorphe, via Φ, à $\mathcal{A}_5$.

Exercice 309

Donner des applications de l'équation aux classes.

Éléments de réponse 309

Applications de l'équation aux classes : le centre d'un p-groupe n'est pas trivial, théorème de Wedderburn.

Exercice 310

Donner des applications de la formule de Burnside.

Éléments de réponse 310

Applications de la formule de Burnside : petit théorème de Fermat, les colliers de Polya.

Exercice 311

Trouver un groupe fini $G \neq \{e\}$ tel que le centre de G est $\{e\}$, le sous-groupe dérivé de G est G mais G n'est pas simple.

Éléments de réponse 311

Considérons $G = G_1 \times G_2$ où G_1 et G_2 sont deux groupes simples non abéliens, par exemple $G_1 = G_2 = \mathcal{A}_5$. Le groupe G n'est pas simple : il contient par exemple le sous-groupe distingué

6. En effet, dès que $m \geq 2$ le seul morphisme non trivial de $\mathfrak{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

7. En effet, dès que $m \geq 2$ le seul morphisme non trivial de $\mathfrak{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

non trivial $\mathrm{G}_1 \times \{e\}$. De plus d'une part $Z(\mathrm{G}) = Z(\mathrm{G}_1) \times Z(\mathrm{G}_2)$, d'autre part $Z(\mathrm{G}_1) = Z(\mathrm{G}_2) = \{e\}$. Et enfin d'une part $[\mathrm{G}, \mathrm{G}] = [\mathrm{G}_1, \mathrm{G}_1] \times [\mathrm{G}_2, \mathrm{G}_2]$ et d'autre part $[\mathrm{G}_i, \mathrm{G}_i] = \mathrm{G}_i$ pour $i = 1$, 2.

Exercice 312

Soit D le groupe diédral d'ordre 8 (groupe des isométries du carré). Calculer le centre, le sous-groupe dérivé et l'abélianisé de D.

Soit $\mathbb{H}_8$ le groupe des quaternions d'ordre 8. Calculer le centre, le sous-groupe dérivé et l'abélianisé de $\mathbb{H}_8$.

Éléments de réponse 312

Le centre $Z(\mathrm{D})$ de D est $\{\pm \mathrm{id}\}$. Puisque le quotient $\mathrm{D}/Z(\mathrm{D})$ est abélien (il est d'ordre 4) son sous-groupe dérivé est inclus dans $Z(\mathrm{D})$. Étant donné que D n'est pas abélien, le groupe dérivé de $\mathrm{D}/Z(\mathrm{D})$ ne peut pas être trivial et coïncide donc avec $Z(\mathrm{D})$. On peut vérifier que tout élément g de D satisfait $g^2 \in Z(\mathrm{D})$. Ainsi tous les éléments non triviaux de $\mathrm{D}/Z(\mathrm{D})$ sont d'ordre 2. Par suite ce groupe d'ordre 4 n'est pas cyclique ; il est donc isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Les règles de calcul dans $\mathbb{H}_8 = \{ \pm 1, \pm i, \pm j, \pm k\}$ sont

$$ij = -ji = k, \qquad ki = -ik = j, \qquad jk = -kj = i, \qquad i^2 = j^2 = k^2 = -1.$$

Le centre $Z(\mathbb{H}_8)$ est donc réduit à $\{\pm 1\}$. Comme pour D nous en déduisons que le groupe dérivé de $\mathbb{H}_8$ est $Z(\mathbb{H}_8)$ et que l'abélianisé $\mathbb{H}_8/Z(\mathbb{H}_8)$ de $\mathbb{H}_8$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Notons que D et $\mathbb{H}_8$ ne sont pas isomorphes pour autant : D possède 5 éléments d'ordre 2 alors que $\mathbb{H}_8$ n'en possède qu'un.

Exercice 313

Soit G un groupe fini tel que le quotient de G par son centre soit abélien. Le groupe G est-il toujours abélien ?

Éléments de réponse 313

Non. Considérons par exemple un groupe non abélien G d'ordre 8 comme le groupe diédral. Son centre $Z(\mathrm{G})$ est non trivial car G est un 2-groupe. Par conséquent le quotient $\mathrm{G}/Z(\mathrm{G})$ est d'ordre au plus 4 et $\mathrm{G}/Z(\mathrm{G})$ est abélien.

Exercice 314

Quels sont les groupes finis G tels que tout élément g de G vérifie $g^2 = e$?

Éléments de réponse 314

Un tel groupe G est abélien ; en effet si g et h sont deux éléments de G alors $g = g^{-1}$ et $h = h^{-1}$ mais aussi $(gh) = (gh)^{-1}$ soit $gh = h^{-1}g^{-1}$ ou encore $gh = hg$. Notons alors G

additivement. Nous avons alors $2g = 0$ pour tout $g \in \mathrm{G}$. Le groupe G est alors isomorphe au groupe additif $\left(\mathbb{Z}/2\mathbb{Z}\right)^r$ pour un certain $r \in \mathbb{N}$. Réciproquement un tel groupe convient.

Exercice 315

Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Éléments de réponse 315

L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre $Z(\mathrm{G})$ de G n'est pas réduit à l'élément neutre. En effet, faisons agir G sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g,h) \mapsto g \cdot h = ghg^{-1}.$$

Notons que g appartient à $Z(\mathrm{G}) = \{h \in \mathrm{G} \,|\, hg = gh \quad \forall\, g \in \mathrm{G}\} = \{h \in \mathrm{G} \,|\, hgh^{-1} = g \quad \forall\, g \in \mathrm{G}\}$ si et seulement si l'orbite $\mathcal{O}_g = \{h \cdot g \,|\, h \in \mathrm{G}\} = \{hgh^{-1} \,|\, h \in \mathrm{G}\}$ de g sous cette action est réduite à $\{g\}$. Les orbites formant une partition de G nous avons $|\mathrm{G}| = \sum_{g \in \mathrm{G}} |\mathcal{O}_g|$ ce que l'on peut réécrire en séparant les orbites non réduites à un point et les orbites réduites à un point :

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

avec $\mathcal{O}_{g_i}$ non réduite à un point pour tout i. Par ailleurs $|\mathcal{O}_{g_i}|$ divise p (cela résulte de la bijection entre $\mathrm{G}/\mathrm{St}(g_i)$ et $\mathcal{O}_{g_i}$) donc

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

conduit à

$$|\mathrm{G}| \equiv |Z(\mathrm{G})| \bmod p$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Mais e_G appartient à $Z(\mathrm{G})$ donc $|Z(\mathrm{G})| \geq p$. Par suite $Z(\mathrm{G})$ est d'ordre p ou p^2.

Si $|Z(\mathrm{G})| = p^2$, alors $\mathrm{G} = Z(\mathrm{G})$ est abélien.

Si $|Z(\mathrm{G})| = p$, alors $\mathrm{G}/Z(\mathrm{G})$ est d'ordre p premier, $\mathrm{G}/Z(\mathrm{G})$ est cyclique et G est abélien [8].

Exercice 316

---

8. Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons qu'alors G est abélien.

Par hypothèse il existe un élément a de G dont la classe $\overline{a} \in \mathrm{G}/Z(\mathrm{G})$ engendre $\mathrm{G}/Z(\mathrm{G})$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(\mathrm{G})$.

Soient g et g' dans G ; alors $g = a^k h$ et $g' = a^{k'} h'$ avec k, k' dans $\mathbb{Z}$ et h, h' dans $Z(\mathrm{G})$; ainsi

$$gg' = a^k h a^{k'} h' \overset{h \in Z(\mathrm{G})}{=} a^k a^{k'} hh' = a^{k+k'} hh' \overset{h' \in Z(\mathrm{G})}{=} a^{k+k'} h'h = a^{k'+k} h'h = a^{k'} a^k h'h \overset{h \in Z(\mathrm{G})}{=} a^{k'} h' a^k h = g'g.$$

Le groupe G est donc abélien.

a) Soit $f\colon \mathrm{G} \to \mathrm{A}$ un morphisme de groupes. Soit H un sous-groupe distingué de G tel que $\mathrm{H} \subset \ker f$. Montrer qu'il existe un unique morphisme de groupes $\overline{f}\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to \mathrm{A}$ tel que $f = p \circ \overline{f}$ où $p\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ est la surjection canonique.

b) Supposons de plus que A est abélien. Montrer que $D(\mathrm{G}) \subset \ker f$; en déduire que f induit un morphisme de groupes $\mathrm{G}_{\mathrm{ab}} \to \mathrm{A}$.

Éléments de réponse 316

Exercice 317

On rappelle que dans le groupe ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, les éléments x qui vérifient $\langle x \rangle = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ sont les $\overline{m}$ tels que m et n soient premiers entre eux.

Un tel élément sera appelé générateur de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Il y a donc $\varphi(n)$ générateurs dans ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, où φ désigne la fonction indicatrice d'Euler.

a) Soit d un diviseur de n. Soit C_d le sous-groupe d'ordre d de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Montrer qu'un élément x de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ est d'ordre d si et seulement si c'est un générateur de C_d.

b) En déduire que $\displaystyle\sum_{d|n} \varphi(d) = n$.

c) Soit $\Bbbk$ un corps. Soit G un sous-groupe fini du groupe multiplicatif $\Bbbk^*$, notons n l'ordre de G. Soit d un diviseur de n. Montrer que G possède au plus $\varphi(d)$ éléments d'ordre d (on observera que si x est un tel élément, alors tous les éléments y de $\langle x \rangle$ vérifient $y^d = 1$, et que cette équation a au plus d solutions dans $\Bbbk$).

d) En déduire que G est cyclique. En particulier, si $\Bbbk$ est un corps fini, alors le groupe multiplicatif $\Bbbk^*$ est cyclique.

Éléments de réponse 317

Exercice 318

On dit qu'une suite (finie ou infinie)

$$\ldots \longrightarrow \mathrm{G}_i \xrightarrow{\varphi_i} \mathrm{G}_{i+1} \xrightarrow{\varphi_{i+1}} \mathrm{G}_{i+2} \longrightarrow \ldots$$

est exacte (les G_i étant des groupes et les φ_i des morphismes) si pour tout i, on a $\operatorname{im} \varphi_i = \ker \varphi_{i+1}$.

a) Montrer que

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

est une suite exacte (dite courte) si et seulement si les trois propriétés suivantes sont satisfaites : i injective, p surjective, $\operatorname{im} i = \ker p$.

b) Montrer que dans ce cas, on a ${}^{\mathrm{G}}\!/_{i(\mathrm{N})} \simeq \mathrm{H}$ (on notera souvent par abus de langage N pour $i(\mathrm{N})$, qui lui est isomorphe, d'où l'écriture ${}^{\mathrm{G}}\!/_{\mathrm{N}} \simeq \mathrm{H}$).

c) Soit $\Bbbk$ un corps. Montrer qu'on a une suite exacte

$$1 \longrightarrow \mathrm{SL}(n,\Bbbk) \longrightarrow \mathrm{GL}(n,\Bbbk) \longrightarrow \Bbbk^* \longrightarrow 1.$$

d) Montrer qu'on a des suites exactes

$$1 \longrightarrow \mathrm{SO}(n,\mathbb{R}) \longrightarrow \mathrm{O}(n,\mathbb{R}) \longrightarrow \{\pm 1\} \longrightarrow 1$$

et

$$1 \longrightarrow \mathrm{SU}(n,\mathbb{C}) \longrightarrow \mathrm{U}(n,\mathbb{C}) \longrightarrow \mathbb{S}^1 \longrightarrow 1,$$

où $\mathbb{S}^1$ désigne le groupe multiplicatif des nombres complexes de module 1.

e) Soit G un groupe de centre $Z(\mathrm{G})$. Soit $(\mathrm{Int}(\mathrm{G}), \circ)$ le groupe des automorphismes intérieurs de G. Montrer qu'on a une suite exacte

$$1 \longrightarrow Z(\mathrm{G}) \longrightarrow \mathrm{G} \longrightarrow \mathrm{Int}(\mathrm{G}) \longrightarrow 1.$$

Éléments de réponse 318

Exercice 319

On note H l'ensemble des matrices de la forme

$$M_{a,b} = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

avec $(a,b) \in \mathbb{C} \times \mathbb{C}$. Posons $H^* = H \smallsetminus \{0\}$.

a) Montrer que H^* est un sous-groupe non abélien de $\mathrm{GL}(2,\mathbb{C})$.

b) On note id la matrice identité, et on pose

$$I := M_{\mathbf{i},0} \qquad J = M_{0,1} \qquad K = M_{0,\mathbf{i}}.$$

Soit $\mathbb{H}_8 = \{\pm\mathrm{id}, \pm I, \pm J, \pm K\}$. Montrer que $\mathbb{H}_8$ est un sous-groupe non abélien d'ordre 8 de H^* (observer que $IJ = K = -IJ$, avec des relations analogues par permutations circulaires de I, J, K).

c) Montrer que le centre et le sous-groupe dérivé de $\mathbb{H}_8$ sont tous deux égaux à $\{\pm 1\}$.

d) Montrer que l'abélianisé de $\mathbb{H}_8$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Éléments de réponse 319

Exercice 320

Faire la liste, à isomorphisme près, des groupes de cardinal ≤ 7.

Éléments de réponse 320

Exercice 321

Soit $\mathrm{G} = \mathrm{GL}(n, \mathbb{C})$. Considérons la matrice

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

a) Quel est l'ordre de M dans G ?

b) Montrer qu'il existe $g \in \mathrm{G}$ tel que $gMg^{-1} = M^2$.

c) Soit H le sous-groupe de G engendré par M. Montrer que $g\mathrm{H}g^{-1}$ est un sous-groupe strict de H, et que l'ensemble des $x \in \mathrm{G}$ tels que $x\mathrm{H}x^{-1} \subset \mathrm{H}$ n'est pas un sous-groupe de G.

d) Soit maintenant G un groupe quelconque, H un sous-groupe de G, et $N_{\mathrm{G}}(\mathrm{H})$ l'ensemble des $x \in \mathrm{G}$ tels que $x\mathrm{H}x^{-1} = \mathrm{H}$. Montrer que $N_{\mathrm{G}}(\mathrm{H})$ est un sous-groupe de G (appelé normalisateur de H dans G), et que si H est fini, il coïncide avec l'ensemble des $x \in \mathrm{G}$ tels que $x\mathrm{H}s^{-1} \subset \mathrm{H}$ (mais pas en général, cf. c).

Éléments de réponse 321

Exercice 322

Soit G un groupe. On note e l'élément neutre de G. Étant donnés deux sous-groupes A et B de G nous désignons par AB le sous-ensemble de G formé des éléments de G de la forme ab où a est dans A et b est dans B.

Considérons désormais deux sous-groupes H et K de G.

1. Montrer que $\mathrm{HK} = \mathrm{KH}$ si et seulement si HK est un sous-groupe de G.
2. Montrer que si H est distingué dans G nous avons $\mathrm{HK} = \mathrm{KH}$ (et donc HK est un sous-groupe de G).
3. Montrer que si H est distingué dans G l'application $\varphi\colon \mathrm{K} \to {}^{\mathrm{HK}}\!/_{\mathrm{H}}$ définie par $\varphi(k) = k\mathrm{H}$ réalise (par passage au quotient) un isomorphisme de ${}^{\mathrm{K}}\!/_{\mathrm{H} \cap \mathrm{K}}$ sur ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$.
4. Montrer que si H et K sont distingués dans G et si $\mathrm{H} \cap \mathrm{K} = \{e\}$, l'application $\psi\colon \mathrm{H} \times \mathrm{K} \to \mathrm{HK}$ définie par $\psi((h, k)) = hk$ est un isomorphisme de groupes.

   Soit $\mathrm{SL}(2, \mathbb{Z})$ le groupe des matrices carrées de taille 2×2 à coefficients dans $\mathbb{Z}$ dont le déterminant est 1. Posons

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad\qquad N = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

5. Déterminer l'ordre de M, l'ordre de N et l'ordre de MN dans $\mathrm{SL}(2, \mathbb{Z})$.
6. Soient H (resp. K) le sous-groupe de $\mathrm{SL}(2, \mathbb{Z})$ engendré par M (resp. par N). Montrer que HK n'est pas un groupe.

Éléments de réponse 322

1. Supposons que HK soit un sous-groupe de G. Soit hk un élément de HK. Cet élément possède un inverse uv dans HK. On a donc $hk = (uv)^{-1} = v^{-1}u^{-1}$ qui est donc dans KH. Cela montre que HK est contenu dans KH. Par ailleurs soit kh un élément de KH. L'inverse de kh qui est $h^{-1}k^{-1}$ appartient à HK. Puisque HK est un sous-groupe de G, kh est donc aussi dans HK. D'où l'inclusion $\mathrm{KH} \subset \mathrm{HK}$, et l'égalité $\mathrm{HK} = \mathrm{KH}$.

   Réciproquement supposons $\mathrm{HK} = \mathrm{KH}$. D'abord $e \in \mathrm{HK}$ et si x est dans HK, il est clair que x^{-1} aussi. Considérons par ailleurs, deux éléments $u = ab$ et $v = cd$ dans HK. On a $bc = fg$ avec f dans H et g dans K. D'où $uv = (af)(gd) \in \mathrm{HK}$. Cela prouve que HK est un sous-groupe de G.

2. Soit hk un élément de HK. On a $hk = k(k^{-1}hk)$, ce qui prouve que hk appartient à KH (rappelons que H est distingué dans G). Par suite $\mathrm{HK} \subset \mathrm{KH}$.

   Réciproquement, soit kh dans KH. L'élément $khk^{-1} = h$ est dans H. D'où $kh = hk$ appartient à HK et $\mathrm{KH} \subset \mathrm{HK}$. D'où le résultat.

3. L'ensemble quotient ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$ est un groupe car H est distingué dans G (donc aussi dans HK) et φ est un morphisme de groupes (car $kk'\mathrm{H} = (k\mathrm{H})(k'\mathrm{H})$). Par ailleurs φ est surjective ; en effet, soit $a = hk\mathrm{H}$ un élément de ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$: on a $a = k'h'\mathrm{H}$ où $k' \in \mathrm{K}$ et $h' \in \mathrm{H}$ (car $\mathrm{KH} = \mathrm{HK}$). D'où $a = k'\mathrm{H}$ et $\varphi(k') = a$. Enfin étant donné un élément k de K, on a $k\mathrm{H} = \mathrm{H}$ si et seulement si k appartient à H. Le théorème de factorisation des morphismes de groupes entraîne alors notre assertion.

4. Par définition l'application ψ est surjective. Elle est injective car $\mathrm{H} \cap \mathrm{K}$ est réduit à l'élément neutre de G. Tout revient à vérifier que ψ est un morphisme de groupes. Considérons pour cela deux éléments (h, k) et (h', k') de $\mathrm{H} \times \mathrm{K}$. Nous avons

$$\psi((h,k)(h',k')) = \psi((hh',kk')) = (hh')(kk')$$

   Par ailleurs tout élément de H commute avec tout élément de K ; en effet si $h \in \mathrm{H}$ et $k \in \mathrm{K}$, alors l'élément $hkh^{-1}k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K}$ (par hypothèse H et K sont distingués dans G). Il en résulte que $hkh^{-1}k^{-1} = e$ et que $hk = kh$. Par conséquent $\psi((h,k)(h',k')) = (hk)(h'k')$, c'est-à-dire $\psi((h,k)(h',k')) = \psi((h,k))\psi((h',k'))$.

5. Soit id la matrice identité de $\mathrm{SL}(2,\mathbb{Z})$. On vérifie que $M^2 \neq \mathrm{id}$ et les égalités $M^4 = \mathrm{id}$, et $N^3 = \mathrm{id}$. Il s'ensuit que l'ordre de M est 4 et celui de N est 3. Par ailleurs, pour tout entier $n \geq 0$ nous avons

$$(MN)^{2n} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \qquad (MN)^{2n+1} = \begin{pmatrix} -1 & -1-2n \\ 0 & -1 \end{pmatrix}$$

   Il en résulte que MN n'est pas d'ordre fini (MN est donc d'ordre infini).

6. Supposons que HK soit un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$; c'est alors un groupe fini (car par exemple l'application

$$\mathrm{H} \times \mathrm{K} \to \mathrm{HK}, \qquad (h,k) \mapsto hk$$

est surjective). Mais cela conduit à une contradiction car MN appartient à HK et MN est d'ordre infini. D'où l'assertion.

Exercice 323

1. Soit G un groupe non abélien d'ordre 10. Montrer que G contient un élément d'ordre 5.
2. Montrer que G contient un sous-groupe distingué H d'ordre 5 et que tout élément $x \in \mathrm{G} \setminus \mathrm{H}$ est d'ordre deux (considérer le groupe quotient G/H).
3. Montrer que G est isomorphe au groupe diédral D_{10} (considérer l'ordre d'un élément xh).

Éléments de réponse 323

1. On rappelle que dans un groupe fini G, l'ordre de tout élément est un diviseur du cardinal de G. Ainsi, si dans un groupe d'ordre 10 il n'y avait aucun élément d'ordre 5, il n'y aurait aucun élément g d'ordre 10 car sinon g^2 serait d'ordre 5, de sorte que tout élément $g \neq 1$ serait d'ordre 2 ce qui est impossible car 10 n'est pas une puissance de 2 [9].
2. Soit g un élément d'ordre 5 ; le sous-groupe H qu'il engendre est d'indice 2 et est donc distingué [10] dans G. Soit alors $x \in \mathrm{H}$. Dans le groupe quotient G/H, nous avons $(\overline{x})^2 = 1$ de sorte que x^2 appartient à H. Si nous avions $x^2 \neq 1$, alors x^2 serait d'ordre 5 et x d'ordre 10 ; le groupe G serait alors cyclique donc abélien.
3. Supposons pour commencer que G est non abélien. Soit $x \in \mathrm{H}$ de sorte que tout élément de G s'écrit de manière unique sous la forme $g^k x^i$ avec $0 \leq k < 5$ et $i = 0, 1$. Considérons alors l'application $f\colon \mathrm{G} \to \mathrm{D}_{10}$ qui envoie $g^k x^i$ sur $r^k \circ s^i$ où r est la rotation d'angle $\frac{2\pi}{5}$ et s la réflexion d'axe (Ox). Montrons que f est un morphisme de groupes, *i.e.* $f(g^k x^i g^{k'} x^{i'}) = r^k s^i r^{k'} s^{i'}$. Pour $i = 0$ ou $k' = 0$ le résultat découle de la définition. Dans le cas $i = i' = 1$ comme $(g^{k'} x)^2 = 1$ (resp. $(r^{k'} x)^2 = 1$), nous avons $g^k x g^{k'} x = g^{k-k'}$ (resp. $r^k s r^{k'} s = r^{k-k'}$) d'où le résultat. Si $i' = 0$ nous écrivons $g^k x g^{k'}$ (resp. $r^k s r^{k'}$) sous la forme $g^k x g^{k'} x x$ (resp. $r^k s r^{k'} s s$) et nous appliquons le calcul précédent.

   Nous obtenons ainsi un morphsime de G dans D_{10} qui est injectif par définition et qui réalise donc étant l'égalité des ordres de G et D_{10} un isomorphisme.

   Si G est abélien nous reprenons le raisonnement de 2. Si $x^2 \neq 1$, x est d'ordre 10 et G est cyclique. Si $x^2 = 1$, x est alors d'ordre 2. Considérons alors $y = xg$ et soit n tel que $y^n = x^n g^n = 1$ soit $x^{-n} = x^n = g^n$. Si n était impair, nous aurions $x \in \mathrm{H}$: impossible car

9. Soit G un groupe dont tous les éléments non triviaux sont d'ordre 2 ; l'ordre de G est de la forme 2^n. En effet supposons, par récurrence, que si l'ordre de G est inférieur à r alors il est de la forme 2^n. La récurrence est vérifiée pour $r = 1$ et $r = 2$, supposons-la vraie jusqu'au rang r et traitons le cas $r+1$. Soit $g_1 \neq 1$ un élément de G qui engendre, par hypothèse, un sous-groupe d'ordre 2 qui est distingué dans G car $gg_1g^{-1} = g_1$. Considérons alors le groupe quotient $\mathrm{G}/\langle g_1 \rangle$ qui est d'ordre $\binom{r}{2}$ et dont tous les éléments sont d'ordre 2. Par récurrence $\binom{r}{2}$ est de la forme 2^n d'où le résultat

10. Si G est un groupe et si H est un sous-groupe d'indice 2 de G, alors H est distingué dans G.

H ne contient pas d'élément d'ordre 2. Ainsi n est pair et $g^n = 1$ soit 5 divise n et donc 10 divise n de sorte que y est d'ordre 10 d'où le résultat.

Exercice 324

Soit G un groupe fini d'ordre 21 agissant sur un ensemble fini E ayant n éléments.

1. Supposons que $n = 19$. Supposons aussi qu'il n'existe pas de point fixe dans E sous l'action de G. Combien y a-t-il d'orbites dans E ? Quel est le nombre d'éléments dans chacune de ces orbites ?
2. Supposons que $n = 11$. Montrer qu'il existe au moins un point fixe dans E sous l'action de G.
3. Soit n un entier > 11. Montrer qu'il existe un ensemble ayant n éléments sur lequel G opère sans point fixe.

Éléments de réponse 324

Rappel : soit K un groupe agissant sur un ensemble X ; X est réunion disjointe des orbites de X sous l'action de K, *i.e.* $|X| = \sum_{i=1}^{p} |\mathcal{O}_i|$ où les $\mathcal{O}_i$ sont les orbites de X sous l'action de K.
Par ailleurs pour tout i nous avons $|\mathcal{O}_i|$ divise |K|.

1. La relation $|E| = \sum_{i=1}^{p} |\mathcal{O}_i|$ combinée avec le fait que $|\mathcal{O}_i|$ divise $|E|$ s'écrit aussi
$$n = a_1 + 3a_2 + 7a_3 + 21a_4$$
où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 19$, l'entier a_4 est nécessairement nul et si par ailleurs on impose a_1 nul alors l'équation aux classes se réécrit $3a_2 + 7a_3 = 19$. Par conséquent $a_3 = 1$ et $a_2 = 4$; autrement dit il y a cinq orbites dont une de cardinal 7 et quatre de cardinal 3.
2. L'équation aux classes s'écrit encore
$$n = a_1 + 3a_2 + 7a_3 + 21a_4$$
où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 11$, l'entier a_4 est nécessairement nul. Par ailleurs l'équation $3a_2 + 7a_3 = 11$ n'a pas de solution entière de sorte que a_1 ne peut pas être nul ; autrement dit il existe au moins un point fixe dans E sous l'action de G.
3. Il suffit de montrer que tout entier $n \geq 12$ peut s'écrire $3a + 7b$ avec a, $b \geq 0$. Or tout entier $n \geq 12$ s'écrit sous la forme $3m + k$ avec $k \in \{0, 1, 2\}$ et
$$3m = 3m + 7 \cdot 0, \qquad 3m + 1 = 3(m - 2) + 7, \qquad 3m + 2 = 3(m - 4) + 7 \cdot 2.$$

Exercice 325

Soit G un groupe qui agit sur un ensemble X. Montrer que G agit transitivement sur chacune des orbites de X.

Éléments de réponse 325

Soit $x \in X$ et soit $\mathcal{O}_x$ son orbite. Soient y, z deux éléments de $\mathcal{O}_x$. Il existe g et h dans G tels que $y = g \cdot x$ et $z = h \cdot x$. Par conséquent

$$z = h \cdot x = hg^{-1}g \cdot x = hg^{-1} \cdot (g \cdot x) = hg^{-1} \cdot y;$$

cela montre que G agit transitivement sur $\mathcal{O}_x$.

Exercice 326

Soit G un groupe qui agit sur un ensemble X.

1. Montrer que si x, $y \in X$ et si $g \in \mathrm{G}$ sont tels que $g \cdot x = y$, alors les stabilisateurs $\mathrm{St}(x)$ et $\mathrm{St}(y)$ sont conjugués dans G.
2. Que se passe-t-il si $\mathrm{St}(x)$ est un sous-groupe distingué de G pour un certain $x \in X$.

Éléments de réponse 326

1. On a

$$\begin{aligned} g\mathrm{St}(x)g^{-1} &= g\{h \in \mathrm{G} \,|\, h \cdot x = x\}g^{-1} \\ &= \{ghg^{-1} \in \mathrm{G} \,|\, h \cdot x = x\} \\ &\overset{x=g^{-1}y}{=} \{ghg^{-1} \in \mathrm{G} \,|\, h \cdot g^{-1} \cdot y = g^{-1} \cdot y\} \\ &= \{ghg^{-1} \in \mathrm{G} \,|\, gh \cdot g^{-1} \cdot y = gg^{-1} \cdot y = y\} \\ &= \{h' \in \mathrm{G} \,|\, gh \cdot h' \cdot y = y\} \end{aligned}$$

2. Soit $x \in X$ tel que $\mathrm{St}(x)$ soit un sous-groupe distingué de G. Alors $\mathrm{St}(x)$ coïncide avec tous ses conjugués. Ainsi tous les éléments de $\mathcal{O}_x$ ont le même stabilisateur.

Exercice 327

Soit G un groupe qui agit sur un ensemble X et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. On désigne par

$$X^{\mathrm{H}} = \{x \in X \,|\, h \cdot x = x \ \ \forall\, h \in \mathrm{H}\}$$

l'ensemble des H-points fixes de X.

Montrer que l'action de G sur X induit une action de G/H sur X^{H}.

Éléments de réponse 327

Considérons l'application

$$\mathrm{G}/\mathrm{H} \times X^{\mathrm{H}} \to X^{\mathrm{H}}, \qquad (g\mathrm{H}, x) \mapsto g \cdot x.$$

Cette application est bien définie :

◇ soient $g \in \mathrm{H}$, $x \in X^{\mathrm{H}}$ et $h \in \mathrm{H}$, nous avons

$$h \cdot (g \cdot x) = gg^{-1}h \cdot (g \cdot x) = g \cdot (g^{-1}hg \cdot x) = g \cdot x$$

car $g^{-1}gh$ appartient à H puisque H est distingué dans G. Par conséquent $g \cdot x$ appartient à X^{H}.

◇ soient g, g' deux éléments de G tels que $g\mathrm{H} = g'\mathrm{H}$, il existe $h \in \mathrm{H}$ tel que $g = g'h$. Pour tout $x \in X^{\mathrm{H}}$ nous avons

$$g\mathrm{H} \cdot x = g \cdot x = g'h \cdot x = g' \cdot (h \cdot x) = g' \cdot x = g'\mathrm{H} \cdot x.$$

Ainsi l'action de gH ne dépend pas du choix de g.

Elle définit une action de G/H sur X^{H} :

◇ Soit $x \in X^{\mathrm{H}}$, nous avons $\mathrm{H} \cdot x = e \cdot x = x$.

◇ Soient g, $g' \in \mathrm{G}$, soit $x \in X^{\mathrm{H}}$ nous avons

$$g\mathrm{H} \cdot (g'\mathrm{H} \cdot x) = g\mathrm{H} \cdot (g' \cdot x) = g \cdot (g' \cdot x) = gg' \cdot x = gg'\mathrm{H} \cdot x.$$

Exercice 328

Soit $\mathbb{R}[x_1, x_2, \ldots, x_n]$ l'ensemble des polynômes de n variables à coefficients réels.

1. Montrer que l'application

$$\mathfrak{S}_n \times \mathbb{R}[x_1, x_2, \ldots, x_n] \to \mathbb{R}[x_1, x_2, \ldots, x_n], \quad (\sigma, P(x_1, x_2, \ldots, x_n)) \mapsto P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

est une action de groupe.

2. Soit

$$\Delta_n(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

i) Déterminer le stabilisateur $\mathrm{St}(\Delta_n)$ de Δ_n.

ii) Déterminer l'orbite $\mathcal{O}_{\Delta_n}$ du polynôme Δ_n.

iii) Vérifier que $|\mathcal{O}_{\Delta_n}| = [\mathfrak{S}_n : \mathrm{St}(\Delta_n)]$.

Éléments de réponse 328

1. Soit P dans $\mathbb{R}[x_1, x_2, \ldots, x_n]$ et soient σ, τ dans $\mathfrak{S}_n$. Alors

◇ $\mathrm{id} \cdot P(x_1, x_2, \ldots, x_n) = P^{\mathrm{id}}(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$;

◇ et

$$\begin{aligned}\sigma\cdot(\tau\cdot P(x_1,x_2,\ldots,x_n)) &= \sigma\cdot P^{\tau}(x_1,x_2,\ldots,x_n)\\ &= \sigma\cdot P(x_{\tau(1)},x_{\tau(2)},\ldots,x_{\tau(n)})\\ &= P^{\sigma}(x_{\tau(1)},x_{\tau(2)},\ldots,x_{\tau(n)})\\ &= (x_{\sigma\tau(1)},x_{\sigma\tau(2)},\ldots,x_{\sigma\tau(n)})\\ &= P^{\sigma\tau}(x_1,x_2,\ldots,x_n)\\ &= (\sigma\tau)\cdot P(x_1,x_2,\ldots,x_n).\end{aligned}$$

2. i) Soit $\sigma\in\mathfrak{S}_n$; alors

$$\sigma\cdot\Delta_n(x_1,x_2,\ldots,x_n)=\Delta_n^{\sigma}(x_1,x_2,\ldots,x_n)=\Delta(x_{\sigma(1)},\,x_{\sigma(2)},\,\ldots,x_{\sigma(n)})=\prod_{1\leq i<j\leq n}(x_{\sigma(i)}-x_{\sigma(j)})$$

Comme σ est une bijection, chaque terme x_i-x_j, pour tous $1\leq i<j\leq n$, apparaît une fois dans le produit Δ_n^{σ} à signe près. On peut montrer que pour une transposition τ de $\mathfrak{S}_n$ nous avons $\tau\cdot\Delta_n=-\Delta_n$. Puisque toute permutation de $\mathfrak{S}_n$ s'écrit comme un produit de transpositions nous obtenons alors que $\sigma\cdot\Delta_n=\varepsilon(\sigma)\Delta_n$ pour tout $\sigma\in\mathfrak{S}_n$ où

$$\mathrm{St}(\Delta_n)=\{\sigma\in\mathfrak{S}_n\,|\,\sigma\cdot\Delta_n=\Delta_n\}=\{\sigma\in\mathfrak{S}_n\,|\,\varepsilon(\sigma)=1\}=\mathcal{A}_n.$$

ii) L'orbite de Δ_n est

$$\mathcal{O}_{\Delta_n}=\{\sigma\cdot\Delta_n\,|\,\sigma\in\mathfrak{S}_n\}=\{\pm\Delta_n\}.$$

iii) Nous avons donc bien

$$2=|\mathcal{O}_{\Delta_n}|=[\mathfrak{S}_n:\mathrm{St}(\Delta_n)]=[\mathfrak{S}_n:\mathcal{A}_n].$$

Exercice 329

Soit G un groupe. Considérons l'action par conjugaison de G sur lui-même.

1. Déterminer le noyau de l'action

$$\gamma\colon \mathrm{G}\to\mathrm{Aut(G)},\qquad\qquad g\mapsto\gamma_g\colon \mathrm{G}\to\mathrm{G},\ x\mapsto gxg^{-1}$$

Qu'en déduit-on par le premier théorème d'isomorphisme ?

2. Notons Int(G) l'image de γ. Montrer que Int(G) est un sous-groupe distingué de Aut(G).
3. Déterminer $\mathrm{Aut}(\mathfrak{S}_3)$ et $\mathrm{Int}(\mathfrak{S}_3)$. (Indication : $\mathfrak{S}_3=\langle\sigma,\,\rho\rangle$ avec $\sigma=(1\ 2)$ et $\rho=(1\ 2\ 3)$).

Éléments de réponse 329

1. Montrons que $\ker\gamma = Z(\mathrm{G})$. Soit $g \in Z(\mathrm{G})$. Alors $gxg^{-1} = xgg^{-1} = x$ pour tout $x \in \mathrm{G}$. D'où $\gamma_g = \mathrm{id}_\mathrm{G}$ et $g \in \ker\gamma$. Inversement soit $g \in \ker\gamma$. Alors $\gamma_g = \mathrm{id}_\mathrm{G}$. Donc, pour tout $x \in X$, $gxg^{-1} = x$, *i.e.* $gx = xg$. Ainsi g appartient à $Z(\mathrm{G})$. Cela montre que $\ker\gamma = Z(\mathrm{G})$. Le premier théorème d'isomorphisme assure que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq \operatorname{im}\gamma = \mathrm{Int}(\mathrm{G})$.

2. Étant donné que $\mathrm{Int}(\mathrm{G})$ est l'image du morphisme γ c'est un sous-groupe de $\mathrm{Aut}(\mathrm{G})$. Il reste à vérifier qu'il est distingué dans $\mathrm{Aut}(\mathrm{G})$. Soit $\gamma_g \in \mathrm{Int}(\mathrm{G})$ avec $g \in \mathrm{G}$ et $\phi \in \mathrm{Aut}(\mathrm{G})$. Calculons $\phi\gamma_g\phi^{-1}$; soit $x \in \mathrm{G}$, ona

$$\phi\gamma_g\phi^{-1}(x) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)\phi(\phi^{-1}(x))\phi(g)^{-1} = \phi(g)x\phi(g)^{-1} = \gamma_{\phi(g)}(x).$$

   Par suite $\phi\gamma_g\phi^{-1} = \gamma_{\phi(g)} \in \mathrm{Int}(\mathrm{G})$ et $\mathrm{Int}(\mathrm{G})$ est distingué dans $\mathrm{Aut}(\mathrm{G})$.

3. Puisque $Z(\mathfrak{S}_3) = \{\mathrm{id}\}$, nous avons $\mathrm{Int}(\mathfrak{S}_3) \simeq {}^{\mathfrak{S}_3}\!/_{Z(\mathfrak{S}_3)} = \mathfrak{S}_3$. Rappelons que $\mathfrak{S}_3 = \langle\sigma, rho\rangle$ avec $\sigma = (1\ 2)$ et $\rho = (1\ 2\ 3)$. L'image d'un morphisme $f\colon \mathfrak{S}_3 \to \mathfrak{S}_3$ est donc entièrement déterminée par $f(\sigma)$ et $f(\rho)$. Comme un automorphisme préserve l'ordre des éléments si $f\colon \mathfrak{S}_3 \to \mathfrak{S}_3$ est un automorphisme, alors $f(\sigma)$ est un élément d'ordre 2 et $f(\rho)$ est un élément d'ordre 3. Ainsi nous avons au plus trois choix pour $f(\sigma)$ et au plus deux choix pour $f(\rho)$. Il y a donc au plus $2 \times 3 = 6$ automorphismes de $\mathfrak{S}_3$ et $\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3) \simeq \mathfrak{S}_3$.

Exercice 330 Soit D_8 le groupe des isométries du carré :

$$\mathrm{D}_8 = \langle r, s \,|\, r^4 = e,\ s^2 = e,\ rsrs = e\rangle.$$

1. Déterminer un morphisme injectif de groupes de D_8 dans $\mathfrak{S}_4$.
2. Les éléments $(1\ 3)$ et $(1\ 2\ 3\ 4)$ engendrent-ils le groupe symétrique $\mathfrak{S}_4$?

Éléments de réponse 330

1. Considérons l'action de D_8 sur les quatre sommets du carré. Comme trois de ces quatre sommets forment un repère affine, l'action est fidèle et le morphisme associé ϕ injectif.
2. Si ϕ est surjectif, alors il est bijectif d'après ce qui précède. Autrement dit ϕ est un isomorphisme entre D_8 et $\mathfrak{S}_4$: absurde, $|\mathrm{D}_8| = 8 \neq |\mathfrak{S}_4| = 24$. Ainsi φ n'est pas surjectif.

   Les deux éléments $(1\ 3)$ et $(1\ 2\ 3\ 4)$ appartiennent à $\operatorname{im}\phi$: $\phi(r) = (1\ 3)$ et $\phi(s) = (1\ 2\ 3\ 4)$. S'ils engendrent $\mathfrak{S}_4$, alors ϕ est surjectif : contradiction.

1.7. Groupe des permutations

Exercice 331

Dans le groupe symétrique $\mathfrak{S}_5$, combien y a-t-il de 5-cycles distincts ? de 4-cycles distincts ?

Éléments de réponse 331

L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire, c'est-à-dire :

$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$

de sorte que chaque classe est constituée de 5 éléments. On obtient alors $\binom{5}{5}(5-1)!$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le même raisonnement donne $\binom{4}{5}3!$.

Plus généralement le nombre de r-cycles dans $\mathfrak{S}_n$ est $\binom{n}{r}(r-1)!$.

Exercice 332

Soient $p \geq 5$ un nombre premier et $\mathrm{H} \subset \mathfrak{S}_p$ un sous-groupe tel que $1 < [\mathfrak{S}_p : \mathrm{H}] < p$.

1. Montrer que tout cycle d'ordre p est contenu dans H.
2. Montrer que tout cycle d'ordre 3 est produit de deux cycles d'ordre p.
3. Montrer que $\mathrm{H} = \mathcal{A}_p$.
4. Montrer que $\mathfrak{S}_5$ ne contient aucun sous-groupe d'ordre 30, 40.

Éléments de réponse 332

1. Soit c un p-cycle et soit $\overline{c}$ son image dans $\mathfrak{S}_{p/\mathrm{H}}$ qui n'est qu'un ensemble et n'est pas muni de structure de groupe car H n'est pas distingué dans $\mathfrak{S}_p$. L'ensemble $\mathfrak{S}_{p/\mathrm{H}}$ étant de cardinal strictement inférieur à p, on en déduit qu'il existe $0 \leq i < j < p$ tel que $\overline{c^i} = \overline{c^j}$ de sorte qu'il existe $h \in \mathrm{H}$ tel que $c^j = c^i h$ soit $c^{j-i} \in \mathrm{H}$. Or p étant premier, il existe u et v tel que $u(j-i) + vp = 1$ de sorte que $c^{(j-i)u} = c \in \mathrm{H}$ (car $c^p = \mathrm{id}$ puisque c est un p-cycle).
2. On remarque que
$$(1\ 3\ 2\ 4\ \ldots\ p)^{-1} \circ (1\ 2\ 3\ \ldots\ p) = (1\ 3\ 2)$$
de sorte que pour un 3-cycle quelconque $(a\ b\ c)$ nous avons
$$(a\ b\ c) = (a\ b\ c\ i_1\ \ldots\ i_{p-3})^{-1} \circ (a\ c\ b\ i_1\ \ldots\ i_{p-3})$$
où $\{i_1, \ldots, i_{p-3}\} = \{1, \ldots, n\} \setminus \{a, b, c\}$.
3. Le groupe $\mathcal{A}_p$ étant engendré par les 3-cycles qui d'après la question précédente appartiennent à H, nous obtenons que $\mathcal{A}_p \subset \mathrm{H} \subset \mathfrak{S}_p$ de sorte que $\frac{p!}{2}$ divise l'ordre de H qui est lui-même un diviseur de $p!$. Comme H est un sous-groupe strict de $\mathfrak{S}_p$, nous en déduisons que H est d'ordre $\frac{p!}{2}$ et donc que $\mathcal{A}_p = \mathrm{H}$.
4. Appliquons ce qui précède au cas $p = 5$. Si H était un sous-groupe de $\mathfrak{S}_5$ de cardinal 30 (resp. 40), il serait d'indice 4 (resp. 3) de sorte qu'il devrait contenir $\mathcal{A}_5$ ce qui n'est pas possible.

Exercice 333

Quel est l'ordre maximal d'un élément de $\mathfrak{S}_5$?

Éléments de réponse 333

Soit σ un élément de $\mathfrak{S}_5$. Soit $\sigma = c_1 \circ c_2 \circ \ldots \circ c_r$ la décomposition en cycles à supports disjoints de σ. Chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints de sorte que l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leq i \leq r$. En particulier dans $\mathfrak{S}_5$ on trouve que l'ordre maximal d'un élément est 6.

Exercice 334

Le groupe $\mathcal{A}_4$ est-il simple ? le groupe $\mathfrak{S}_4$ est-il simple ?

Éléments de réponse 334

Le groupe $\mathcal{A}_4$ n'est pas simple : le groupe

$$\mathcal{K} \simeq \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué non trivial et strict de $\mathcal{A}_4$.

Le groupe $\mathfrak{S}_4$ n'est pas simple : le groupe $\mathcal{A}_4$ est un sous-groupe distingué non trivial et strict de $\mathfrak{S}_4$.

Exercice 335

Décomposer la permutation $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2)$ en produit de cycles à support disjoint.

Éléments de réponse 335

On a $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2) = (2\ 1\ 4\ 5)$.

Exercice 336

Exprimer comme produit de cycles disjoints :

1. $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$;
2. $(1\ 2)(1\ 2\ 3)(1\ 2)$.

Quelle est la signature de ces permutations ?

Éléments de réponse 336

1. Posons $\sigma_1 = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$. Explicitons σ_1 :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 1\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 6\ 7\ 8\ 9\ 1 \\ 4\ 2\ 3\ 5\ 6\ 7\ 8\ 9\ 1 \\ 4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2 \end{array}$$

Donc $\sigma_1 = (4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2)$.

C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

2. Posons $\sigma_2 = (1\ 2)(1\ 2\ 3)(1\ 2)$. Explicitons σ_2 :

$$\begin{array}{c} 1\ 2\ 3 \\ 2\ 1\ 3 \\ 3\ 2\ 1 \\ 3\ 1\ 2 \end{array}$$

Ainsi $\sigma_2 = (3\ 1\ 2)$.

C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

Exercice 337

Calculer aba^{-1} pour

1. $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$;
2. $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$.

Éléments de réponse 337

1. Calcul de aba^{-1} pour $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$.

Explicitons a :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 1\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 3\ 5\ 4\ 1\ 6\ 7\ 8\ 9 \end{array}$$

autrement dit $a = (1\ 2\ 3\ 5)$. Il s'en suit que

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9 \end{array}$$

Finalement nous obtenons

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9 \\ 7\ 5\ 2\ 4\ 3\ 6\ 9\ 8\ 1 \\ 7\ 1\ 3\ 4\ 5\ 6\ 9\ 8\ 2 \end{array}$$

2. Calcul de aba^{-1} pour $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$. Les cycles a et b sont à supports disjoints donc commutent. Ainsi $aba^{-1} = aa^{-1}b = b$, autrement dit $aba^{-1} = b$.

Exercice 338 Considérons les éléments suivants de $\mathfrak{S}_5$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

1. Calculer les puissances successives et déterminer l'ordre de σ.
2. Calculer les puissances successives et déterminer l'ordre de ρ.
3. Calculer les puissances successives et déterminer l'ordre de $\sigma\rho$.
4. Calculer les puissances successives et déterminer l'ordre de $\rho\sigma$.
5. Calculer les puissances successives et déterminer l'ordre de $\sigma\rho^{-1}$.
6. Calculer les puissances successives et déterminer l'ordre de $\rho^{-1}\sigma$.

Éléments de réponse 338

Exercice 339

Déterminer la parité des permutations suivantes et les écrire comme produits de transpositions :

$$\sigma_1 = (1\ 3\ 5)(5\ 4\ 3\ 2)(5\ 6\ 7\ 8), \qquad \sigma_2 = (1\ 2)(2\ 4)(1\ 7)(7\ 6\ 8).$$

Éléments de réponse 339

L'application signature est un morphisme de $\mathfrak{S}_8$ dans le groupe multiplicatif $\{-1, 1\}$.

La permutation σ_1 est le produit d'un cycle pair avec deux cycles impairs, elle est donc paire.

La permutation σ_2 est le produit de 3 cycles impairs et d'un cycle pair, elle est donc impaire.

Autre méthode :

$$\sigma_1 = (3\ 5)(5\ 1)(2\ 3)(4\ 2)(2\ 5)(7\ 8)(6\ 8)(5\ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^8 = 1$ et

$$\sigma_2 = (1\ 2)(2\ 4)(1\ 7)(6\ 8)(7\ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^5 = -1$.

Exercice 340

Soit σ la permutation de $\{1, 2, \ldots, 12\}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

Calculer σ^{2000}.

Éléments de réponse 340

Posons $\sigma_1 = (1\ 10\ 5\ 7\ 2\ 9\ 12)$, $\sigma_2 = (3\ 8\ 6)$ et $\sigma_3 = (4\ 11)$.

Ces trois permutations sont à supports disjoints deux à deux donc commutent. Il en résulte que $\sigma^{2000} = \sigma_1^{2000}\sigma_2^{2000}\sigma_3^{2000}$.

Par ailleurs σ_1 est d'ordre 7 et $2000 = 285 \times 7 + 5$ d'où $\sigma_1^{2000} = \sigma_1^5$.
De plus σ_2 est d'ordre 3 et $2000 = 666 \times 3 + 2$ d'où $\sigma_2^{2000} = \sigma_2^2$.
Enfin σ_3 est d'ordre 2 et $2000 = 1000 \times 2$ d'où $\sigma_3^{2000} = \mathrm{id}$.
Par suite

$$\sigma^{2000} = \sigma_1^5\sigma_2^2 = (1\ 9\ 7\ 10\ 12\ 2\ 5)(3\ 8\ 6)$$

Exercice 341

Soit n un entier, soit σ une permutation de $\{1, 2, \ldots, n\}$ et soit $(x_1\ x_2\ \ldots\ x_k)$ un cycle de $\mathfrak{S}_n$.
Calculer $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}$.

Éléments de réponse 341

Pour $1 \leq i \leq j$ posons $\sigma(x_i) = y_i$. Alors $\sigma^{-1}(y_i) = x_i$ et $((x_1\ x_2\ \ldots\ x_k)\sigma^{-1})(y_i) = ((x_1\ x_2\ \ldots\ x_k))(x_i) = x_{i+1}$ donc $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}(y_i) = \sigma(x_{i+1}) = y_{i+1}$.
Par ailleurs si $y \notin \{y_1, y_2, \ldots, y_k\}$, alors $(\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1})(y) = y$.
Il en résulte que

$$\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \ldots\ \sigma(x_k))$$

Exercice 342

Dans le groupe $\mathfrak{S}_7$ calculer le produit

$$(4\ 5\ 6)(5\ 6\ 7)(6\ 7\ 1)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

Éléments de réponse 342

Nous avons

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7 \\ 1\ 2\ 4\ 5\ 3\ 6\ 7 \\ 1\ 3\ 2\ 5\ 4\ 6\ 7 \\ 2\ 1\ 3\ 5\ 4\ 6\ 7 \\ 2\ 6\ 3\ 5\ 4\ 7\ 1 \\ 2\ 7\ 3\ 6\ 4\ 5\ 1 \\ 2\ 7\ 3\ 4\ 5\ 6\ 1 \end{array}$$

Exercice 343

Soit n un entier. Construire des morphismes injectifs de $\mathfrak{S}_n$ dans $\mathfrak{S}_{n+1}$.

Éléments de réponse 343

Soit x un élément de $\{1, 2, \ldots, n+1\}$. Posons $E_x = \{1, 2, \ldots, n+1\} \setminus \{x\}$. Il existe un isomorphisme φ entre $\mathfrak{S}_n$ et $\mathfrak{S}_{E_x}$. Le morphisme $f_x \colon \mathfrak{S}_n \to \mathfrak{S}_{n+1}$ défini par

$$\begin{cases} f_x(\sigma)(i) = \varphi(\sigma)(i) \text{ pour } i \in E_x \\ f_x(\sigma)(x) = x \end{cases}$$

est injectif.

Exercice 344

Montrer que si c et γ sont des n-cycles de $\mathfrak{S}_n$ qui commutent entre eux, il existe un entier r tel que $\gamma = c^r$.

Éléments de réponse 344

Soient $c = (1\ c(1)\ c^2(1)\ \ldots\ c^{n-1}(1))$ et $\gamma = (1\ \gamma(1)\ \gamma^2(1)\ \ldots\ \gamma^{n-1}(1))$ deux n-cycles de $\mathfrak{S}_n$ qui commutent entre eux, *i.e.* $c\gamma = \gamma c$.

L'ensemble $\{1, 2, \ldots, n\}$ coïncide avec $\{1, c(1), c^2(1), \ldots, c^{n-1}(1)\}$. Par conséquent il existe $0 \leq r \leq n-1$ tel que $\gamma(1) = c^r(1)$. De plus si $i \in \{1, \ldots, n\}$, alors il existe $0 \leq s \leq n-1$ tel que $i = c^s(1)$. Il en résulte que

$$\gamma(i) = \gamma(c^s(1)) = c^s(\gamma(1)) = c^s(c^r(1)) = c^r(c^s(1)) = c^s(i).$$

Par suite $\gamma = c^s$.

Autre méthode : faisons agir $\mathfrak{S}_n$ sur l'ensemble des n-cycles par conjugaison (c'est possible car les n-cycles sont dans la même orbite pour cette action). Cet ensemble est de cardinal $(n-1)!$ En effet un n-cycle σ s'écrit $(1\ \sigma(1)\ \sigma(2)\ \ldots\ \sigma(n-1))$ et nous avons $(n-1)$ choix pour $\sigma(1)$ puis $(n-2)$ choix pour $\sigma(2)$ etc. Le groupe $\mathfrak{S}_n$ agit transitivement sur cet ensemble. L'indice du stabilisateur de c pour cette action est $(n-1)!$ et son cardinal est n. Ce stabilisateur est le centralisateur de c qui contient au moins les n puissances de c et tout n-cycle qui commute avec c est donc égal à une puissance de c.

Exercice 345

Soit $n \geq 3$ un entier. Sachant que le groupe $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de $\{1, 2, \ldots, n\}$ montrer que $\mathfrak{S}_n$ est engendré par les ensembles suivants de permutations :

1. $(1\ 2)$, …, $(1\ n)$;
2. $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$;
3. $(1\ 2)$, $(2\ 3\ \ldots\ n)$.

Éléments de réponse 345

1. Notons que $(i\ j) = (i\ 1)(j\ 1)(i\ 1)$ lorsque $i \neq j$;
2. Soit $i < j$.

   Si $j > i+1$, alors

$$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j) \tag{1.7.1}$$

Si $j-1=i+1$, alors $(i\ j)\in\langle(1\ 2),\ (2\ 3),\ \ldots,\ (n-1\ n)\rangle$.

Sinon nous appliquons (1.17.1) en remplaçant $(i\ j)$ par $(i\ j-1)$ et nous arrivons de proche en proche au résultat.

3. Nous avons
$$(2\ 3\ \ldots\ n)(1\ 2)(2\ 3\ \ldots\ n)^{-1}=(1\ 3).$$
Par suite par récurrence pour $i>2$ nous avons
$$(1\ i)=(2\ 3\ \ldots\ n)^{i-2}(1\ 2)(2\ 3\ \ldots\ n)^{-i+2}$$
d'où le résultat (en utilisant la première question).

Exercice 346

Soit G un sous-groupe de $\mathfrak{S}_4$ opérant sur $\{1,\ 2,\ 3,\ 4\}$ par l'action induite par l'action naturelle de $\mathfrak{S}_4$.

Pour $i=1,\ 2,\ 3,\ 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i.

Déterminer $\mathcal{O}_i$ et S_i pour $i=1,\ 2,\ 3,\ 4$ dans chacun des cas suivants :

1. $\mathrm{G}=\langle(1\ 2\ 3)\rangle$;
2. $\mathrm{G}=\langle(1\ 2\ 3\ 4)\rangle$;
3. $\mathrm{G}=\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$;
4. $\mathrm{G}=\{e,\ (1\ 2),\ (1\ 2)(3\ 4),\ (3\ 4)\}$;
5. $\mathrm{G}=\mathcal{A}_4$.

Éléments de réponse 346

1. Supposons que $\mathrm{G}=\langle(1\ 2\ 3)\rangle$.
   Si $i=1$, alors $\mathcal{O}_i=\{1,\ 2,\ 3\}$ et $S_i=\mathrm{id}$.
   Si $i=2$, alors $\mathcal{O}_i=\{1,\ 2,\ 3\}$ et $S_i=\mathrm{id}$.
   Si $i=3$, alors $\mathcal{O}_i=\{1,\ 2,\ 3\}$ et $S_i=\mathrm{id}$.
   Si $i=4$, alors $\mathcal{O}_i=\{4\}$ et $S_i=\mathrm{G}$.
2. Supposons que $\mathrm{G}=\langle(1\ 2\ 3\ 4)\rangle$.
   Si $i=1$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=2$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=3$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=4$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
3. Supposons que $\mathrm{G}=\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.
   Si $i=1$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=2$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=3$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.
   Si $i=4$, alors $\mathcal{O}_i=\{1,\ 2,\ 3,\ 4\}$ et $S_i=\mathrm{id}$.

4. Supposons que $G = \{\mathrm{id}, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
5. Supposons que $G = \mathcal{A}_4$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(2\ 3\ 4)\rangle$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 3\ 4)\rangle$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 2\ 4)\rangle$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 2\ 3)\rangle$.

Exercice 347

Établir la table de $\mathfrak{S}_3$ et de $\mathbb{Z}/6\mathbb{Z}$.
Quels sont les sous-groupes de $\mathfrak{S}_3$?
Quels sont les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$?

Éléments de réponse 347

La table de $\mathfrak{S}_3$ est

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

La table de $\mathbb{Z}/6\mathbb{Z}$ est

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[4]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Les sous-groupes de $\mathfrak{S}_3$ sont :

- un sous-groupe d'ordre 1 ;
- trois sous-groupes d'ordre 2 : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$;
- un sous-groupe d'ordre 3 : $\langle(1\ 2\ 3)\rangle$.

Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont :

- un sous-groupe d'ordre 1 ;
- un sous-groupes d'ordre 2 : $\langle[3]\rangle$;
- un sous-groupes d'ordre 3 : $\langle[2]\rangle$.

Exercice 348

a) Déterminer les classes de conjugaison dans $\mathfrak{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 348

a) Soit $c = (a_1\ \ldots\ a_k)$ un k-cycle de $\mathfrak{S}_n$. Pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1)\ \ldots\ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathfrak{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathfrak{S}_n$ la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1\ \ldots\ a_{2k+1}) \qquad\qquad c' = (a'_1\ \ldots\ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1\ a'_1)\ldots(a_{2k+1}\ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathfrak{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i\ j)\sigma(i\ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 349

Considérons les deux éléments suivants du groupe symétrique $\mathfrak{S}_9$

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathfrak{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathfrak{S}_9$?

Éléments de réponse 349

Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

nous trouvons parmi de nombreux choix possibles $\omega = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathfrak{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 350

Montrer que le groupe symétrique $\mathfrak{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathfrak{S}_3)$.

Éléments de réponse 350

L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathfrak{S}_3$ dans $\mathrm{Aut}(\mathfrak{S}_3)$, car le centre de $\mathfrak{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathfrak{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathfrak{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 351

Montrer que tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Éléments de réponse 351

Soit H un sous-groupe d'indice n dans $\mathfrak{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $\mathrm{H} \not\simeq \mathfrak{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q - 1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathfrak{S}_n$, et donc aussi H, opère par translation à gauche sur $E = \mathfrak{S}_n/\mathrm{H}$ d'où un morphisme

$$\varphi \colon \mathfrak{S}_n \to \mathfrak{S}_E \simeq \mathfrak{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathfrak{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathfrak{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$). Pour des raisons de cardinalité ($|\mathfrak{S}_n| = |\mathfrak{S}_E \simeq \mathfrak{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathfrak{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathfrak{S}_{n-1}$.

Exercice 352

a) Déterminer les classes de conjugaison dans $\mathfrak{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 352

a) Soit $c = (a_1 \ \ldots \ a_k)$ un k-cycle de $\mathfrak{S}_n$. Pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \ldots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathfrak{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathfrak{S}_n$ la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \dots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathfrak{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 353

Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathfrak{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathfrak{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathfrak{S}_n$.

b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1\ 2\ 3)$, …, $(1\ 2\ n)$. En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathfrak{S}_n$ (autrement dit $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathfrak{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré

— si n est impair ≥ 5 par $(1\ 2\ 3)$ et $(3\ 4\ \dots\ n)$;

— si n est pair ≥ 4 par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \dots\ n)$.

c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathfrak{S}_n$ de la forme $(a\ b)(c\ d)$ avec a, b, c, d deux à deux distincts.

Éléments de réponse 353

a) Soient $i < j < k < l$. Nous avons

$$(i \ j)(k \ l) = (i \ j)(j \ k)(j \ k)(k \ l)$$

Or $(i\ j)(j\ k) = (i\ j\ k)$ donc

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

b) i) Soient i, j et k des éléments de $\{1, \ldots, n\}$ tels que $i < j < k$. Nous avons

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

et

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle.$$

Soient ϕ un automorphisme de $\mathfrak{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathfrak{S}_n$.

ii) Pour $i \geq 4$ et $n \geq 4$ nous avons

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

Par ailleurs si $n \geq 5$ est impair, $(3\ 4\ \ldots\ n)$ est une permutation paire car c'est un cycle de longueur impaire $n-2$. Ainsi pour $n \geq 5$ impair on a

$$\mathcal{A}_n = \langle (1\ 2\ 3), (3\ 4\ \ldots\ n)\rangle$$

Nous avons

$$(1\ 2)^{\alpha}(1\ 2\ i)(1\ 2)^{\alpha} = \begin{cases} (1\ 2\ i) \text{ pour } \alpha \text{ pair} \\ (1\ 2\ i)^{-1} \text{ pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geq 4$ et $n \geq 4$

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

alors pour $i \geq 4$ impair et $n \geq 4$

$$(1\ 2\ i) = [(1\ 2)(3\ 4\ \ldots\ n)]^{i-3}(1\ 2\ 3)[(1\ 2)(3\ 4\ \ldots\ n)]^{-3+i}.$$

Et pour $i \geq 4$ pair et $n \geq 4$

$$(1\ 2\ i) = \big[\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{i-3}(1\ 2\ 3)\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{-3+i}\big]^{-1}.$$

Or si $n \geq 4$ est pair $(1\ 2)(3\ 4\ \ldots\ n)$ est une pemutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Il suffit de montrer que tout 3-cycle $(i\ j\ k)$ (avec $i<j<k$) est produit de permutations de la forme $(a\ b)(c\ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n\geq 5$ il existe ℓ et m dans $\{1,\,2,\,\ldots,n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or nous avons

$$(i\ j\ k)=(m\ \ell)(j\ k)(m\ \ell)(i\ k)$$

d'où le résultat.

Exercice 354

Soit $n\in\mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathfrak{S}_n$ dans $\mathcal{A}_{n+2}$.

Éléments de réponse 354

Considérons l'application $\psi\colon \mathfrak{S}_n\to\mathcal{A}_{n+2}$ définie par

$$\begin{cases}\psi(\sigma)=\sigma \text{ si } \sigma \text{ est une permutation paire}\\ \psi(\sigma)=\sigma\circ(n+1\ n+2) \text{ si } \sigma \text{ est une permutation impaire}\end{cases}$$

L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints.

On peut vérifier que ψ est un morphisme de groupes.

Exercice 355

Construire un morphisme surjectif de $\mathfrak{S}_4$ sur $\mathfrak{S}_3$.

Éléments de réponse 355

Faire agir $\mathfrak{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathfrak{S}_4$ qui ne sont pas des transpositions.

Exercice 356

On rappelle que le groupe symétrique $\mathfrak{S}_n$ agit par applications linéaires sur $\mathbb{R}^n$ muni de sa base canonique (e_i), en posant pour tout $\sigma\in\mathfrak{S}_n$ et tout vecteur e_i de la base canonique $\sigma\cdot e_i=e_{\sigma(i)}$. Pour $\sigma=(1\ 2\ 3)\in\mathfrak{S}_3$ expliciter la matrice associée et calculer $\sigma\cdot(x_1,x_2,x_3)$.

Éléments de réponse 356

L'action de $\mathfrak{S}_3$ par applications linéaires sur $\mathbb{R}^3$ correspond à un morphisme de $\mathfrak{S}_3$ vers le groupe $\mathrm{GL}(3,\mathbb{R})$ des bijections linéaires de $\mathbb{R}^3$. Il s'agit de trouver l'image de $\sigma=(1\ 2\ 3)\in\mathfrak{S}_3$. L'application linéaire est entièrement déterminée par l'image d'une base : puisque $e_1\mapsto e_2$, $e_2\mapsto e_3$, $e_3\mapsto e_1$ nous obtenons la matrice

$$\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$$

et finalement l'image de (x_1, x_2, x_3) est (x_3, x_1, x_2) car

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}.$$

Remarque : une erreur classique est de croire que l'action est donnée par

$$\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

Ce n'est pas le cas, cette définition donnerait une action à droite, pas à gauche ! En fait on peut vérifier que la formule correcte pour l'action exprimée en coordonnées est

$$\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

Exercice 357

Considérons le groupe alterné $\mathcal{A}_4$. Rappelons que $D(\mathcal{A}_4)$ désigne son groupe dérivé. Soit $\mathcal{K}$ le sous-groupe de $\mathcal{A}_4$ constitué de l'identité et des doubles transpositions.

1. Montrer que $\mathcal{K}$ est un sous-groupe distingué de $\mathcal{A}_4$.
2. Montrer que $D(\mathcal{A}_4)$ est contenu dans $\mathcal{K}$ (indication : $\mathcal{A}_4/\mathcal{K}$ est d'ordre 3).
3. Montrer que $D(\mathcal{A}_4)$ n'est pas trivial.
4. Montrer que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.
5. En déduire que $D(\mathcal{A}_4) = \mathcal{K}$.

Éléments de réponse 357

1. Montrons que $\mathcal{K} \triangleleft \mathcal{A}_4$.

   Si on conjugue la double transposition $(a\ b)(c\ d)$ par une permutation σ nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ ce qui montre que $\mathcal{K}$ est distingué dans $\mathfrak{S}_4$ donc a fortiori dans $\mathcal{A}_4$.
2. Montrons que $D(\mathcal{A}_4) \subset \mathcal{K}$.

   Comme $\mathcal{A}_4/\mathcal{K}$ est d'ordre $\frac{12}{4} = 3$, il est cyclique d'ordre 3 (car 3 est premier) et en particulier abélien ce qui montre que $D(\mathcal{A}_4) \subset \mathcal{K}$.
3. Montrons que $D(\mathcal{A}_4) \neq \{1\}$.

   Le groupe $\mathcal{A}_4$ n'est pas abélien donc $D(\mathcal{A}_4) \neq \{1\}$.
4. Montrons que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.

   Soit H un sous-groupe d'ordre 2 de $\mathcal{A}_4$. Il est composé de l'identité et d'une double transposition $\tau = (a\ b)(c\ d)$. Si on conjugue τ par $\sigma \in \mathcal{A}_4$, nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ qui n'appartient pas à H si on choisit par exemple $\sigma \in \mathcal{A}_4$ tel que $\sigma(a) = a$ et $\sigma(b) = c$ ce qui est toujours possible.
5. Montrons que $D(\mathcal{A}_4) = \mathcal{K}$.

   Nous avons vu que $D(\mathcal{A}_4) \subset \mathcal{K}$ donc l'ordre de $D(\mathcal{A}_4)$ divise 4. Mais nous avons aussi vu que $D(\mathcal{A}_4)$ n'est d'ordre ni 1, ni 2. Il en résulte que $D(\mathcal{A}_4)$ est d'ordre 4 et que $D(\mathcal{A}_4) = \mathcal{K}$.

1.8. Autour des théorèmes de Sylow

Exercice 358

Donner un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 358

Le sous-groupe des matrices triangulaires supérieures strictes de $\mathrm{GL}(n, \mathbb{F}_p)$ est un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Exercice 359

Parmi les assertions suivantes, démontrer celles qui sont vraies et donner un contre-exemple pour celles qui sont fausses (on indiquera d'abord si l'assertion est vraie ou fausse).

a) Soit G un groupe quelconque. Soient x, y dans G. Si xy est d'ordre fini p dans G, alors yx est d'ordre fini p dans G.

b) Si G est un groupe fini abélien et p est un nombre premier divisant $|\mathrm{G}|$, alors G contient un unique p-Sylow.

c) Soit p un nombre premier. Soit G un groupe fini vérifiant : pour tout $x \in \mathrm{G}$, il existe $m \in \mathbb{N}^*$ tel que $x^{p^m} = e_{\mathrm{G}}$. Alors G est un p-groupe.

Éléments de réponse 359

a) C'est vrai. Remarquons que

$$(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n \text{ termes}} = x\,\underbrace{(yx)(yx)\dots(yx)}_{(n-1) \text{ termes}}\,y = x(yx)^{n-1}y.$$

Ainsi

$$(xy)^n = e \iff x(yx)^{n-1}y = e \iff yx(yx)^{n-1}y = y \iff (yx)^n = e$$

ce qui montre que les ordres de xy et yx sont identiques.

b) C'est vrai. En effet, on sait que G possède un p-Sylow S et que tout p-Sylow H est conjugué à S mais comme G est abélien ceci implique $\mathrm{H} = \mathrm{S}$.

c) C'est vrai. Sinon $|\mathrm{G}|$ aurait un diviseur premier $q \neq p$ et G contiendrait donc un q-Sylow non trivial H. Tout élément x dans $\mathrm{H} \setminus \{e_{\mathrm{G}}\}$ serait alors d'ordre q^s avec $s > 0$ ce qui n'est pas possible étant donné que par hypothèse l'ordre de x est de la forme p^r avec $r > 0$.

Exercice 360

Déterminer les p-Sylow de $\mathbb{Z}/n\mathbb{Z}$ pour tout diviseur p de n.

Éléments de réponse 360

Posons $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$. Le groupe G est abélien ; par suite tous les sous-groupes de G sont distingués. En particulier si H est un p-Sylow de G, alors H est un p-Sylow de G distingué dans

G donc H est l'unique p-Sylow de G. Il en résulte que G possède un seul p-Sylow, et ce pour tout diviseur p de n.

Plus précisément, si on écrit n sous la forme $p^\alpha m$ avec $p \nmid m$, le groupe H est le sous-groupe $m\mathbb{Z}/n\mathbb{Z}$ de $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m modulo n.

Exercice 361

Montrer qu'un groupe d'ordre 30 n'est pas simple.

Éléments de réponse 361

Supposons qu'il existe un groupe simple G d'ordre 30. Considérons les p-Sylow de G. Désignons par n_p le nombre de p-Sylow de G.

Rappelons que $30 = 2 \times 3 \times 5$.

Les théorèmes de Sylow assurent que

$$\begin{aligned} n_2 &\equiv_2, & n_2 \mid 3 \times 5 = 15 \\ n_3 &\equiv_3 1, & n_3 \mid 2 \times 5 = 10 \\ n_5 &\equiv_5 1, & n_5 \mid 2 \times 3 = 6 \end{aligned}$$

i.e.

$$n_2 \in \{1, 3, 5, 15\}, \qquad n_3 \in \{1, 10\}, \qquad n_5 \in \{1, 6\}.$$

Mais G est simple donc $n_2 \neq 1$, $n_3 \neq 1$ et $n_5 \neq 1$; finalement

$$n_2 \in \{3, 5, 15\}, \qquad n_3 = 10, \qquad n_5 = 6.$$

On en déduit que le groupe G contient $6 \times 4 = 24$ éléments d'ordre 5 (les intersections des 5-Sylow sont restreintes à l'élément neutre [11] et au moins 20 éléments d'ordre 3. En particulier d'une part $|\mathrm{G}| = 30$, d'autre part $|\mathrm{G}| \geq 44$: contradiction.

Exercice 362

Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Montrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Éléments de réponse 362

11. En effet un 5-Sylow P est un groupe d'ordre 5 donc est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et tout élément de $\mathrm{P} \setminus \{e\}$ engendre P ; en particulier si P et S sont deux 5-Sylow distincts et si g appartient à $\mathrm{P} \cap \mathrm{S} \setminus \{e\}$, alors d'une part $\langle g \rangle = \mathrm{P}$ et d'autre part $\langle g \rangle = \mathrm{S}$ d'où $\mathrm{S} = \mathrm{P}$: contradiction. Il en résulte que $\mathrm{P} \cap \mathrm{S} = \{e\}$.

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv_3 1$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \{\mathrm{id}, g, h\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 5-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv_5 1$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a nécessairement huit éléments d'ordre 15. Ainsi G possède un élément g d'ordre son cardinal ; G est donc le groupe cyclique engendré par g, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 363

Montrer qu'un groupe d'ordre 200 n'est pas simple.

Éléments de réponse 363

Soit G un groupe d'ordre 200. Notons que $200 = 2^3 \times 5^2$. D'après les Théorèmes de Sylow le nombre de 5-Sylow de G est congru à 1 modulo 5 et divise $2^3 = 8$ donc vaut 1. L'unique 5-Sylow de G est donc nécessairement distingué dans G ; en particulier G n'est pas simple.

Exercice 364

Soient p et q deux nombres premiers distincts. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Éléments de réponse 364

Soit G un groupe d'ordre p^2q. Soit n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G. Nous allons distinguer le cas $q < p$ du cas $p < q$.

- ◇ Si $p > q$, alors n_p divise q et $n_p \equiv 1 \bmod p$. Comme $q < p$ nécessairement $n_p = 1$; le groupe G possède alors un unique p-Sylow qui est distingué dans G et G n'est pas simple.
- ◇ Si $p < q$, alors n_q divise p^2 et $n_q \equiv 1 \bmod q$. Ainsi n_q appartient à $\{1, p, p^2\}$ et $n_q \equiv 1 \bmod q$. Puisque $q < p$, $n_q \neq p$, *i.e.* n_q appartient à $\{1, p^2\}$. Si $n_q = 1$, alors le groupe G n'est pas simple. Étudions la dernière possibilité : $n_q = p^2$. Si $n_q = p^2$, alors $p^2 \equiv 1 \bmod q$ et $p \equiv \pm 1 \bmod q$. Comme $p < q$ ceci entraîne que $p = q - 1$; étant donné que p et q sont premiers nous obtenons $p = 2$ et $q = 3$. Dans ce dernier cas, il y a quatre 3-Sylow d'ordre 3 qui contiennent huit éléments d'ordre 3 ; il ne reste de la place que pour un seul 2-Sylow qui devrait être distingué. Ce dernier cas est donc lui aussi impossible.

Exercice 365

Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Démontrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Éléments de réponse 365

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv 1 \bmod 3$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \{\mathrm{id}, g, h\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a huit éléments d'ordre 15. Ainsi G possède un élément d'ordre son cardinal ; G est donc le groupe cyclique engendré par cet élément, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 366

(1) Quel est le nombre de 2-Sylow dans le groupe symétrique $\mathfrak{S}_4$?

(2) Rappelons que $\mathfrak{S}_4$ est isomorphe au groupe des rotations de $\mathbb{R}^3$ préservant un cube. Interpréter géométriquement la réponse à la question précédente.

Éléments de réponse 366

(1) Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2 \times 3 \times 3$. Le nombre n de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $8 = 2^3$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n = 1$ ou $n = 3$. Montrons que $n = 1$ est impossible. Si $n = 1$, alors l'unique 2-Sylow serait un sous-groupe distingué de $\mathfrak{S}_4$. Mais les classes de conjugaison de $\mathfrak{S}_4$ sont de cardinaux 1, 3 et 8, et il est impossible d'obtenir 8 en sommant 1 et 3 ou 8 (rappelons qu'un sous-groupe contient le neutre, donc la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : $\mathfrak{S}_4$ contient 3 sous-groupes d'ordre 8.

(2) Cherchons géométriquement un sous-groupe d'ordre 8 dans $\mathfrak{S}_4$ vu comme le groupe des rotations préservant un cube. Il y a cinq groupes d'ordre 8 à isomorphisme près, dont le groupe diédral D_8. Comme il y a un air de famille entre le cube et le carré, cela incite à chercher un sous-groupe de $\mathfrak{S}_4$ isomorphe à D_8. Effectivement il y en a : on tranche le cube suivant un « carré équateur » et on considère le sous-groupe des rotations préservant à la fois le cube et ce carré : il y en a 8.

Exercice 367

Montrer que tout groupe d'ordre 217 est cyclique (Indication : commencer par calculer le nombre de p-Sylow pour chaque diviseur premier p de 217).

Éléments de réponse 367

Soit G un groupe d'ordre 217. Notons que $217 = 7 \times 31$ et que 7 et 31 sont premiers. Le nombre de 7-Sylow de G est congru à 1 modulo 7 et divise 31 : la seule possibilité est donc 1. D'autre part le nombre de 31-Sylow est congru à 1 modulo 31 et divise 7 ; de nouveau la seule possibilité est 1. Ainsi G contient un unique 7-Sylow S_7, qui est donc distingué, et de même contient un unique 31-Sylow S_{31}, lui-aussi distingué dans G.

L'intersection $S_7 \cap S_{31}$ est triviale par Lagrange (en effet l'ordre d'un élément de $S_7 \cap S_{31}$ divise 7 et 11 donc vaut 1).

Puisque S_7 est distingué dans G, $S_7 S_{31}$ est un sous-groupe de G [12]. Comme il contient strictement S_7 et S_{31}, son ordre est un multiple strict de 7 et de 31, la seule possibilité est donc 217 et on conclut que $\mathrm{G} = S_7 S_{31}$.

Puisque S_7 et S_{31} sont d'ordre premier ils sont cycliques et $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z}$; par le théorème chinois on conclut que $\mathrm{G} \simeq \mathbb{Z}/217\mathbb{Z}$.

Exercice 368

Combien le groupe symétrique $\mathfrak{S}_4$ contient-il de 2-Sylow ?

Éléments de réponse 368

Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $8 = 2^3$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n = 1$ ou $n = 3$. Montrons que $n = 1$ est impossible. Si $n = 1$, alors l'unique 2-Sylow serait un sous-groupe distingué de $\mathfrak{S}_4$. Mais $\mathfrak{S}_4$ possède 24 éléments répartis en 5 classes de conjugaison. En effet, il y a :

- ◇ le neutre seul dans sa classe ;
- ◇ six transpositions ;
- ◇ huit 3-cycles ;
- ◇ six 4-cycles ;
- ◇ trois double transpositions.

12. On utilise la propriété suivante : si K est un sous-groupe distingué de G et H est un sous-groupe de G, alors $\mathrm{KH} = \{kh \mid k \in \mathrm{K},\ h \in \mathrm{H}\}$ est un sous-groupe de G ; cela découle de :

$$\forall\, k_1,\, k_2 \in \mathrm{K},\ \forall\, h_1,\, h_2 \in \mathrm{H} \qquad (k_1 h_1)(k_2 h_2) = \underbrace{k_1 \underbrace{h_1 k_2 h_1^{-1}}_{\in \mathrm{K}} \underbrace{h_1 h_2}_{\in \mathrm{H}}}_{\in \mathrm{K}} \in \mathrm{KH}$$

Il est impossible d'écrire $8 = |\text{2-Sylow}|$ sous la forme

$$1 + 6\ell + 8k + 3p$$

avec $\ell \in \{0, 1, 2\}$, $k \in \{0, 1\}$, $p \in \{0, 1\}$ (rappelons que d'une part un sous-groupe distingué est une union de classes de conjugaison et que d'autre un groupe contient l'élément neutre ; en particulier la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : le groupe $\mathfrak{S}_4$ contient trois sous-groupes d'ordre 8.

Exercice 369

Soient p un nombre premier et n un entier naturel avec $p > n$. Considérons un groupe G d'ordre pn et H un sous-groupe de G d'ordre p. Montrer que H est un sous-groupe distingué de G.

Indication : compter les p-Sylow de G.

Éléments de réponse 369

D'après les hypothèses, $\text{pgcd}(p, n) = 1$, donc H est un p-Sylow de G. Notons n_p le nombre de p-Sylow de G. Alors par les théorèmes de Sylow, $n_p \equiv 1 \bmod p$ et $n_p | n$. Si $n_p \neq 1$, alors $n_p \geq p + 1$, ce qui contredit que n_p divise n puisque $n < p$. Ainsi, $n_p = 1$ et H est l'unique p-Sylow de G donc est distingué dans G.

Exercice 370

Déterminer à isomorphisme près tous les groupes d'ordre 33.

Éléments de réponse 370

Soit G un groupe d'ordre 33.

Les éléments de G sont d'ordre 1, 3, 11 ou 33. Une application directe des théorèmes de Sylow montre que G contient un unique 3-Sylow S_3 et un unique 11-Sylow S_{11}. En effet soit n_p le nombre de p-Sylow de G ; d'une part $n_3 \equiv 1 \bmod 3$ et $n_3 | 11$, d'autre part $n_{11} \equiv 1 \bmod 11$ et $n_{11} | 3$, *i.e.* $n_{11} = 1$. Les éléments d'ordre 3 sont contenus dans S_3, les éléments d'ordre 11 dans S_{11}. On a au plus

$$\underbrace{1}_{\text{élément neutre } e} + \underbrace{3-1}_{\text{éléments de } S_3 \smallsetminus \{e\}} + \underbrace{11-1}_{\text{éléments de } S_{11} \smallsetminus \{e\}} = 1 + 2 + 10 = 13$$

éléments d'ordre 1, 3 ou 11. Puisque $|\text{G}| = 33$ le groupe G contient un élément d'ordre 33 et est donc cyclique isomorphe à $\mathbb{Z}/33\mathbb{Z}$.

Exercice 371

Considérons le groupe $\text{G} = \text{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ des matrices inversibles de taille 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Déterminer l'ordre de G.
2. Déterminer les classes de conjugaison de G.

3. Déterminer les centralisateurs des éléments de G (on rappelle que le centralisateur d'un élément g de G est $Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}$).
4. Déterminer les sous-groupes de G.
5. Déterminer les sous-groupes de Sylow de G.
6. Déterminer les sous-groupes distingués de G.
7. Déterminer le centre de G.
8. Déterminer le groupe dérivé de G.
9. Déterminer les normalisateurs et les classes de conjugaison des sous-groupes de G.

Éléments de réponse 371

1. Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $n \in \mathbb{N}^*$. Le groupe $\mathrm{GL}(n, \mathbb{F}_p)$ est un fini de cardinal

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$

en effet se donner une matrice de $\mathrm{GL}(n, \mathbb{F}_p)$ revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. Nous obtenons que $|\mathrm{GL}(2, \mathbb{F}_2)| = (2^2-1)(2^2-2) = 6$. Ses éléments sont

$$\mathrm{id}, \quad S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_3 = {}^{\mathrm{t}}S_2, \quad R = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad R^2 = R^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

2. Déterminons les classes de conjugaison de G.

> Rappel : soit G un groupe, la classe de conjugaison d'un élément g de G est
> $$\{hgh^{-1} \,|\, h \in \mathrm{G}\}$$
> Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n (cela découle de la formule $(hgh^{-1})^k = hg^kh^{-1}$).

On vérifie sans difficulté que S_1, S_2, S_3 sont d'ordre 2 et R, R^{-1} sont d'ordre 3.

Puisque

$$S_2RS_2^{-1} = S_2RS_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = R^{-1}$$

l'élément R^{-1} est dans la classe de conjugaison de R ; c'est le seul avec R (tout élément de la classe de conjugaison de R est nécessairement d'ordre 3).

Les éléments S_2 et S_3 appartiennent à la classe de conjugaison de S_1 : $RS_1R^{-1} = S_3$ et $R^{-1}S_1R = S_2$ et ce sont les seuls avec S_1 (tout élément de la classe de conjugaison de S_1 est nécessairement d'ordre 2) : la classe de conjugaison de S_1 est $\{S_1, S_2, S_3\}$.

De même on obtient que la classe de conjugaison de S_2 (resp. S_3) est $\{S_1, S_2, S_3\}$.

On remarque que la trace d'une matrice non scalaire caractérise sa classe de conjugaison.

3. Déterminons les centralisateurs des éléments de G.

Rappel : si G est un groupe, alors le centralisateur de l'élément $g \in \mathrm{G}$ est $Z_g = \{h \in \mathrm{G} \mid hg = gh\}$. de

Le centralisateur de R ou R^{-1} est d'ordre $\frac{|\mathrm{G}|}{2} = 3$; puisqu'il contient $\langle R\rangle$ qui est d'ordre 3 le centralisateur de R et $\langle R\rangle$ coïncident.

Le centralisateur d'un élément S de la classe de conjugaison $\{S_1, S_2, S_3\}$ est d'ordre $\frac{|\mathrm{G}|}{3} = 2$, il s'agit donc de $\langle S\rangle$.

4. Déterminons les sous-groupes de G.

Les sous-groupes non triviaux de G sont $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$, et $\langle R\rangle = \langle R^{-1}\rangle$.

5. Déterminons les sous-groupes de Sylow de G.

Notons que $|\mathrm{G}| = 2 \times 3$; par suite nous nous intéressons aux 2-Sylow et aux 3-Sylow de G.

Les 2-Sylow de G sont $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$.

Le groupe G possède un unique 3-Sylow : $\langle R\rangle = \langle R^{-1}\rangle$.

6. Déterminons les sous-groupes distingués propres de G.

Première méthode.

Puisque la classe de conjugaison de S_i n'est pas contenue dans $\langle S_i\rangle$ le sous-groupe $\langle S_i\rangle$ n'est pas distingué dans G.

Comme la classe de conjugaison de R est contenue dans $\langle R\rangle$ le sous-groupe $\langle R\rangle$ est distingué dans G.

Seconde méthode.

Puisque $\langle R\rangle$ est l'unique 3-Sylow de G, il est distingué dans G.

Les 2-Sylow étant au nombre de 3, ils ne sont pas distingués dans G.

Par suite G contient un unique sous-groupe distingué non trivial : $\langle R\rangle$.

7. Déterminons le centre de G.

Rappelons que si G est un groupe ; alors $\bigcap_{g\in\mathrm{G}} Z_g = Z(\mathrm{G})$.

Or d'après 3.

$$\bigcap_{g\in \mathrm{G}} Z_g = \mathrm{G} \cap \langle S_1\rangle \cap \langle S_2\rangle \cap \langle S_3\rangle \cap \langle R\rangle = \{\mathrm{id}\},$$

le centre de G est donc réduit à $\{\mathrm{id}\}$.

8. Déterminons le groupe dérivé de G.

> Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
> Le groupe $D(\mathrm{G})$ est un sous-groupe distingué de G.
> Le groupe $\mathrm{G}/D(\mathrm{G})$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que $\mathrm{G}/D(\mathrm{G})$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

Les sous-groupes distingués de G sont $\{\mathrm{id}\}$, $\langle R\rangle$ et G ; ainsi les quotients à considérer sont $\mathrm{G}/\{\mathrm{id}\} = \mathrm{G}$, $\mathrm{G}/\langle R\rangle$ et $\mathrm{G}/\mathrm{G} = \{\mathrm{id}\}$. Le groupe G n'étant pas abélien, le plus grand (au sens de l'inclusion) quotient abélien de G est $\mathrm{G}/\langle R\rangle$ ou $\{\mathrm{id}\}$. Nous sommes donc ramenés à considérer la question suivante : le groupe $\mathrm{G}/\langle R\rangle$ est-il abélien ? Notons que $\left|\mathrm{G}/\langle R\rangle\right| = \frac{|\mathrm{G}|}{|\langle R\rangle|} = \frac{6}{3} = 2$; or un sous-groupe d'ordre 2 est abélien donc $\mathrm{G}/\langle R\rangle$ est abélien et c'est le plus grand quotient abélien de G. Il en résulte que $D(\mathrm{G}) = \langle R\rangle$.

9.

> Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est
> $$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$
> Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Puisque $\langle R\rangle$ est distingué dans G le normalisateur $N_{\mathrm{G}}(\langle R\rangle)$ est G. De plus le fait que $\langle R\rangle$ soit distingué dans G implique que la classe de conjugaison de $\langle R\rangle$ est

$$C_{\langle R\rangle} = \{g\langle R\rangle g^{-1} \,|\, g \in \mathrm{G}\} = \{\langle R\rangle\}.$$

Considérons désormais l'action de G sur l'ensemble X des sous-groupes de G :

$$\mathrm{G} \times X \to X, \qquad\qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}.$$

De même que précédemment nous pouvons vérifier que $\mathrm{St}(\mathrm{H}) = N_{\mathrm{G}}(\mathrm{H})$, que $\mathcal{O}_{\mathrm{H}} = C_{\mathrm{H}}$ et que $|\mathrm{G}| = |N_{\mathrm{G}}(\mathrm{H})|\,|C_{\mathrm{H}}|$.

Les $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$ forment une classe de conjugaison puisque les S_i sont conjugués, *i.e.* $C_{\langle S_i\rangle} = \{\langle S_1\rangle, \langle S_2\rangle, \langle S_3\rangle\}$ pour tout $i \in \{1, 2, 3\}$. Il en résulte que le normalisateur

$N_{\langle S_i\rangle}(\mathrm{G})$ de $\langle S_i\rangle$ est d'ordre $\frac{|\mathrm{G}|}{|C_{\langle S_i\rangle}|} = \frac{6}{3} = 2$; de plus $N_{\langle S_i\rangle}(\mathrm{G})$ contient $\langle S_i\rangle$. Par suite $N_{\langle S_i\rangle}(\mathrm{G}) = \langle S_i\rangle$. Enfin G compte trois 2-Sylow qui sont les $\langle S_i\rangle$.

Remarque. Le groupe G est d'ordre 6 non abélien donc isomorphe à $\mathfrak{S}_3$.

Exercice 372

1. Quels sont les sous-groupes de Sylow de $\mathcal{A}_4$?
2. Déterminer l'ordre de tous les éléments de $\mathcal{A}_4$.

   Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.

   Montrer que H contient au moins trois éléments d'ordre 3.

   Peut-il être isomorphe à $\mathfrak{S}_3$?
4. Donner la liste des sous-groupes distingués du groupe alterné $\mathcal{A}_4$, en justifiant rapidement que votre liste est complète et non redondante.
5. En déduire qu'il n'y a pas de sous-groupe d'ordre 6 dans $\mathcal{A}_4$.
6. Donner la liste des sous-groupes de $\mathcal{A}_4$.

Éléments de réponse 372

1. Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$.

   L'ordre de $\mathcal{A}_4$ est $12 = 2^2 \times 3$. Soient n_2 le nombre de sous-groupes de Sylow d'ordre $2^2 = 4$ et n_3 le nombre de sous-groupes de Sylow d'ordre 3. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \text{ et } n_2|3, \qquad n_3 \equiv 1 \bmod 3 \text{ et } n_3|2^2 = 4$$

   autrement dit que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$.

   Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 (ils sont de signature -1) et ne contient pas de transpositions (elles sont de signature -1) donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois donc $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4 isomorphe au groupe de Klein, *i.e.* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet d'après le théorème de Lagrange un sous-groupe K de $\mathcal{A}_4$ d'ordre 4 contient des éléments d'ordre 1, 2 ou 4 ; mais $\mathcal{A}_4$ ne contient pas d'élément d'ordre 2 donc K contient des éléments d'ordre 1 ou 4. Comme $\mathcal{A}_4$ contient un seul élément d'ordre 1 et trois éléments d'ordre 4 il contient un seul sous-groupe d'ordre 4).

   Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.
2. Déterminons l'ordre de tous les éléments de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?

   Le groupe $\mathcal{A}_4$ contient trois éléments d'ordre 2, huit éléments d'ordre 3 et un élément d'ordre 1. Le groupe $\mathcal{A}_4$ ne contient donc aucun élément d'ordre 6 ; par suite il ne contient pas de sous-groupe cyclique d'ordre 6.

3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3 ; désignons par $(a\ b)(c\ d)$ l'élément d'ordre 2 et par $(a\ b\ c)$ celui d'ordre 3.

   Notons que

   $$(a\ b)(c\ d)(a\ b\ c) = (b\ d\ c) \qquad (a\ b\ c)(a\ b)(c\ d) = (a\ c\ d).$$

   Le groupe H contient les 3-cycles : $(a\ b\ c)$, $(a\ c\ d)$ et $(b\ d\ c)$ donc les trois sous-groupes d'ordre 3

   $$\langle (a\ b\ c)\rangle, \qquad \langle (a\ c\ d)\rangle, \qquad \langle (b\ d\ c)\rangle.$$

   Un groupe d'ordre 6 ne contient qu'un sous-groupe d'ordre 3 (en effet soit K un sous-groupe d'ordre $6 = 2\times 3$. Désignons par n_3' le nombre de 3-Sylow de K ; d'une part $n_3' \equiv 1$ mod 3 d'autre part $n_3'|2$ donc $n_3' = 1$). Par conséquent le groupe H n'est pas d'ordre 6. En particulier, H ne peut pas être isomorphe à $\mathfrak{S}_3$ qui est d'ordre 6.

4. Il y a quatre classes de conjugaison dans $\mathcal{A}_4$, qui sont l'identité, les trois double-transpositions, et deux classes de 3-cycles (chacune de cardinal 4 : en effet le stabilisateur d'un 3-cycle est d'ordre exactement 3, puisque c'était déjà le cas dans $\mathfrak{S}_4$). Comme tous sous-groupe distingué est une union de classes de conjugaison, et est d'ordre un diviseur de 12, on obtient exactement trois sous-groupes distingués dans $\mathcal{A}_4$: $\{\mathrm{id}\}$, $\mathcal{A}_4$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le sous-groupe d'ordre 4 contenant les double-transpositions.
5. Un sous-groupe d'ordre 6 de $\mathcal{A}_4$ serait d'indice 2, donc distingué car tout sous-groupe d'indice 2 est distingué. On conclut par la question précédente que $\mathcal{A}_4$ n'admet aucun sous-groupe d'ordre 6.
6. Le groupe $\mathcal{A}_4$ contient :
   - un sous-groupe d'ordre 1 : $\{\mathrm{id}\}$;
   - trois sous-groupes d'ordre 2 :

     $$\langle (1\ 2)(3\ 4)\rangle \qquad \langle (1\ 3)(2\ 4)\rangle \qquad \langle (1\ 4)(2\ 3)\rangle;$$

   - quatre sous-groupes d'ordre 3 :

     $$\langle (1\ 2\ 3)\rangle \qquad \langle (1\ 2\ 4)\rangle \qquad \langle (1\ 3\ 4)\rangle \qquad \langle (2\ 3\ 4)\rangle;$$

   - un sous-groupe d'ordre 4 :

     $$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 373 [Simplicité de $\mathcal{A}_n$, $n \geq 5$]

I) Commençons par démontrer que le groupe $\mathcal{A}_5$ est simple.

Soit G un groupe. Un sous-groupe H de G est caractéristique si pour tout automorphisme φ de G on $\varphi(\mathrm{H}) \subset \mathrm{H}$.

I) a) Montrer que tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

I) b) Montrer que tout groupe d'ordre 15 est cyclique.

I) c) Montrer que tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

I) d) Montrer que tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

I) e) Montrer que tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

I) f) Montrer que tout groupe d'ordre 12 contient un sous-groupe caractéristique.

I) g) Montrer que tout groupe d'ordre 6 contient un sous-groupe caractéristique.

I) h) Montrer que tout groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow est simple.

I) i) Montrer que le groupe $\mathcal{A}_5$ est simple.

II) Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué de $\mathcal{A}_n$ non trivial.

II) a) Montrer qu'il existe $\tau \in \mathrm{H}$ distinct de l'identité qui a au moins un point fixe.

II) b) Montrer que pour tout $1 \leq j \leq n$ le sous-groupe $\mathrm{G}_j = \mathrm{St}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

II) c) Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$. Montrer que $\mathcal{A}_n = \mathrm{H}$.

II) d) En déduire que $\mathcal{A}_n$ est simple pour $n \geq 5$.

Éléments de réponse 373

I) a) Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué dans G. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué dans G. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$.

I) b) Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique.

I) c) Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.

Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.

— Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant id fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 de G.

— Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $K \cap H = \{id\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

I) d) Au I) c) on a vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caractéristiques (voir I)a)) dans le groupe KH qui est cyclique et distingué dans G (car d'indice 2 dans G). Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow.

I) e) Soit G un groupe d'ordre $20 = 2^2 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$.

I) f) Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué dans G ; ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (cf I) a)).

— Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \mid 3$$

Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué dans G et donc caractéristique dans G (cf I) a)).

I) g) Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ses 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et I) b) permet de conclure.

I) h) Soit G un groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 12$$

d'où $n_5 \in \{1, 6\}$. Par hypothèse $n_5 \neq 1$ donc $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G. Notons que

$$|\mathrm{H}| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

- ◇ Si $|\mathrm{H}|$ est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en déduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs $|\mathrm{H}|$ divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$). Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 (voir I)d)) : contradiction avec le fait qu'il en contient 6. Par suite $|\mathrm{H}|$ n'est pas divisible par 5.
- ◇ Si $|\mathrm{H}|$ appartient à $\{6, 12\}$, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4 (d'après I)f) et I)g)). Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G.
- ◇ Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4. Dans ce cas G/H est d'ordre 30, 20 ou 15 (on renvoie à I)d) si G/H est d'ordre 30, à I)e) si G/H est d'ordre 20 ; enfin si G/H est d'ordre $15 = 3 \times 5$ et si n_5 est le nombre de 5-Sylow de G/H, les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et n_5 divise 3 donc $n_5 = 1$). Donc G/H contient un sous-groupe K distingué d'ordre 5. Considérons la surjection canonique $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $\mathrm{K} = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction (voir le premier ◇ du I)h)).

I) i) Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles (1 2 3 4 5) et (1 3 2 4 5). D'après I) h) le groupe $\mathcal{A}_5$ est simple.

II) a) **Remarque**. Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Raisonnons par l'absurde : supposons qu'aucun élément non trivial de H n'a de point fixe, *i.e.* supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$.

- ◇ Montrons dans un premier temps qu'aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Raisonnons par l'absurde : supposons qu'il existe τ dans H tel que la décomposition de τ en produit de cycles disjoints contient un cycle d'ordre ≥ 3 alors on peut écrire

$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$

Puisque $n \geq 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors

$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$

Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La remarque qui précède assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Les éléments de H sont donc des produits de transpositions disjointes.

$\diamond$ Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ est une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit

$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$

Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a

$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$

D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (cf Remarque). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction.

Le groupe H contient donc au moins un élément non trivial qui possède un point fixe.

II) b) Soit τ un élément de $\mathrm{H} \setminus \{\mathrm{id}\}$ pour lequel il existe $1 \leq i \leq n$ tel que $\tau(i) = i$ (l'existence d'un tel τ est assurée par II) a)). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple donc ou bien $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$ ou bien $\mathrm{G}_i \cap \mathrm{H} = \{\mathrm{id}\}$. Or τ est un élément non trivial de $\mathrm{G}_i \cap \mathrm{H}$ donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathfrak{S}_n$ on a $\sigma\mathrm{G}_i\sigma^{-1} = \mathrm{G}_{\sigma(i)}$ d'où $\mathrm{G}_i \subset \mathrm{H}$ donc $\mathrm{G}_{\sigma(i)} = \sigma\mathrm{G}_i\sigma^{-1} \subset \sigma\mathrm{H}\sigma^{-1} = \mathrm{H}$. Autrement dit pour tout $1 \leq j \leq n$ on a l'inclusion $\mathrm{G}_j \subset \mathrm{H}$.

II) c) Bien sûr $\mathrm{H} \subset \mathcal{A}_n$ donc pour montrer que $\mathcal{A}_n = \mathrm{H}$ il suffit de montrer que $\mathcal{A}_n \subset \mathrm{H}$. Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \ldots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n$. Mais $\mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n \subset \mathrm{H}$ (cf II) b)). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$.

II) d) Le groupe $\mathcal{A}_5$ est simple (I)i)). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (cf II) c)).

Exercice 374

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.

   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}.$$

   Montrer par un calcul direct que cette action est transitive.

   Quel est le stabilisateur de

   $$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

3. On note $\mathfrak{S}_X$ le groupe des bijections de X dans lui-même.

   Montrer que

   $$\phi \colon \mathrm{G} \to \mathfrak{S}_X, \qquad\qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

Éléments de réponse 374

1. Déterminons l'ordre de G. Se donner un élément de G c'est se donner une première colonne non nulle ($2^2 - 1 = 3$ choix) et une seconde colonne non colinéaire à la première ($2^2 - 2 = 2$ choix). Nous en déduisons que $|\mathrm{G}| = 6$.

   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?

   Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \text{ et } n_2 | 3, \qquad\qquad n_3 \equiv 1 \bmod 3 \text{ et } n_3 | 2$$

   Par conséquent $n_3 = 1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $D^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

   Les éléments d'ordre 2 sont

   $$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

   chacun engendre un 2-Sylow de G.

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\{\langle A\rangle, \langle B\rangle, \langle C\rangle\}$.

   On fait agir G sur X par conjugaison :

   $$\mathrm{G} \times X \to X, \qquad\qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1} = \{ghg^{-1} \mid h \in \mathrm{H}\}.$$

Montrons que cette action est transitive ; cela revient à montrer qu'il y a une seule orbite. Par exemple montrons que $\mathcal{O}_{\langle A\rangle} = X$; un calcul direct conduit à :

$$A \cdot \langle A\rangle = \langle A\rangle \qquad B \cdot \langle A\rangle = \langle C\rangle \qquad C \cdot \langle A\rangle = \langle B\rangle$$

dont on déduit l'inclusion $X \subset \mathcal{O}_{\langle A\rangle}$; comme par définition $\mathcal{O}_{\langle A\rangle} \subset X$ nous obtenons finalement que $\mathcal{O}_{\langle A\rangle} = X$.

Déterminons le stabilisateur $\mathrm{St}(\langle A\rangle) = \{g \in \mathrm{G} \,|\, g \cdot \langle A\rangle = \langle A\rangle\}$ de $\langle A\rangle$. La bijection entre ${}^{\mathrm{G}}\!/_{\mathrm{St}(\langle A\rangle)}$ et $\mathcal{O}_{\langle A\rangle}$ assure que $\#{}^{\mathrm{G}}\!/_{\mathrm{St}(\langle A\rangle)} = \#\mathcal{O}_{\langle A\rangle}$; ceci entraîne :

$$|\mathrm{St}(\langle A\rangle)| = \frac{|\mathrm{G}|}{\#\mathcal{O}_{\langle A\rangle}} = \frac{|\mathrm{G}|}{\#X} = \frac{6}{3} = 2.$$

Un calcul direct montre que Id et A appartiennent à $\mathrm{St}(\langle A\rangle)$. Finalement $\mathrm{St}(\langle A\rangle) = \{\mathrm{Id}, A\}$

3. On note $\mathfrak{S}_X$ le groupe des bijections de X dans lui-même. Soit ϕ le morphisme de groupes associé à l'action de G sur X :

$$\phi\colon \mathrm{G} \to \mathfrak{S}_X, \qquad g \mapsto (\mathrm{S} \mapsto g \cdot \mathrm{S} = g\mathrm{S}g^{-1})$$

Il est injectif car

$$\begin{aligned}
\ker\phi &= \{g \in \mathrm{G} \,|\, \phi(g) = \mathrm{id}_{\mathfrak{S}_X}\} \\
&= \{g \in \mathrm{G} \,|\, g \cdot \mathrm{S} = \mathrm{S} \quad \forall\, \mathrm{S} \in X\} \\
&= \bigcap_{\mathrm{S}\in X} \mathrm{St}(\mathrm{S}) \\
&= \langle A\rangle \cap \langle B\rangle \cap \langle C\rangle \cap \\
&= \{e\}.
\end{aligned}$$

De plus $|\mathfrak{S}_X| = |\mathrm{G}| = 6$ nous obtenons que ϕ est un isomorphisme de groupes.

Exercice 375

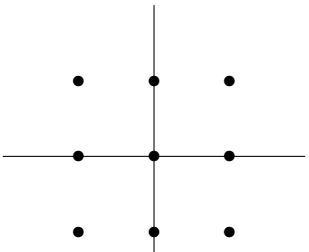
Considérons le sous-groupe H de $\mathrm{GL}(2,\mathbb{R})$ engendré par $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Donner tous les éléments de H.
2. À quel groupe classique H est-il isomorphe ?

   Considérons l'ensemble : $E := \left\{ \begin{pmatrix} x \\ y \end{pmatrix},\ (x,y) \in \{-1;0;1\}^2 \right\}$.
3. Représenter l'ensemble E sur un graphique.
4. Montrer que

$$\varphi\colon \mathrm{H} \times E \to E, \qquad (M, X) \mapsto MX$$

définit bien une action de groupe de H sur E.



5. Cette action est-elle fidèle ?
6. Cette action est-elle transitive ? En donner les orbites.
7. Déterminer le stabilisateur de l'ensemble $\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}-1\\0\end{pmatrix}\right\}$.
8. Décrire les sous-ensembles de E admettant un stabilisateur non-trivial.

Éléments de réponse 375

1. Notons P la matrice $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$; alors

$$P^2 = -\mathrm{Id}, \qquad P^3 = -P, \qquad P^4 = \mathrm{Id}.$$

   Les éléments de H sont donc : Id, P, $-\mathrm{Id}$ et $-P$.

2. Le groupe H est d'ordre 4 et contient un élément d'ordre 4 (la matrice $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$) donc H est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

   Considérons l'ensemble : $E := \left\{\begin{pmatrix}x\\y\end{pmatrix},\ (x,y) \in \{-1;0;1\}^2\right\}$.

3. L'ensemble E est constitué des neuf points de coordonnées

$$(-1,-1),\quad (-1,0),\quad (-1,1),\quad (0,-1),\quad (0,0),\quad (0,1),\quad (1,-1),\quad (1,0),\quad (1,1).$$

4. Montrons que

$$\mathrm{H} \times E \to E, \qquad (M,X) \mapsto M \cdot X = MX$$

   définit bien une action de H sur E :

   ◇ pour tout $X \in E$ nous avons $\mathrm{Id} \cdot X = \mathrm{Id}X = X$;

◇ pour tous M, N dans H, pour tout $X \in E$ nous avons

$$(MN)\cdot X = (MN)X = MNX \qquad M\cdot(N\cdot X) = M\cdot(NX) = M(NX) = MNX$$

d'où $(MN)\cdot X = M\cdot(N\cdot X)$.

5. Soit $M \in \mathrm{H}$ tel que $M\cdot X = X$ pour tout $X \in E$, *i.e.* tel que $MX = X$ pour tout $X \in E$. Écrivons M sous la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

   D'une part $M\cdot\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ implique $M\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ou encore

   $$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

   D'autre part $M\cdot\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ implique $M\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ou encore

   $$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

   Autrement dit $M = \mathrm{Id}$ est l'unique élément de H à vérifier $M\cdot\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $M\cdot\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. L'action est donc fidèle.

6. Pour tout $M \in \mathrm{H}$ nous avons $M\cdot\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, l'action n'est donc pas transitive.

   Par définition

   $$\begin{aligned} \mathcal{O}_X &= \mathcal{O}_{\begin{pmatrix} x \\ y \end{pmatrix}} \\ &= \{M\cdot X \,|M \in \mathrm{H}\} \\ &= \{MX \,|M \in \mathrm{H}\} \\ &= \{\mathrm{Id}X,\, PX,\, -\mathrm{Id}X,\, -PX\} \\ &= \{\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} -y \\ x \end{pmatrix}, \begin{pmatrix} -x \\ -y \end{pmatrix}, \begin{pmatrix} y \\ -x \end{pmatrix}\} \end{aligned}$$

   D'où

   $$\mathcal{O}_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\mathcal{O}\begin{pmatrix}1\\0\end{pmatrix}=\mathcal{O}\begin{pmatrix}-1\\0\end{pmatrix}=\mathcal{O}\begin{pmatrix}0\\1\end{pmatrix}=\mathcal{O}\begin{pmatrix}0\\-1\end{pmatrix}=\left\{\begin{pmatrix}-1\\0\end{pmatrix},\begin{pmatrix}0\\-1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$$

$$\mathcal{O}\begin{pmatrix}-1\\-1\end{pmatrix}=\mathcal{O}\begin{pmatrix}1\\-1\end{pmatrix}=\mathcal{O}\begin{pmatrix}1\\1\end{pmatrix}=\mathcal{O}\begin{pmatrix}-1\\1\end{pmatrix}=\left\{\begin{pmatrix}-1\\-1\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}-1\\1\end{pmatrix}\right\}$$

Dans le second cas nous

7. Déterminons le stabilisateur de l'ensemble $\Upsilon=\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}-1\\0\end{pmatrix}\right\}$.

   On cherche les $M\in \mathrm{H}$ tels que

   - ou bien $M\cdot\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$ et $M\cdot\begin{pmatrix}-1\\0\end{pmatrix}=\begin{pmatrix}-1\\0\end{pmatrix}$ ce qui conduit à $M=\mathrm{Id}$;
   - ou bien $M\cdot\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}-1\\0\end{pmatrix}$ et $M\cdot\begin{pmatrix}-1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$ ce qui conduit à $M=-\mathrm{Id}$.

   Par conséquent le stabilisateur de Υ est $\{\mathrm{Id},-\mathrm{Id}\}$.

8. Posons $\Omega_0=\{(0,0)\},\Omega_1=\{(1,0),\,(-1,0)\},\Omega_2=\{(0,1),\,(0,-1)\},\Omega_3=\{(1,1),\,(-1,-1)\}$ et $\Omega_4=\{(1,-1),\,(-1,1)\}$.

   Le seul sous-groupe non-trivial de H est $\{\mathrm{Id},-\mathrm{Id}\}$. Ainsi, si F est un sous-ensemble de stabilisateur non-trivial celui-ci est $\{\mathrm{Id},-\mathrm{Id}\}$. Un tel ensemble F doit satisfaire la propriété suivante : si x appartient à F, alors $-x$ appartient à F, *i.e.* il est nécessairement réunion de certains des sous-ensembles suivants : Ω_0, Ω_1, Ω_2, Ω_3 et Ω_4.

   Par conséquent il y a $2^5=32$ sous-ensembles éventuellement possibles. Nous excluons ceux dont le stabilisateur est H qui sont les sous-ensembles que l'on obtient à partir des 3 orbites :

$\emptyset$,	$\Omega_1\cup\Omega_2$,	$\Omega_3\cup\Omega_4$,	$\Omega_1\cup\Omega_2\cup\Omega_3\cup\Omega_4$,
Ω_0,	$\Omega_0\cup\Omega_1\cup\Omega_2$,	$\Omega_0\cup\Omega_3\cup\Omega_4$,	$\Omega_0\cup\Omega_1\cup\Omega_2\cup\Omega_3\cup\Omega_4$.

   Ainsi les sous-ensembles de E admettant un stabilisateur non-trivial sont les 24 ensembles suivants :

Ω_1,	Ω_2,	Ω_3,	Ω_4,
$\Omega_1\cup\Omega_3$,	$\Omega_1\cup\Omega_4$,	$\Omega_2\cup\Omega_3$,	$\Omega_2\cup\Omega_4$,
$\Omega_1\cup\Omega_2\cup\Omega_3$,	$\Omega_1\cup\Omega_2\cup\Omega_4$,	$\Omega_1\cup\Omega_3\cup\Omega_4$,	$\Omega_2\cup\Omega_3\cup\Omega_4$,
$\Omega_0\cup\Omega_1$,	$\Omega_0\cup\Omega_2$,	$\Omega_0\cup\Omega_3$,	$\Omega_0\cup\Omega_4$,
$\Omega_0\cup\Omega_1\cup\Omega_3$,	$\Omega_0\cup\Omega_1\cup\Omega_4$,	$\Omega_0\cup\Omega_2\cup\Omega_3$,	$\Omega_0\cup\Omega_2\cup\Omega_4$,
$\Omega_0\cup\Omega_1\cup\Omega_2\cup\Omega_3$,	$\Omega_0\cup\Omega_1\cup\Omega_2\cup\Omega_4$,	$\Omega_0\cup\Omega_1\cup\Omega_3\cup\Omega_4$,	$\Omega_0\cup\Omega_2\cup\Omega_3\cup\Omega_4$.

Exercice 376

Déterminer les p-Sylow de $\mathbb{Z}/n\mathbb{Z}$ pour tout diviseur p de n.

Éléments de réponse 376

Posons $G = \mathbb{Z}/n\mathbb{Z}$. Le groupe G est abélien ; par suite tous les sous-groupes de G sont distingués. En particulier si H est un p-Sylow de G, alors H est un p-Sylow de G distingué dans G donc H est l'unique p-Sylow de G. Il en résulte que G possède un seul p-Sylow, et ce pour tout diviseur p de n.

Plus précisément, si on écrit n sous la forme $p^\alpha m$ avec $p \not| m$, le groupe H est le sous-groupe $m\mathbb{Z}/n\mathbb{Z}$ de $G = \mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m modulo n.

Exercice 377

Montrer que $\mathfrak{S}_4$ possède trois 2-sous-groupes de Sylow isomorphes à D_8.

Éléments de réponse 377

Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $D_8 \subset \mathfrak{S}_4$.

Soit n_2 le nombre de 2-Sylow de $\mathfrak{S}_4$. Le groupe D_8 est l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathfrak{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathfrak{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathfrak{S}_4$.

Exercice 378

Soit G un groupe. Soit p un nombre premier divisant $|G|$.

Montrer que si H est un p-sous-groupe de G distingué dans G, alors H est contenu dans tout p-sous-groupe de Sylow de G.

Éléments de réponse 378

Si H est un p-sous-groupe de G, il existe un p-Sylow de G qui contient H. Puisque H est distingué dans G et que les p-Sylow sont conjugués entre eux, H se trouve dans tous les p-Sylow de G.

Exercice 379

Montrer qu'un groupe d'ordre 56 n'est pas simple.

Éléments de réponse 379

Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-Sylow et n_7 le nombre de 7-Sylow.

D'après les théorèmes de Sylow

$$n_2 \equiv 1 \pmod 2 \qquad n_2 | 7$$

$$n_7 \equiv 1 \pmod 7 \qquad n_7 | 8$$

Par conséquent $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7-1$ = nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc « listé » 49 éléments du groupe G. Nous allons les noter $g_1 = e$, g_2, …, g_{49}. Supposons que $n_2 = 7$. Soit S un 2-Sylow de G ; il est d'ordre 8. Notons e, h_2, …, h_8 ses éléments. Pour des raisons d'ordre les h_i n'appartiennent pas $\{g_1, g_2, \ldots, g_{49}\}$. Donc G contient les éléments distincts g_1, g_2, …, g_{49}, h_2, h_3, …, h_8 ; en particulier $|\mathrm{G}| \geq 49 + 7 = 56$. Par hypothèse $n_2 = 7$ donc G contient un 2-Sylow T distinct de S. Soit k dans $\mathrm{T} \setminus \mathrm{S}$. Pour des raisons d'ordre k n'appartient pas $\{g_1, g_2, \ldots, g_{49}\}$. Par suite G contient les éléments distincts g_1, g_2, …, g_{49}, h_2, h_3, …, h_8, k. En particulier $|\mathrm{G}| \geq 49 + 7 + 1 = 57$: contradiction. Par conséquent $n_2 \neq 7$ et $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 380

1. Montrer qu'il n'y a pas de groupe simple d'ordre 42.
2. Montrer qu'il n'y a pas de groupe simple d'ordre 105.

Éléments de réponse 380

1. Montrons qu'il n'y a pas de groupe simple d'ordre 42.

   Soit G un groupe d'ordre 42. La décomposition de 42 en nombres premiers est $42 = 2 \times 3 \times 7$. Désignons par s_7 le nombre de 7-Sylow de G. Les théorèmes de Sylow assurent que d'une part $s_7 \equiv 1 \pmod 7$ et que d'autre part $s_7 \,|\, 6$. Il s'en suit que $s_7 = 1$, autrement dit G contient un seul 7-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.

2. Montrons qu'il n'y a pas de groupe simple d'ordre 105.

   Soit G un groupe d'ordre 105. La décomposition de 105 en nombres premiers est $105 = 3 \times 5 \times 7$. Désignons par s_7 (resp. s_5) le nombre de 7-Sylow (resp. 5-Sylow) de G. Les théorèmes de Sylow assurent que d'une part $s_7 \equiv 1 \pmod 7$ et que d'autre part $s_7 \,|\, 15$. Il s'en suit que $s_7 \in \{1, 15\}$. Étudions chacune de ces éventualités :

   - ◇ Si $s_7 = 1$, G contient un seul 7-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.

◇ Si $s_7 = 15$, alors il y a six éléments d'ordre 7 dans chaque 7-Sylow ; comme ces 7-Sylow ne peuvent s'intersecter qu'en l'élément neutre (Lagrange), un total de $6 \times 15 = 90$ éléments. Les théorèmes de Sylow assurent que d'une part $s_5 \equiv 1 \pmod 5$ et que d'autre part $s_5 \mid 21$. Par conséquent $s_5 \in \{1, 21\}$.

— Si $s_5 = 1$, G contient un seul 5-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.

— Si $s_5 = 21$, alors chaque 5-Sylow contient quatre éléments d'ordre 5 et

$$\underbrace{\text{nb d'éléments d'ordre 7}}_{90} + \underbrace{\text{nb d'éléments d'ordre 5}}_{84} + \underbrace{\text{neutre}}_{1} > 105 = |\mathrm{G}|$$

contradiction.

Exercice 381

1. Quel est l'ordre du groupe $\mathfrak{S}_4$?
2. Quels sont les ordres des éléments de $\mathfrak{S}_4$? Préciser le nombre d'éléments pour chaque ordre. Vérifier que leur somme est bien égale au cardinal de $\mathfrak{S}_4$.
3. Déterminer le nombre de 3-Sylow dans $\mathfrak{S}_4$.
4. Déterminer le nombre de 2-Sylow dans $\mathfrak{S}_4$.
5. Donner la liste des sous-groupes distingués de $\mathfrak{S}_4$.

Éléments de réponse 381

1. Le groupe $\mathfrak{S}_4$ est d'ordre 24.
2. Le groupe $\mathfrak{S}_4$ possède 24 éléments repartis en cinq classes de conjugaison. En effet, il y a :
   ◇ le neutre, seul dans sa classe ;
   ◇ $\binom{4}{2} = 6$ transpositions ;
   ◇ $2 \times \binom{4}{3} = 8$ 3-cycles ;
   ◇ $3 \times 2 = 6$ 4-cycles ;
   ◇ $\frac{1}{2} \times \binom{4}{2} = 3$ double transpositions.

   On vérifie : $1 + 6 + 8 + 6 + 3 = 24$.
3. Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n_3 de 3-Sylow est congru à 1 modulo 3 et divise 8. Nous avons donc les deux possibilités $n_3 = 1$ ou $n_3 = 4$. Les 3-Sylow de $\mathfrak{S}_4$ sont d'ordre 3. Or un sous-groupe S_3 d'ordre 3 de $\mathfrak{S}_4$ est engendré par un élément d'ordre 3 et chacun contenant deux éléments d'ordre 3 il y en a $\frac{8}{2} = 4$, du type $\langle (a\ b\ c) \rangle$. Puisque les 3-cycles sont conjiugués, les quatre sous-groupes d'ordre 3 sont conjugués ; ce sont les 3-Sylow de $\mathfrak{S}_4$.

4. Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n_2 de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $2^3 = 8$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n_2 = 1$ ou $n_2 = 3$. Montrons que $n_2 = 1$ est impossible. Si $n_2 = 1$, alors l'unique 2-Sylow est un sous-groupe distingué de $\mathfrak{S}_4$. Mais les classes de conjugaison de $\mathfrak{S}_4$ sont de cardinaux 1, 3 et 8, et il est impossible d'obtenir 8 en sommant 1 et 3 ou 8 (rappelons qu'un sous-groupe contient le neutre, donc la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : $\mathfrak{S}_4$ contient trois sous-groupes d'ordre 8.

   Autre rédaction possible

   Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Soit D_8 le groupe des isométries du plan qui préservent un carré ; D_8 est un sous-groupe d'ordre 8 de $\mathfrak{S}_4$. Soit n_2 le nombre de 2-Sylow de $\mathfrak{S}_4$. Les 2-Sylow de $\mathfrak{S}_4$ sont d'ordre 8 ; le groupe D_8 est donc l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathfrak{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathfrak{S}_4$. Il y a donc trois sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathfrak{S}_4$.

5. Les sous-groupes distingués de $\mathfrak{S}_4$ sont : $\{\mathrm{id}\}$, $\mathcal{A}_4$ et $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$, $\mathfrak{S}_4$.

Exercice 382

Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Éléments de réponse 382

Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G.

Les théorèmes de Sylow assurent que $n_p \equiv 1 \pmod p$ et n_p divise q, autrement dit que $n_p \equiv 1 \pmod p$ et $n_p \in \{1, q\}$. Mais comme $p > q$, $q \not\equiv 1 \pmod p$. Par suite $n_p = 1$, *i.e.* il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué et propre. Il s'en suit que G n'est pas simple.

Exercice 383

Soient p et q deux nombres premiers.

Montrer qu'il existe au plus deux structures de groupes d'ordre pq.

Éléments de réponse 383

Exercice 384

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_3)$ le groupe des matrices 2×2 de déterminant égal à 1 et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que G est d'ordre 24.
2. Quel est l'ordre des éléments $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de G ?
3. Combien G a-t-il de 3-sous-groupes de Sylow ?
4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
5. Montrer que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
6. Montrer que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.

Éléments de réponse 384

1. Montrons que G est d'ordre 24.

   Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $n \in \mathbb{N}^*$. Le groupe $\mathrm{GL}(n, \mathbb{F}_p)$ est un fini de cardinal

   $$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$

   en effet se donner une matrice de $\mathrm{GL}(n, \mathbb{F}_p)$ revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. Nous obtenons que $|\mathrm{GL}(2, \mathbb{F}_3)| = 48$.

   Considérons le morphisme $\det\colon \mathrm{GL}(2, \mathbb{F}_3) \to \mathbb{F}_3^*$. C'est un morphisme surjectif et dont le noyau est $\mathrm{SL}(n, \mathbb{F}_3)$. Par conséquent $\mathrm{GL}(2, \mathbb{F}_3)/\mathrm{SL}(2, \mathbb{F}_3) \simeq \mathbb{F}_3^*$ d'où $|\mathrm{SL}(2, \mathbb{F}_3)| = \frac{\mathrm{GL}(2, \mathbb{F}_3)}{|\mathbb{F}_3^*|} = \frac{48}{2} = 24$.
2. Les ordres cherchés sont des diviseurs de 24 bien sûr. La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6. Les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sont d'ordre 3.
3. Soit n_3 le nombre de 3-Sylow de G qui est d'ordre $24 = 2^3 \times 3$. Notons que les 3-Sylow sont donc d'ordre 3. Les théorèmes de Sylow assurent que $n_3 \equiv 1 \pmod 3$ et que n_3 divise $2^3 = 8$. Il s'en suit que $n_3 \in \{1, 4\}$. D'après 2. il y a au moins deux sous-groupes de G d'ordre 3. Par conséquent $n_3 = 4$.
4. Montrons que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.

   Vérifions dans un premier temps que H est d'ordre 8. En effet, $A^2 = B^2 = -\mathrm{id}$ donc A et B sont d'ordre 4. Posons $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. On vérifie que

   $$\mathrm{H} = \{\mathrm{id}, -\mathrm{id}, A, -A, B, -B, C, -C\}$$

(le groupe H est le groupe des quaternions).

Soit $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $N^{-1} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$.

Posons $M = NAN^{-1}$ et $L = NBN^{-1}$. Remarquons que si x appartient à $\mathbb{Z}/3\mathbb{Z}$ et $x \neq \overline{0}$, alors $x^2 = \overline{1}$.

Un calcul montre que

$$M = \begin{pmatrix} bd + ac & -(a^2 + b^2) \\ (c^2 + d^2) & -(bd + ac) \end{pmatrix}$$

Comme N appartient à G, nous avons $ad - bc = \overline{1}$.

Si $a = \overline{0}$, alors $-bc = \overline{1}$ et $b = -c$. Si $d = \overline{0}$, alors $M = A$ appartient à H. Si $d \neq \overline{0}$, alors $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$ ou $M = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -M$; dans les deux cas M appartient à H.

Si maintenant $abcd \neq \overline{0}$, alors $a = -d$ et $b = c$ donc $M = -A$ appartient à H.

On démontre de manière analogue que L appartient à H. Ainsi H est distingué dans G. En effet, soit $P \in$ G, soit $Q \in$ H ; remarquons que Q s'écrit $A^{m_1}B^{p_1}A^{m_2}B^{p_2}\dots A^{m_\ell}B^{p_\ell}$ et

$$\begin{aligned} PQP^{-1} &= P(A^{m_1}B^{p_1}A^{m_2}B^{p_2}\dots A^{m_\ell}B^{p_\ell})P^{-1} \\ &= PA^{m_1}P^{-1}PB^{p_1}P^{-1}PA^{m_2}P^{-1}PB^{p_2}P^{-1}P\dots P^{-1}PA^{m_\ell}P^{-1}PB^{p_\ell}P^{-1} \\ &= (PA^{m_1}P^{-1})(PB^{p_1}P^{-1})(PA^{m_2}P^{-1})(PB^{p_2}P^{-1})P\dots P^{-1}(PA^{m_\ell}P^{-1})(PB^{p_\ell}P^{-1}) \\ &= (PAP^{-1})^{m_1}(PBP^{-1})^{p_1}(PAP^{-1})^{m_2}(PBP^{-1})^{p_2}P\dots P^{-1}(PAP^{-1})^{m_\ell}(PBP^{-1})^{p_\ell} \end{aligned}$$

Or comme on vient de le voir pour tout $P \in$ G PAP^{-1} et PBP^{-1} appartiennent à H ; puisque H est un groupe, nous obtenons que $(PAP^{-1})^{m_i}$ et $(PBP^{-1})^{p_i}$ appartiennent à H pour tous m_i et p_i et finalement que PQP^{-1} appartient à H.

Or H est un 2-Sylow de G, il y a donc un unique sous-groupe d'ordre 8 dans G qui est H.

5. Montrons que G est produit semi-direct de H par un sous-groupe K d'ordre 3.

   Soit K l'un des sous-groupes d'ordre 3 de G. Nous avons les propriétés suivantes : $\mathrm{H} \cap \mathrm{K} = \{e\}$, H est distingué dans G et $3 \times 8 = 24$. Il s'en suit que G est un produit semi-direct de H par K.

   Nous avons $\mathrm{G} = \mathrm{H} \rtimes_\rho \mathrm{K}$ où $\rho\colon \mathrm{K} \to \mathrm{Aut(H)}$ est tel que $\rho(k)$ est l'automorphisme intérieur associé à l'élément $k \in$ K.

6. Montrons que le centre de Z(G) de G est égal à {id, −id}.

   Un élément M de G appartient à Z(G) si en particulier $MA = AM$ et $MB = BM$.

   Or $AM = MA$ si et seulement si

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

et $BM = MB$ si et seulement si

$$\begin{pmatrix} a+b & b+d \\ a+c & b-d \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix}.$$

Ces deux égalités conduisent à $a = d$, $b = -c$, $b + d = a - b$, $a = d$ et $b = c$, soit à $a = d$ et $b = c = 0$, *i.e.* à $M = \pm\mathrm{id}$. Par suite $Z(\mathrm{G}) = \{\mathrm{id}, \mathrm{id}\}$.

Exercice 385

Soit $\mathrm{G} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ où $n \geq 1$.

1. Déterminer l'ordre de G et de ses éléments.
2. Déterminer les sous-groupes de G.
3. Déterminer les quotients de G.

Éléments de réponse 385 Première méthode :

1. et 2. Établissons un résultat dont nous aurons besoin par la suite.

Lemme.

Soit G un groupe. Soit H un sous-groupe distingué de G. Soit $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ le morphisme quotient. Nous avons les deux assertions suivantes :

- ◇ Soit Γ un sous-groupe de G. Alors $\mathrm{H} \cap \Gamma$ est un sous-groupe distingué de Γ et $\pi(\Gamma)$ est isomorphe à ${}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.
- ◇ Les formules $\Gamma \mapsto \pi(\Gamma)$ et $\Delta \mapsto \pi^{-1}(\Delta)$ établissent une bijection croissante (pour l'inclusion) entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Démonstration du Lemme.

Puisque $\mathrm{H} = \ker \pi$, le noyau de $\pi_{|\Gamma}$ est égal à $\mathrm{H} \cap \Gamma$. Ce dernier est donc distingué dans Γ et $\pi(\Gamma) \simeq {}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.

Montrons maintenant la seconde assertion. Soit Γ un sous-groupe de G contenant H. Montrons que $\pi^{-1}(\pi(\Gamma)) = \Gamma$. Nous avons l'inclusion $\Gamma \subset \pi^{-1}(\pi(\Gamma))$. Réciproquement soit $g \in \mathrm{G}$ tel que $\pi(g) \in \pi(\Gamma)$. Il existe alors $\gamma \in \Gamma$ tel que $\pi(g) = \pi(\gamma)$, c'est-à-dire tel que $\pi(g\gamma^{-1}) = e$. Ainsi $g\gamma^{-1}$ appartient à $\ker \pi = \mathrm{H} \subset \Gamma$. Puisque $g = (g\gamma^{-1})\gamma$ nous avons $g \in \Gamma$.

La surjectivité de π implique par ailleurs que $\pi(\pi^{-1}(\Delta)) = \Delta$ pour toute partie Δ de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$; c'est en particulier le cas lorsque Δ est un sous-groupe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Ainsi les formules données établissent bien une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Par ailleurs elles définissent des applications croissantes. □

Soit G un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et soit Γ son image réciproque dans $\mathbb{Z}$. On peut écrire $\Gamma = a\mathbb{Z}$ pour un unique $a \in \mathbb{N}$. Le groupe G étant égal à l'image de Γ, il vient $G = \langle \overline{a} \rangle$ (Lemme).

Soit $a \in \mathbb{Z}$. Soit $r \in \mathbb{N}$ le pgcd de a et n. L'image réciproque de $\langle \overline{a} \rangle$ dans $\mathbb{Z}$ est égale à $a\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$. Le Lemme assure que le groupe $\langle \overline{a} \rangle$ coïncide avec l'image de $r\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $\langle \overline{r} \rangle$. Le quotient $\mathbb{Z}/n\mathbb{Z}/\langle \overline{a} \rangle$ s'identifie canoniquement à $\mathbb{Z}/r\mathbb{Z}$.

L'intérêt de cette remarque est le suivant. Comme r divise n, l'ordre de $\overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$ est très facile à calculer. En effet si m est un entier, nous avons les équivalences suivantes

$$m\overline{r} = \overline{0} \iff n \text{ divise } mr \iff \frac{n}{r} \text{ divise } m.$$

L'ordre de $\overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$ est donc égal à $\frac{n}{r}$.

Description des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: il résulte de ce qui précède que pour tout diviseur d de n il existe un et un seul sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Il est cyclique, engendré par $\overline{\frac{n}{d}}$. Le quotient correspondant de $\mathbb{Z}/n\mathbb{Z}$ s'identifie canoniquement à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$.

3. Déterminons les quotients de G. Le quotient du groupe cyclique G par son sous-groupe d'ordre d où d est un diviseur donné de n est cyclique et donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$ où $q = \frac{n}{d}$.

Deuxième méthode :

1. Déterminons l'ordre de G et de ses éléments.

   Le groupe G est d'ordre n : ses éléments sont $\overline{1}$, $\overline{2}$, …, $\overline{n} = \overline{0}$.

   Si $1 \leq k \leq n$, alors $\overline{k}$ est d'ordre $\frac{n}{d}$ où $d = \text{pgcd}(n, k)$. En effet si $m \in \mathbb{Z}$ vérifie $m\overline{k} = \overline{0}$, alors n divise mk et donc $\frac{n}{d}$ divise $m\frac{k}{d}$ et comme les entiers $\frac{n}{d}$ et $\frac{k}{d}$ sont premiers entre eux c'est que, par Gauss, $\frac{n}{d}$ divise m de sorte que m appartient à $\frac{n}{d}\mathbb{Z}$ ce qui permet de conclure puisque $\frac{n}{d}k = n\frac{k}{d} \in n\mathbb{Z}$.

2. Déterminons les sous-groupes de G. Soit $\overline{\mathrm{H}}$ un sous-groupe de G. Alors $\mathrm{H} = \{k \in \mathbb{Z} \,|\, \overline{k} \in \overline{\mathrm{H}}\}$ est un sous-groupe de $\mathbb{Z}$ (c'est l'image réciproque de $\overline{\mathrm{H}}$ par la projection canonique $\pi : \mathbb{Z} \to \mathrm{G}$, $x \mapsto \overline{x}$). Par suite il existe $d \in \mathbb{N}$ tel que $\mathrm{H} = d\mathbb{Z}$ et comme H contient $n\mathbb{Z}$, d divise n. Par définition $\overline{\mathrm{H}} = \{\overline{k} \,|\, k \in \mathrm{H}\}$ donc $\overline{\mathrm{G}} = d\mathbb{Z}/n\mathbb{Z}$ et $\overline{\mathrm{H}}$ est le sous-groupe cyclique engendré par $\overline{d}$. De plus, puisque $\text{pgcd}(n, d) = d$, l'ordre de $\overline{\mathrm{H}}$ est $\frac{n}{d}$. Ce qui précède montre qu'il existe un unique sous-groupe d'ordre un diviseur donné δ de n : il s'agit du groupe cyclique engendré par $\overline{q}$ où $q = \frac{n}{\delta}$.

3. Déterminons les quotients de G. Le quotient du groupe cyclique G par son sous-groupe d'ordre d où d est un diviseur donné de n est cyclique et donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$ où $q = \frac{n}{d}$.

Exercice 386

Déterminer l'ordre des éléments de $\mathfrak{S}_3$, les classes de conjugaison et les centralisateurs des éléments de $\mathfrak{S}_3$. Déterminer les sous-groupes de $\mathfrak{S}_3$, les sous-groupes distingués et les groupes-quotients correspondants, les classes de conjugaison et les normalisateurs des sous-groupes de $\mathfrak{S}_3$. Déterminer le centre de $\mathfrak{S}_3$ et le groupe dérivé de $\mathfrak{S}_3$.

Éléments de réponse 386

Commençons par :

Rappel : si G est un groupe, la classe de conjugaison de l'élément $g \in \mathrm{G}$ est

$$\{hgh^{-1} \,|\, h \in \mathrm{G}\}$$

et le centralisateur de l'élément $g \in \mathrm{G}$ est

$$Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}.$$

Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n. De plus nous avons $|\text{classe de conjugaison de } g| = \frac{|\mathrm{G}|}{|\text{centralisateur de } g|}$.

Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est

$$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$

Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Clairement id est d'ordre 1, la classe de conjugaison de id est

$$\{g\mathrm{id}g^{-1} \,|\, g \in \mathfrak{S}_3\} = \mathrm{id}$$

et le centralisateur de id est

$$\{g \in \mathfrak{S}_3 \,|\, g\mathrm{id} = \mathrm{id}g\} = \{g \in \mathfrak{S}_3 \,|\, g = g\} = \mathfrak{S}_3.$$

Traitons un autre exemple : (1 2 3) est d'ordre 3 :

$$(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2), \qquad (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)(1\ 2\ 3) = \mathrm{id}$$

La classe de conjugaison de (1 2 3) est $\{(1\ 2\ 3), (1\ 3\ 2)\}$; en effet d'une part tout élément de la classe de conjugaison de (1 2 3) est d'ordre 3 et d'autre part $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$. Le centralisateur de (1 2 3) est d'ordre

$$\frac{|\mathfrak{S}_3|}{|\text{classe de conjugaison de } (1\ 2\ 3)|} = \frac{6}{2} = 3$$

et contient $\langle(1\ 2\ 3)\rangle$; par suite le centralisateur de (1 2 3) est $\langle(1\ 2\ 3)\rangle$.

Nous avons les tableaux suivants :

élément	ordre	classe de conjugaison	centralisateur
id	1	$\{\mathrm{id}\}$	$\mathfrak{S}_3$
(1 2)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(1\ 2)\rangle$
(1 3)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(1\ 3)\rangle$
(2 3)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(2\ 3)\rangle$
(1 2 3)	3	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\langle(1\ 2\ 3)\rangle$
(1 3 2)	3	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\langle(1\ 3\ 2)\rangle$

sous-groupe	ordre	quotient	classe de conjugaison	normalisateur
$\langle\mathrm{id}\rangle$	1	$\mathfrak{S}_3$	$\langle\mathrm{id}\rangle$	$\mathfrak{S}_3$
$\langle(1\ 2)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(1\ 2)\rangle$
$\langle(1\ 3)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(1\ 3)\rangle$
$\langle(2\ 3)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(2\ 3)\rangle$
$\mathcal{A}_3 = \langle(1\ 2\ 3)\rangle$	3	$\mathbb{Z}/2\mathbb{Z}$	$\mathcal{A}_3$	$\mathfrak{S}_3$
$\mathfrak{S}_3$	6	$\{1\}$	$\mathfrak{S}_3$	$\mathfrak{S}_3$

dont on déduit : $Z(\mathfrak{S}_3) = \{\mathrm{id}\}$; en effet

$$Z(\mathfrak{S}_3) = \bigcap_{\sigma\in\mathfrak{S}_3} Z_\sigma = \mathfrak{S}_3 \cap \langle(1\ 2)\rangle \cap \langle(1\ 3)\rangle \cap \langle(2\ 3)\rangle \cap \langle(1\ 2\ 3)\rangle \cap \langle(1\ 3\ 2)\rangle$$

Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
Remarque : $D(\mathrm{G})$ est un sous-groupe distingué de G.
Remarque : $\mathrm{G}/D(\mathrm{G})$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que $\mathrm{G}/D(\mathrm{G})$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

D'après le second tableau, les quotients de $\mathfrak{S}_3$ sont $\{\mathrm{id}\}$, $\mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3$. Le groupe $\mathfrak{S}_3$ n'étant pas abélien le plus grand quotient abélien de $\mathfrak{S}_3$ est $\mathbb{Z}/2\mathbb{Z}$ et $D(\mathfrak{S}_3) = \mathcal{A}_3$.

Exercice 387

Soit $\mathbb{H}_8$ le groupe des quaternions, *i.e.* $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ la multiplication étant définie par la règle des signes et les formules

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

1. Déterminer l'ordre des éléments de $\mathbb{H}_8$.
2. Déterminer les classes de conjugaison des éléments de $\mathbb{H}_8$.
3. Déterminer les centralisateurs des éléments de $\mathbb{H}_8$.
4. Déterminer les sous-groupes de $\mathbb{H}_8$.
5. Déterminer les sous-groupes distingués et les groupes-quotients correspondants, les classes de conjugaisons et les normalisateurs des sous-groupes de $\mathbb{H}_8$ en reconnaissant d'éventuels isomorphismes avec des groupes connus.
6. Déterminer le groupe dérivé de $\mathbb{H}_8$.
7. Déterminer le centre $Z(\mathbb{H}_8)$.

Éléments de réponse 387

1. Nous avons :
   - ◇ -1 est d'ordre 2.
   - ◇ si $x \in \{\pm i, \pm j, \pm k\}$, alors x est d'ordre 4.
2. Déterminons les classes de conjugaison des éléments de $\mathbb{H}_8$.

Rappel : si G est un groupe, la classe de conjugaison de l'élément $g \in \mathrm{G}$ est $$\{hgh^{-1} \,|\, h \in \mathrm{G}\}$$ Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n.

   Comme 1 est l'unique élément d'ordre 1 de $\mathbb{H}_8$, la classe de conjugaison de 1 est $\{1\}$.

   Comme -1 est l'unique élément d'ordre 2 de $\mathbb{H}_8$, la classe de conjugaison de -1 est $\{-1\}$.

   Si $x \in \{\pm i, \pm j, \pm k\}$ et $y \in \{\pm i, \pm j, \pm k\}$ tel que $y \notin \{x, -x\}$, alors $xy = -yx$, *i.e.* $yxy^{-1} = -x$. De plus, si x appartient à $\{\pm i, \pm j, \pm k\}$ et $y = \pm 1$, alors $yxy^{-1} = x$. Nous en déduisons que les conjugués de x dans $\mathbb{H}_8$ sont x et $-x$.
3. Déterminons les centralisateurs des éléments de $\mathbb{H}_8$.

Rappel : si G est un groupe, le centralisateur de l'élément $g \in \mathrm{G}$ est $$Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}.$$ De plus nous avons $\lvert\text{classe de conjugaison de } g\rvert = \frac{\lvert\mathrm{G}\rvert}{\lvert\text{centralisateur de } g\rvert}$.

   Nous avons :
   - ◇ $Z_1 = \mathbb{H}_8$.
   - ◇ $Z_{-1} = \mathbb{H}_8$.

◇ soit $x \in \{\pm i, \pm j, \pm k\}$. D'une part la classe de conjugaison de x dans $\mathbb{H}_8$ est de cardinal 2 d'où $|Z_x| = \frac{|\mathbb{H}_8|}{2} = 4$; d'autre part $\langle x\rangle \subset Z_x$ et $|\langle x\rangle| = 4$. Ainsi $Z_x = \langle x\rangle$.

4. Le groupe $\mathbb{H}_8$ n'admettant qu'un seul élément d'ordre 2 aucun sous-groupe d'ordre 4 n'est isomorphe au groupe de Klein. Par suite les sous-groupes propres de $\mathbb{H}_8$ sont cycliques.

5. Commençons par :

> Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est
> $$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$
> Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Chaque sous-groupe propre de $\mathbb{H}_8$ étant réunion de classes de conjugaison ces sous-groupes sont tous distingués ; on en déduit que si H est un sous-groupe de $\mathbb{H}_8$, alors

◇ sa classe de conjugaison est $\{\mathrm{H}\}$;

◇ son normalisateur est $\mathbb{H}_8$.

Intéressons-nous maintenant aux groupes quotients de $\mathbb{H}_8$.

◇ Si $\mathrm{H} = \{\mathrm{id}\}$, alors $\mathbb{H}_8/\mathrm{H} = \mathbb{H}_8$.

◇ Si $\mathrm{H} = \mathbb{H}_8$, alors $\mathbb{H}_8/\mathrm{H} = \{\mathrm{id}\}$.

◇ Si $\mathrm{H} = \langle x\rangle$ avec $x \in \{\pm i, \pm j, \pm k\}$, alors $\mathbb{H}_8/\mathrm{H}$ est d'ordre $\left|\mathbb{H}_8/\mathrm{H}\right| = \frac{|\mathbb{H}_8|}{|\mathrm{H}|} = \frac{8}{4} = 2$; par suite $\mathbb{H}_8/\mathrm{H}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

◇ Si $\mathrm{H} = \{-1, 1\}$, alors $\mathbb{H}_8/\mathrm{H}$ est d'ordre $\left|\mathbb{H}_8/\mathrm{H}\right| = \frac{|\mathbb{H}_8|}{|\mathrm{H}|} = \frac{8}{2} = 4$. Par suite ou bien $\mathbb{H}_8/\mathrm{H}$ est isomorphe à $\mathbb{Z}/4\mathrm{Z}$, ou bien $\mathbb{H}_8/\mathrm{H}$ est isomorphe au groupe de Klein $\mathbb{Z}/2\mathrm{Z} \times \mathbb{Z}/2\mathbb{Z}$. Remarquons que si g appartient à $\mathbb{H}_8$, alors g^2 appartient à H. Soit $g\mathrm{H}$ un élément de $\mathbb{H}_8/\mathrm{H}$, alors $g\mathrm{H} \cdot g\mathrm{H} = g^2\mathrm{H}$; mais g^2 appartenant à H nous avons $g^2\mathrm{H} = \mathrm{H}$ et $g\mathrm{H} \cdot g\mathrm{H} = \underbrace{\mathrm{H}}_{\text{neutre de } \left(\mathbb{H}_8/\mathrm{H}, \cdot\right)}$. En particulier, $g\mathrm{H}$ est d'ordre ≤ 2. Il s'en suit que $\mathbb{H}_8/\{-1, 1\}$ est isomorphe au groupe de Klein.

6. Déterminons le groupe dérivé de $\mathbb{H}_8$.

Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
Remarque : $D(\mathrm{G})$ est un sous-groupe distingué de G.
Remarque : ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

Puisque ${}^{\mathbb{H}_8}\!/_{\{-1,\,1\}}$ est isomorphe au groupe de Klein, $D(\mathbb{H}_8) \subseteq \{-1, 1\}$. Comme de plus $\mathbb{H}_8$ n'est pas abélien, $D(\mathbb{H}_8) \neq \{1\}$ et $D(\mathbb{H}_8) = \{-1, 1\}$.

7. Le centre de $\mathbb{H}_8$ est

$$\bigcap_{g\in\mathbb{H}_8} Z_g = \mathbb{H}_8 \cap \mathbb{H}_8 \cap \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle \cap \langle -i\rangle \cap \langle -j\rangle \cap \langle -k\rangle = \mathbb{H}_8 \cap \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle = \{1, -1\}.$$

Exercice 388

Soit G' un sous-groupe d'ordre $p(p-1)$ de $\mathfrak{S}_p$.
Montrer que G' est le normalisateur d'un p-Sylow de $\mathfrak{S}_p$.
En déduire que K est conjugué de tous les sous-groupes d'ordre $p(p-1)$ de $\mathfrak{S}_p$.

Éléments de réponse 388 Rappelons que dans un groupe G le normalisateur d'une partie X est l'ensemble, noté $N_{\mathrm{G}}(X)$, des éléments g de G qui normalisent X, *i.e.* qui vérifient $gXg^{-1} = X$:

$$N_{\mathrm{G}}(X) = \{g \in \mathrm{G} \,|\, gXg^{-1} = X\} = \{g \in \mathrm{G} \,|\, gX = Xg\}$$

$N_{\mathrm{G}}(\mathrm{H})$ est le plus grand sous-groupe de G dans lequel H est distingué ; en particulier $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{G}$ si et seulement si $\mathrm{H} \lhd \mathrm{G}$.

Exercice 389

Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.

(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{e\}$.
(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ soit cyclique. Montrer qu'alors G est abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Éléments de réponse 389

Faisons agir G par conjugaison sur lui-même :

$$\begin{aligned} \mathrm{G}\times\mathrm{G} &\to \mathrm{G}\\ (g,h) &\mapsto g\cdot h = ghg^{-1}\end{aligned}$$

(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

Le centre de G est par définition l'ensemble

$$\begin{aligned} Z(\mathrm{G}) &= \{x\in\mathrm{G}\,|\,gx=xg \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,gxg^{-1}=x \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,g\cdot x=x \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,\mathcal{O}_x=\{x\}\}\end{aligned}$$

(rappelons que $\mathcal{O}_x=\{g\cdot x\,|\,g\in\mathrm{G}\}=\{gxg^{-1}\,|\,g\in\mathrm{G}\}$).

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{e\}$. Notons Ω_i, $i\in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|\mathrm{G}|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv_p |Z(\mathrm{G})|.$$

Puisque $|Z(\mathrm{G})|\geq 1$ (en effet $Z(\mathrm{G})$ contient 1) l'égalité $0\equiv_p |Z(\mathrm{G})|$ entraîne $|Z(\mathrm{G})|\geq p$. En particulier $Z(\mathrm{G})\neq\{1\}$.

(ii) Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons qu'alors G est abélien.

Par hypothèse il existe un élément a de G dont la classe $\overline{a}\in \mathrm{G}/Z(\mathrm{G})$ engendre $\mathrm{G}/Z(\mathrm{G})$. Tout élément de G peut alors s'écrire a^kh avec $k\in\mathbb{Z}$ et $h\in Z(\mathrm{G})$.

Soient g et g' dans G ; alors $g=a^kh$ et $g'=a^{k'}h'$ avec k, k' dans $\mathbb{Z}$ et h, h' dans $Z(\mathrm{G})$; ainsi

$$gg' = a^kha^{k'}h' \overset{h\in Z(\mathrm{G})}{=} a^ka^{k'}hh' = a^{k+k'}hh' \overset{h'\in Z(\mathrm{G})}{=} a^{k+k'}h'h = a^{k'+k}h'h = a^{k'}a^kh'h \overset{h\in Z(\mathrm{G})}{=} a^{k'}h'a^kh = g'g$$

Le groupe G est donc abélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G}=\left\{\begin{pmatrix}1&a_1&a_2\\0&1&a_3\\0&0&1\end{pmatrix}\,\middle|\, a_i\in\mathrm{GL}(3,\mathbb{F}_p)\right\}$$

est un groupe non-abélien d'ordre p^3.

Chacun des coefficients a_i est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 390

Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset \mathrm{G}$ un p-Sylow de G et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $gSg^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Éléments de réponse 390

Nous avons $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. Faisons agir G (et donc également H) par translation sur l'ensemble ${}^{\mathrm{G}}\!/_{S}$ des classes à gauche de G modulo S

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{S} \to {}^{\mathrm{G}}\!/_{S}, \qquad (g, aS) \mapsto g \cdot (aS) = (ga)S$$

Notons que $g' \in \mathrm{St}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble ${}^{\mathrm{G}}\!/_{S}$ est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de ${}^{\mathrm{G}}\!/_{S}$ sous l'action de H est donc de cardinal p^c pour un certain $c \leq b$. Mais comme de plus $|\mathrm{St}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{St}(x)| = p^b$ comme attendu.

Exercice 391

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}(n, \Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 391

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathfrak{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathfrak{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathfrak{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 392

Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-Sylow.

b) Montrer que G contient dix 3-Sylow. Montrer que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-Sylow).

c) Conclure.

Éléments de réponse 392

a) Montrons que G contient trente six 5-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-Sylow serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $\mathrm{G} \to \mathfrak{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Le morphisme $\mathrm{G} \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ donné par la signature a nécessairement un noyau trivial donc G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathfrak{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|\mathrm{G}| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-Sylow serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathfrak{S}_4$ ce qui est impossible car $180 = |\mathrm{G}| > |\mathfrak{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e$.

Soient S et T deux 3-Sylow de G distincts. Soit $g \in S \cap T$. Notons $Z = \{x \in \mathrm{G} \mid xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|Z| \in \{18, 36, 45, 90\}$. L'action transitive de G sur ${}^{\mathrm{G}}\!/_{Z}$ induit un morphisme injectif de G vers $\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}$. Or $|\mathrm{G}| = 180$ et $\left|\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}\right| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $\left|\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}\right| = 10!$ et $|Z| = 18$. Ainsi S et T sont des 3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow d'où $S = T$: contradiction. Finalement $S \cap T = \{e\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.

D'après b) le groupe G contient dix 3-Sylow dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_{G} d'ordre divisant 9.

Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.

Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 393

Expliciter les sous-groupes de Sylow des groupes alternés $\mathcal{A}_4$.

Éléments de réponse 393

Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

Les théorèmes de Sylow assurent que

— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;

— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Exercice 394

Expliciter les sous-groupes de Sylow du groupe alterné $\mathcal{A}_5$.

Éléments de réponse 394

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. S'il y en a quatre l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathfrak{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathfrak{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient pas d'élément d'ordre 4. En effet, les éléments d'ordre 4 du groupe symétrique $\mathfrak{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1, 2, 3, 4, 5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

Exercice 395

Expliciter les sous-groupes de Sylow des groupes diédraux D_8 et D_{10}.

Éléments de réponse 395

i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $\frac{2\pi}{5}$ dont le centre est le centre du pentagone.

Exercice 396

a) Quel est l'ordre d'un p-Sylow de $\mathfrak{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathfrak{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Éléments de réponse 396

a) L'ordre de $\mathfrak{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathfrak{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathfrak{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathfrak{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathfrak{S}_p$ car $\mathfrak{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathfrak{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathfrak{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 397

On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p. Notons n_p le nombre de p-Sylow de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Éléments de réponse 397

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.

Les 60 éléments de $\mathcal{A}_5$ sont les suivants :

- l'identité d'ordre 1 qui forme une classe de conjugaison ;

- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;
- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de (1 2 3 4 5) et (2 1 3 4 5).

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $\mathrm{H} \neq \{e\}$ un sous-groupe distingué de $\mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans $\mathcal{A}_5$. Comme aucun des entiers $1 + 15 = 16$, $1 + 12 = 13$, $1 + 24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 20 + 15 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison de $\mathcal{A}_5$, donc $\mathrm{H} = \mathcal{A}_5$.

c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-Sylow. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $\mathrm{G} \to \mathfrak{S}_{\mathrm{Syl}_p} \simeq \mathfrak{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|\mathrm{G}|$ divise $|\mathfrak{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-Sylow de G est égal à 5 ou à 15.

Soit n_2 le nombre de 2-Sylow. Les théorèmes de Sylow assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|\mathrm{G}|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

e) Montrons que G contient un sous-groupe d'ordre 12.

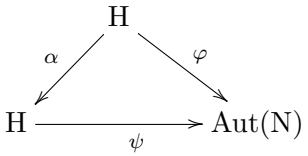
Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.

Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et T tels que $|\mathrm{S} \cap \mathrm{T}| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de Sylow assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46 + 24 = 70$ éléments et d'autre par $|\mathrm{G}| = 60$: contradiction. On dispose donc de deux 2-Sylow distincts S et T tels que $\mathrm{S} \cap \mathrm{T} = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6. Ainsi $|\mathrm{H}|$ appartient à $\{12, 20, 60\}$. Si $|\mathrm{H}| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $\mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathfrak{S}_3$: contradiction. Si $|\mathrm{H}| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(\mathrm{G})$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|\mathrm{H}| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathfrak{S}_5$. Ainsi G est isomorphe à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$ qui est nécessairement $\mathcal{A}_5$.

Exercice 398

Rappelons l'énoncé suivant dont nous aurons besoin : Soient H et N deux groupes. Soient φ et ψ deux opérations de H sur N et α un automorphisme de H tels que le diagramme suivant commute



i.e. $\varphi = \psi \circ \alpha$.

L'application $(n, h) \mapsto (n, \alpha(h))$ est un isomorphisme de $\mathrm{N} \rtimes_\psi \mathrm{H}$ sur $\mathrm{N} \rtimes_\varphi \mathrm{H}$.

Soient p et q des nombres premiers avec $p < q$. Montrer que

1. Si p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.
2. Si p divise $q-1$, alors il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.

Indication : $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ ([Perrin, Cours d'algèbre, p. 24])

Éléments de réponse 398

Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Calculons ces produits. On a $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

On a l'alternative suivante :

- p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique.

- p divise $q-1$, $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. L'énoncé rappelé assure que les produits correspondants sont isomorphes.

Exercice 399

Soit $n \geq 1$. On note $\mathrm{Int}(\mathfrak{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathfrak{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition.

Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathfrak{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\}$$

de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}^n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$ montrer qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Soit q une puissance D'un nombre premier et $n \geq 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}(n, \mathbb{F}_q) \to \mathfrak{S}_N$ avec $N = \frac{q^n-1}{q-1}$.

g) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

h) En déduire que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Éléments de réponse 399

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition.

Montrons que ϕ est intérieur.

Puisque tout automorphisme de $\mathfrak{S}_i$ est intérieur dès que $i \leq 3$ (à vérifier) on peut supposer que $n \geq 4$.

Le groupe symétrique est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geq 2$. Comme τ_i et τ_j ne commutent pas si $i \neq j$ les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun noté α_1. Puisque $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ils ont nécessairement tous α_1 en commun. Écrivons $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. L'application φ étant injective $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, 2 \ldots, n\}$. Définissons la permutation $\alpha \in \mathfrak{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $1 \leq i \leq n$. Ainsi φ est la conjugaison par α et φ appartient à $\mathrm{Int}(\mathfrak{S}_n)$.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminons le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathfrak{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\}$$

de σ. Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, …, k_n cycles de longueur n, avec $n = \sum_i ik_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles pour tout k. Ainsi le commutant d'un n-cycle de $\mathfrak{S}_n$ est composé des puissances de ce dernier. Finalement on obtient

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Montrons que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Soit φ un automorphisme de $\mathfrak{S}_n$. Si τ est une transposition de $\mathfrak{S}_n$, alors $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. On a $|Z(\tau)| = |Z(\varphi(\tau))|$ ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Puisque $n \neq 6$ on a $k = 1$. D'après a) φ est donc intérieur.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}^n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrons que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués. Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$. L'action transitive de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/\mathrm{H}$ induit un morphisme de groupes

$$\phi\colon \mathfrak{S}_n \to \mathfrak{S}_{\mathfrak{S}_n/\mathrm{H}} \simeq \mathfrak{S}_n.$$

Puisque $\ker\phi$ est un sous-groupe distingué de $\mathfrak{S}_n$, $\ker\phi \in \{\{\mathrm{id}\}, \mathcal{A}_n, \mathfrak{S}_n\}$. Le groupe $\ker\phi$ agit trivialement sur la classe de H dans $\mathfrak{S}_n/\mathrm{H}$, d'où $\ker\phi \subset \mathrm{H}$. Il en résulte que $\ker\phi = \{\mathrm{id}\}$, *i.e.* que ϕ est injective. Ainsi φ appartient à $\mathrm{Aut}(\mathfrak{S}_n)$. Par hypothèse il existe une permutation σ telle que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathfrak{S}_{\mathfrak{S}_n/\mathrm{H}} \simeq \mathfrak{S}_n$. Enfin dans $\mathfrak{S}_n$ les stabilisateurs d'un point de $\{1, 2, \ldots, n\}$ sont tous conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$ montrons qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Les théorèmes de Sylow assurent que $\mathfrak{S}_5$ admet un ou six 5-Sylow. Comme $\mathcal{A}_5$ est simple $\mathfrak{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5 et $\mathfrak{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathfrak{S}_5$. L'action de $\mathfrak{S}_5$ sur X par conjugaison est transitive et induit un morphisme de groupes

$$\mu\colon \mathfrak{S}_5 \to \mathfrak{S}_X \simeq \mathfrak{S}_6$$

dont le noyau est trivial (les sous-groupes distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathfrak{S}_5$). Le groupe $\mathrm{H} = \mu(\mathfrak{S}_5) \subset \mathfrak{S}_6$ est un sous-groupe d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Preuve géométrique, par récurrence sur n : l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $\Bbbk$ (disons $\Bbbk^n$) et d'un hyperplan projectif de

dimension $n-2$, *i.e.* isomorphe à un $\mathbb{P}^{n-2}(\Bbbk)$, appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(\Bbbk) = \Bbbk^{-1} \sqcup \mathbb{P}^{n-2}(\Bbbk)$. On en déduit par récurrence la formule suivante

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \ldots + q + 1.$$

Autre preuve : le groupe $\mathrm{PGL}(\mathbb{F}_q^n)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_q^n)$ d'où le morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = \mathbb{F}_q^n \smallsetminus \{0\}\big/\mathbb{F}_q^*$ donc $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1}$. Par conséquent il existe un morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

g) Construisons géométriquement un sous-groupe H' d'indice 6 dans $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

Le groupe $\mathrm{H}' = \mathrm{PGL}(2, \mathbb{F}_5)$ vu comme sous-groupe de $\mathfrak{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ n'est pas conjugué à $\mathfrak{S}_5 = \mathrm{St}(6) \subset \mathfrak{S}_6$ puisqu'il ne fixe aucun point.

h) Montrons que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Les d), e) et g) assurent que le groupe $\mathfrak{S}_6$ possède au moins un automorphisme extérieur.

Exercice 400 [Simplicité de $\mathcal{A}_n$, $g \geq 5$, version 2]

a) Montrer que le groupe $\mathcal{A}_5$ est simple.

b) Soit $n \geq 3$. Montrer que les 3-cycles engendrent $\mathcal{A}_n$.

c) Montrer que $\mathcal{A}_n$ est simple dès que $n \geq 5$.

d) Montrer que $\mathcal{A}_4$ n'est pas simple.

e) Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

f) Soit $n \geq 3$. Montrer que le centre de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$.

g) Soit $n \geq 5$. Montrer que les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

Éléments de réponse 400

a) Le groupe $\mathcal{A}_5$ a 60 éléments :

— le neutre ;

— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;

— 20 éléments d'ordre 3 (3-cycles) ;

— 24 éléments d'ordre 5 (5-cycles).

Les 3-cycles sont conjugués dans $\mathcal{A}_5$ [13]. Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.

Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.

Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geq 15 + 20 + 1 + 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$.

b) Puisque le groupe $\mathfrak{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

c) Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geq 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

---

13. Le groupe $\mathcal{A}_5$ est 3 fois transitif sur $\{1, 2, \ldots, 5\}$, *i.e.* si a_1, a_2, a_3 sont distincts et b_1, b_2, b_3 sont distincts il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, 5\} = \{a_1, a_2, \ldots, a_5\} = \{b_1, b_2, \ldots, b_5\}$$

et considérons $\sigma \in \mathfrak{S}_5$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, 5$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_4\ a_5)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_5$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;

— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E\smallsetminus F} = \mathrm{id}_{|E\smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors

— $\mathrm{H}_0 \lhd \mathcal{A}(F)$;

— $\rho_{|F} \in \mathrm{H}_0$;

— $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ [14] ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (cf b)) on a $\mathrm{H} = \mathcal{A}_n$.

d) Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

e) Calcul direct.

f) Soit σ un élément du centre de $\mathfrak{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite d'après e)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

---

14. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$, *i.e.* si $a_1, a_2, \ldots, a_{n-2}$ sont distincts et b_1, b_2, b_{n-2} sont distincts il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, n$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_{n-1}\ a_n)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ \ldots\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_n$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

g) Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \triangleleft \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \{\mathrm{id}, \mathcal{A}_n\}$.

Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathfrak{S}_n$.

Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leq 2$. Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathfrak{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathfrak{S}_n$ d'où $\sigma = \mathrm{id}$ (f)) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$.

Exercice 401

Soit G un groupe d'ordre 2009.

1. Montrer que $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$ où P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.
2. Classifier à isomorphisme près tous les groupes d'ordre 2009.
3. Soient P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. Montrer que $\mathrm{Aut}(\mathrm{G}) \simeq \mathrm{Aut}(\mathrm{P}) \times \mathrm{Aut}(\mathrm{Q})$.
4. Montrer que
   a) si Q est cyclique, alors Aut(Q) est cyclique aussi. Quel est l'ordre de Aut(Q) quand Q est cyclique ?
   b) si Q n'est pas cyclique, alors Aut(Q) est isomorphe à $\mathrm{GL}(2, \mathbb{F}_7)$ où $\mathbb{F}_7$ est le corps à 7 éléments. Quel est l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$?

Éléments de réponse 401

1. Notons que $|\mathrm{G}| = 2009 = 7^2 \times 41$. D'après le premier théorème de Sylow le groupe G possède un 41-Sylow P d'ordre 41 et un 7-Sylow Q d'ordre 49. Notons n_p le nombre de p-Sylow de G. D'après le troisième théorème de Sylow
   - $\diamond$ n_{41} est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
   - $\diamond$ n_7 est congru à 1 modulo 7 et divise 41 donc est égal à 1.

   Nous en déduisons que $\mathrm{P} \triangleleft \mathrm{G}$ et $\mathrm{Q} \triangleleft \mathrm{G}$.

   Nous constatons aussi que $\mathrm{P} \cap \mathrm{Q} = \{e\}$, que $\mathrm{G} = \mathrm{PQ}$ et que les deux sous-groupes dans le produit sont distingués dans G. Tout ceci revient à dire $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$.

   Reste à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs les éléments de P commutent avec ceux de Q. Ainsi G est abélien.
2. D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

soit encore

$$\mathbb{Z}/2009\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$

3. **Remarque**. Si φ est un automorphisme de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$ et $\varphi(\mathrm{Q}) = \mathrm{Q}$. En effet comme dans tout groupe et pour tout p premier l'image par un morphisme d'un p-élément est un p-élément et que P et Q sont les seuls 41-Sylow et 7-Sylow de G respectivement, $\varphi(\mathrm{P}) \subset \mathrm{P}$ et $\varphi(\mathrm{Q}) \subset \mathrm{Q}$. Comme φ est une bijection ces deux inclusions sont en fait des égalités.

   Il découle de la Remarque précédente que la restriction de tout automorphisme $\varphi \in \mathrm{Aut(G)}$ au sous-groupe P (respectivement Q) est un automorphisme qu'on appellera φ_P (respectivement φ_Q) de P (respectivement Q). Les automorphismes de φ_P et φ_Q ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

   Considérons l'application

$$\Phi\colon \mathrm{Aut(G)} \to \mathrm{Aut(P)} \times \mathrm{Aut(Q)}, \qquad \varphi \mapsto (\varphi_\mathrm{P}, \varphi_\mathrm{Q})$$

   Remarquons que $\Phi(\mathrm{id}) = (\mathrm{id}, \mathrm{id})$. Soient φ et ϕ deux éléments de Aut(G). Alors d'une part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{P}(\mathrm{P}) &= (\varphi \circ \phi)(\mathrm{P}) \\ &= \varphi(\phi(\mathrm{P})) \\ &= \varphi_\mathrm{P}(\phi_\mathrm{P}(\mathrm{P})) \\ &= (\varphi_\mathrm{P} \circ \phi_\mathrm{P})(\mathrm{P})\end{aligned}$$

   et d'autre part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{Q}(\mathrm{Q}) &= (\varphi \circ \phi)(\mathrm{Q}) \\ &= \varphi(\phi(\mathrm{Q})) \\ &= \varphi_\mathrm{Q}(\phi_\mathrm{Q}(\mathrm{Q})) \\ &= (\varphi_\mathrm{Q} \circ \phi_\mathrm{Q})(\mathrm{Q})\end{aligned}$$

   Autrement dit Φ est un morphisme de groupes.

   Montrons maintenant que Φ est un isomorphisme.

   Commençons par montrer que Φ est injective. Un automorphisme φ de Aut(G) appartient à $\ker\Phi$ si et seulement si $\varphi_\mathrm{P} = \mathrm{id}_\mathrm{P}$ et $\varphi_\mathrm{Q} = \mathrm{id}_\mathrm{Q}$. Or tout élément de G s'écrit sous la forme xy avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_\mathrm{P}(x)\varphi_\mathrm{Q}(y) = \mathrm{id}_\mathrm{P}(x)\mathrm{id}_\mathrm{Q}(y) = xy.$$

   Montrons que Φ est surjective. Soient φ_1 dans Aut(P) et φ_2 dans Aut(Q). Considérons l'application

$$\varphi\colon \mathrm{G} \to \mathrm{G}, \qquad xy \mapsto \varphi_1(x)\varphi_2(y)$$

avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. L'application φ est définie sans ambiguïté puisque G étant la somme directe de P et de Q chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q Montrons que φ est un automorphisme de G dont l'image sous l'action de Φ est (φ_1, φ_2).

Le fait que φ_1 et φ_2 soient des morphismes de groupes entraîne que φ est un morphisme de groupes. Il en est de même pour la surjectivité de φ. Supposons que $\varphi(xy) = 1$ pour $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. La définition de φ implique que $\varphi_1(x)\varphi_2(x) = 1$. Or $\varphi_1(x)$ appartient à P, $\varphi_2(y)$ appartient à Q et $\mathrm{P} \cap \mathrm{Q} = \{e\}$ donc $\varphi_1(x) = \varphi_2(y) = 1$. Puisque φ_1 est un automorphisme de P et φ_2 un automorphisme de Q nous obtenons $x = y = 1$. Comme $\mathrm{G} = \mathrm{PQ}$ tout élément de $\ker\varphi$ s'écrit comme produit d'un $x \in \mathrm{P}$ et d'un $y \in \mathrm{Q}$. Ainsi $\ker\varphi = \{e\}$.

Finalement φ est un automorphisme de G. Il s'ensuit de la définition de φ que $\varphi_{\mathrm{P}} = \varphi_1$ et $\varphi_{\mathrm{Q}} = \varphi_2$. Par conséquent $\Phi(\varphi) = (\varphi_1, \varphi_2)$. Ainsi Φ est surjective.

4. a) Si Q est cyclique, il est isomorphe à $\left(\mathbb{Z}/49\mathbb{Z}, +\right)$. Alors $|\mathrm{Aut}(\mathrm{Q})| = \varphi(49) = 7 \times 6 = 42$ où φ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$ le théorème chinois assure que $\mathrm{Aut}(\mathrm{Q})$ est cyclique d'ordre 42.

   b) Supposons maintenant que Q soit non cyclique. Alors $\mathrm{Q} \simeq \left(\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +\right)$. Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1,0)$ et $e_2 = (0,1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \qquad \lambda e_2 = \underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}$$

   avec $\lambda \in \mathbb{F}_7$, identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.

   Soit $\varphi \in \mathrm{Aut}(\mathrm{Q})$, alors

$$\begin{aligned}
\varphi(\lambda e_1) &= \varphi(\underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(1,0) + \varphi(1,0) + \ldots + \varphi(1,0)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((1,0)) \\
&= \lambda\varphi(e_1)
\end{aligned}$$

et

$$\begin{aligned}\varphi(\lambda e_2) &= \varphi(\underbrace{(0,1)+(0,1)+\ldots+(0,1)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(0,1)+\varphi(0,1)+\ldots+\varphi(0,1)}_{\lambda \text{ fois}} \\ &= \lambda\varphi((0,1)) \\ &= \lambda\varphi(e_2)\end{aligned}$$

Ainsi φ est une application linéaire. Étant bijectif $\varphi \in \mathrm{GL}(2,\mathbb{F}_7)$. Par suite $\mathrm{Aut}(\mathrm{Q}) \subset \mathrm{GL}(2,\mathbb{F}_7)$. L'autre inclusion est claire car chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Finalement $|\mathrm{GL}(2,\mathbb{F}_7)| = (7^2-1)(7^2-7)$.

Exercice 402

1. Soit H un sous-groupe distingué de $\mathfrak{S}_4$ qui contient un 4-cycle. Montrer que $\mathrm{H} = \mathfrak{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathfrak{S}_4$. Supposons que $\mathrm{P}_1 \cap \mathrm{P}_2$ contienne un 4-cycle. Montrer que $\mathrm{P}_1 = \mathrm{P}_2$ (indication : on montre que le normalisateur de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathfrak{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$, on considère le sous-groupe engendré par $\mathrm{P}_1 \cup \mathrm{P}_2$ et on utilise 1.)
3. D'après ce qui précède un 4-cycle est dans un unique sous-groupe d'ordre 8 de $\mathfrak{S}_4$. En déduire le nombre de sous-groupes d'ordre 8 de $\mathfrak{S}_4$ en comptant le nombre de 4-cycles.

Éléments de réponse 402

1. Les sous-groupes distingués de $\mathfrak{S}_4$ sont id, $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\mathcal{A}_4$ et $\mathfrak{S}_4$. Le seul de ces sous-groupes qui contient un 4-cycle est $\mathfrak{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathfrak{S}_4$. Si $\mathrm{P}_1 \neq \mathrm{P}_2$, alors $\mathrm{P}_1 \cap \mathrm{P}_2$ contient un 4-cycle et est donc d'ordre 4. Par conséquent $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_1 donc distingué dans P_1. De même $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_2 donc distingué dans P_2. Par suite le normalisateur N de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathfrak{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$. Ainsi N est un sous-groupe de $\mathrm{P}_1 \cap \mathrm{P}_2$ d'ordre un diviseur de 24 qui est un multiple de 8 et > 8. Il en résulte que $|\mathrm{N}| = 24$ et donc que $\mathrm{N} = \mathfrak{S}_4$. Ainsi $\mathrm{P}_1 \cap \mathrm{P}_2 \triangleleft \mathfrak{S}_4$ et $\mathrm{P}_1 \cap \mathrm{P}_2 = \mathfrak{S}_4$: absurde.
3. Déterminons le nombre de 4-cycles de $\mathfrak{S}_4$. Un 4-cycle s'écrit de manière unique $(1\ i\ j\ k)$ où i, j et k sont trois entiers distincts parmi $\{2, 3, 4\}$. Il y a donc $3 \times 2 \times 1 =$ six 4-cycles dans $\mathfrak{S}_4$. Soit n_2 le nombre de sous-groupes d'ordre 8. Ils sont tous isomorphes car ce sont les 2-Sylow qui sont tous conjugués. Soit k le nombre de 4-cycles dans un 2-Sylow. Nous avons donc $n_2 k = 6$ car un 4-cycle engendre un 2-groupe forcément contenu dans un 2-Sylow. De plus $k \geq 2$ car si c est un 4-cycle dans un sous-groupe P d'ordre 8, alors c^{-1} appartient à P. Si n_2 vaut 1 l'unique 2-Sylow contient un 4-cycle et est distingué dans $\mathfrak{S}_4$ donc est $\mathfrak{S}_4$: contradiction. Par suite $n_2 = 3$ et $k = 2$.

Exercice 403

Soit $n \geq 5$.

a) Montrer qu'un sous-groupe H d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

b) En utilisant les théorèmes de Sylow sur les 5-Sylow de $\mathfrak{S}_5$ construire un sous-groupe de $\mathfrak{S}_6$ d'indice 6 qui n'est pas de la forme

$$\mathfrak{S}_6(i) = \{\sigma \in \mathfrak{S}_6 \,|\, \sigma(i) = i\}$$

avec $1 \leq i \leq 6$.

Éléments de réponse 403

a) Faire agir $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ par translation. Comme nous connaissons les sous-groupes distingués de $\mathfrak{S}_n$ nous obtenons que le morphisme

$$\varphi\colon \mathrm{H} \to \mathrm{Bij}\Big({}^{\mathfrak{S}_n}\!/_{\mathrm{H}}\Big)$$

est injectif. De plus les éléments de $\varphi(\mathrm{H})$ fixent la classe H d'où le résultat.

b) Le troisième théorème de Sylow assure que $\mathfrak{S}_5$ compte six 5-Sylow. Faisons agir $\mathfrak{S}_5$ par conjugaison sur l'ensemble X des 5-Sylow. On obtient un morphisme de groupes

$$\varphi\colon \mathfrak{S}_5 \to \mathrm{Bij}(X).$$

Le premier théorème de Sylow assure que cette action est transitive. Puisque nous connaissons les sous-groupes distingués de $\mathfrak{S}_n$ nous obtenons que φ est injective. Finalement l'image de φ répond à la question.

Exercice 404

1. Soit G un groupe fini. Notons $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-sous-groupes de Sylow de G. Supposons que $|\mathrm{Syl}_p(\mathrm{G})| = m$. Montrons qu'il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathfrak{S}_m$.
2. Soit G un groupe de cardinal 36. Montrer qu'il n'est pas simple.

Éléments de réponse 404

1. D'après les théorèmes de Sylow l'action par conjugaison

$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}) \qquad\qquad (g, P) \mapsto gPg^{-1}$$

est transitive et détermine donc un morphisme non trivial $\rho\colon \mathrm{G} \to \mathrm{Bij}(\mathrm{Syl}_p(\mathrm{G})) \simeq \mathfrak{S}_m$.

2. Remarquons que $|\mathrm{G}| = 2^2 \times 3^2$. Soit n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise $2^2 = 4$ et que $n_3 \equiv 1 \bmod 3$, autrement dit que n_3 appartient à $\{1, 4\}$.

Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est forcément distingué dans G ; en particulier G n'est pas simple.

Si $n_3 = 4$, alors d'après 1. il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathfrak{S}_4$. Puisque $|\mathrm{G}| = 36$ ne divise pas $|\mathfrak{S}_4| = 24$ ce morphisme n'est pas injectif et $\ker\rho$ est un sous-groupe distingué non trivial et propre de G.

Exercice 405

Soit G un groupe d'ordre 231.

1. Montrer que G admet un seul 7-Sylowet un seul 11-Sylow.
2. Montrer que si P est le 11-Sylow de G, alors P est contenu dans le centre de G (indication : on considère l'action d'un 3-Sylowet l'action d'un 7-Sylow de G sur P par conjugaison).
3. Montrer que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G. Est-ce que ce sous-groupe d'ordre 77 est cyclique ? Justifier.
4. Montrer que G admet un sous-groupe cyclique d'ordre 33.

Éléments de réponse 405

1. Montrons que G admet un seul 7-Sylowet un seul 11-Sylow.

   Soit n_p le nombre de p-Sylowde G.

   Le troisième théorème de Sylow assure que $n_7 \equiv 1 \bmod 7$ et que n_7 divise 33, soit que $n_7 = 1$.

   Le troisième théorème de Sylow assure que $n_{11} \equiv 1 \bmod 11$ et que n_{11} divise 21, soit que $n_{11} = 1$.

2. Montrons que si P est le 11-Sylow de G, alors P est contenu dans le centre de G.

   Comme $n_{11} = 1$ nous avons $\mathrm{P} \lhd \mathrm{G}$. Soit Q un 3-Sylow ; il agit sur P par conjugaison.

   L'équation aux classes s'écrit $|\mathrm{P}| = \sum_i \mathcal{O}_i$. Chaque orbite est de cardinal $\frac{|\mathrm{Q}|}{|\mathrm{St}\mathcal{O}_i|}$ et $\frac{|\mathrm{Q}|}{|\mathrm{St}\mathcal{O}_i|} \in \{1, 3\}$. C'est 1 si l'orbite est réduite à un point x_i tel que pour tout $g \in \mathrm{Q}$ $gx_ig^{-1} = x_i$. Par suite

   $$|\mathrm{P}| = |\mathrm{P}^{\mathrm{Q}}| \bmod 3$$

   où

   $$\begin{aligned} \mathrm{P}^{\mathrm{Q}} &= \{p \in \mathrm{P} \mid \forall\, q \in \mathrm{Q},\, q \cdot p = p\} \\ &= \{p \in \mathrm{P} \mid \forall\, q \in \mathrm{Q},\, qpq^{-1} = p\} \\ &= \{p \in \mathrm{P} \mid \forall\, q \in \mathrm{Q},\, qp = pq\}. \end{aligned}$$

   Comme $|\mathrm{P}^{\mathrm{Q}}|$ divise 11 et $11 \neq 1 \bmod 3$, $\mathrm{P}^{\mathrm{Q}} = \mathrm{P}$, *i.e.* le sous-groupe des éléments qui commutent à tous les éléments de P contient Q. De même les éléments qui commutent à tous les éléments de P contient un 7-Sylow et bien entendu P car P est cyclique. Le sous-groupe des éléments qui commutent à tous les éléments de P est d'ordre un multiple de 3, 7 et 11, c'est donc G.

3. Montrons que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G.

   Commençons par montrer l'existence d'un tel sous-groupe. Soit Q un 7-Sylow. Puisque $P \triangleleft G$ et $P \cap Q = \{id\}$, PQ est un sous-groupe de G d'ordre 77. Comme $Q \triangleleft G$, $PQ \triangleleft G$.

   Montrons maintenant l'unicité. Soit H un sous-groupe de G d'ordre 77. Alors H contient un 11-Sylow et un 7-Sylow. Donc H = PQ. Soit p dans P d'ordre 11 et soit q dans Q d'ordre 7. Puisque $pq = qp$ (rappelons que p appartient à P et que $P \subset Z(G)$) pq est d'ordre 77 donc PQ est cyclique.

4. Montrons que G admet un sous-groupe cyclique d'ordre 33.

   Soit R un 3-Sylow. Alors PR est un sous-groupe distingué de G d'ordre 33. En effet soient p d'ordre 11 dans P et r d'ordre 3 dans R. Puisque P est contenu dans le centre de G nous avons $pr = rp$ et pr est d'ordre 33.

Exercice 406

Rappelons que D_{2n} désigne le groupe à $2n$ éléments des isométries d'un polygone régulier à n côtés. On se propose de montrer que si G est un groupe de cardinal 70, alors G est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Partie I

Soit G un groupe. Notons n_p le nombre de p-sous-groupes de Sylow de G et $o(n)$ le nombre d'éléments d'ordre n.

1. Soit p un premier impair. Montrer pourquoi un groupe de cardinal $2p$ est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou D_{2p}.
2. Que valent n_2 et n_p lorsque $G = D_{2p}$?

   Si S et T sont deux sous-groupes de G tels que $S \cap T = \{e\}$, alors on considère $ST = \{st \mid s \in S, t \in T\}$.
3. Montrer que si S est distingué dans G, alors ST = TS est un sous-groupe de cardinal $|S||T|$.
4. Montrer que si S et T sont distingués dans G, alors ST est un sous-groupe isomorphe à $S \times T$. En déduire qu'un groupe de cardinal 35 est cyclique.

Partie II

Soit G un groupe de cardinal 70.

1. Exprimer $o(p)$ en terme de n_p et énumérer les valeurs possibles a priori pour n_2, n_5 et n_7.
2. Déduire de ce qui précède que G possède un sous-groupe K d'ordre 35. Montrer que K est distingué dans G.
3. En déduire que G contient un sous-groupe distingué $H \simeq \mathbb{Z}/35\mathbb{Z}$.

4. Calculer n_2 dans le cas des quatre groupes

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

En déduire qu'ils ne sont pas isomorphes.

5. Inversement montrer en considérant les valeurs possibles de n_2 que G est isomorphe à l'un des quatre groupes

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Éléments de réponse 406

Partie I

1. Si $|G| = 2p$, les théorèmes de Sylow assurent l'existence d'un sous-groupe distingué H de cardinal p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et un sous-groupe d'ordre 2 disons $K = \{e, s\}$. Soit r un générateur de H. Alors srs^{-1} appartient à H donc est égal à r^a pour un certain a. Alors d'une part $sr^as^{-1} = r^{a^2}$ et d'autre part $r = s^{-1}r^as$ qui se réécrit $r = sr^as^{-1}$ puisque $s^2 = e$. On en déduit que $r^{a^2} = r$ et donc $a^2 \equiv 1 \bmod p$ et donc $a \equiv \pm 1 \bmod p$. Si $a = 1$, l'élément s commute avec r donc rs est d'ordre $2p$ et $G \simeq \mathbb{Z}/2p\mathbb{Z}$. Si $a = -1$, alors $srs^{-1} = r^{-1}$ ce qui caractérise le groupe diédral.

2. Nous avons $n_p = 1$ (il n'y a qu'un seul p Sylow qui est distingué dans G) et $n_2 = p$ (en effet il y a p éléments d'ordre 2, les symétries).

3. Si S est distingué dans G, alors pour tout $t \in G$ nous avons $St = tS$ d'où l'égalité $ST = TS$. Si $g = st$ et $g' = s't'$, alors $gg' = sts't' = s(ts't^{-1})tt'$ appartient à ST. Si $g = st$, alors $g^{-1} = t^{-1}s^{-1}$ appartient à $TS = ST$. Par suite ST est bien un sous-groupe de G.

   Montrons que l'application

$$\phi\colon S \times T \to G \qquad\qquad (s,t) \mapsto st$$

est injective. Soient (s,t) et (s',t') dans $S \times T$ tels que $\phi(s,t) = \phi(s',t')$. L'égalité $\phi(s,t) = \phi(s',t')$ se réécrit $st = s't'$ dont on déduit $(s')^{-1}s = t't^{-1}$. En particulier $(s')^{-1}s = t't^{-1}$ est un élément de $S \cap T$; comme $S \cap T = \{e\}$, on obtient que $(s')^{-1}s = t't^{-1} = e$, soit que $s = s'$ et $t = t'$. Ainsi l'application ϕ est injective ; de plus son image est par définition ST. Par conséquent $|S \times T| = |ST|$. Mais $|S \times T| = |S| \cdot |T|$ d'où $|S| \cdot |T| = |ST|$.

4. D'une part $sts^{-1}t^{-1} = s(ts^{-1}t^{-1})$ donc $sts^{-1}t^{-1}$ appartient à S (par hypothèse $S \lhd G$), d'autre part $sts^{-1}t^{-1} = (sts^{-1})t^{-1}$ donc $sts^{-1}t^{-1}$ appartient à T (par hypothèse $T \lhd G$). Ainsi $sts^{-1}t^{-1}$ appartient à $S \cap T = \{e\}$, donc $sts^{-1}t^{-1} = e$ autrement dit s et t commutent. Ceci entraîne que ϕ est un morphisme ; en effet

$$\phi((s,t)\cdot(s',t')) = \phi(ss',tt') = ss'tt' = sts't' = \phi(s,t)\phi(s',t').$$

D'après ce qui précède $\phi\colon S \times T \to ST$ est donc un isomorphisme.

Si $|\mathrm{G}| = 35$ le groupe contient un unique 5-Sylow $\mathrm{S} \simeq \mathbb{Z}/5\mathbb{Z}$ et un unique 7-Sylow $\mathrm{T} \simeq \mathbb{Z}/7\mathbb{Z}$. Comme ils sont tous les deux distingués dans G d'intersection triviale nous obtenons d'après les questions précédentes que

$$\mathrm{ST} = \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Enfin $|\mathrm{ST}| = 35 = |\mathrm{G}|$ conduit à $\mathrm{ST} = \mathrm{G}$.

Partie II

Soit G un groupe de cardinal 70.

1. Comme les p-Sylow sont de cardinal p (pour $p = 2$, 5 ou 7) ils sont deux à deux disjoints hormis l'élément e bien sûr qui est présent dans chacun d'entre eux. Ainsi si H_1, H_2, …, H_{n_p} désignent les p-Sylow de G nous avons

$$\Big|\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}\Big| = n_p(p-1)$$

Par ailleurs d'après les théorèmes de Sylow $\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}$ est l'ensemble des éléments d'ordre p. Ainsi $o(p) = n_p(p-1)$.

D'après les théorèmes de Sylow n_7 divise 10 et $n_7 \equiv 1 \bmod 7$ donc $n_7 = 1$.

D'après les théorèmes de Sylow n_5 divise 14 et $n_5 \equiv 1 \bmod 5$ donc $n_5 = 1$.

D'après les théorèmes de Sylow n_2 divise 35 et $n_2 \equiv 1 \bmod 2$ donc $n_2 \in \{1, 5, 7, 35\}$.

2. Soient S l'unique 5-Sylow de G et T l'unique 7-Sylow de G. Ils sont tous les deux distingués dans G donc $\mathrm{K} = \mathrm{ST}$ est un sous-groupe de cardinal 35 qui est automatiquement distingué dans G (on peut aussi remarquer que $[\mathrm{G} : \mathrm{K}] = 2$ donc K est distingué dans G).

3. D'après les questions qui précèdent nous avons

$$\mathrm{K} = \mathrm{ST} \simeq \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}.$$

4. Désignons par $n_2(\mathrm{G})$ le nombre de 2-Sylow du groupe G.

Le groupe $\mathbb{Z}/70\mathbb{Z}$ étant abélien nous avons $n_2\big(\mathbb{Z}/70\mathbb{Z}\big) = 1$.

Le groupe D_{2n} contient n symétries d'ordre 2. Par conséquent $n_2(\mathrm{D}_{70}) = 35$. De plus si B est de cardinal impair, un 2-Sylow de $\mathrm{A} \times \mathrm{B}$ est contenu dans $\mathrm{A} \times \{e\}$ donc $n_2(\mathrm{A} \times \{e\}) = n_2(\mathrm{A})$; par suite

$$n_2\Big(\mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}\Big) = n_2(\mathrm{D}_{14}) = 7 \qquad n_2\Big(\mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z}\Big) = n_2(\mathrm{D}_{10}) = 5.$$

5. Choisissons un générateur r de $\mathrm{ST} = \mathrm{K} \simeq \mathbb{Z}/35\mathbb{Z}$ et s un élément d'ordre 2. Posons $\mathrm{R} = \{e, s\}$. Observons que $srs^{-1} = r^a$ avec $a \in \mathbb{Z}/35\mathbb{Z}$ et $a^2 = 1$. Comme $a^2 \equiv 1 \bmod 35$ équivaut par le Lemme chinois à $a^2 \equiv 1 \bmod 5$ et $a^2 \equiv 1 \bmod 7$ on a quatre solutions :

— $a \equiv 1 \bmod 35$,

— $a \equiv -1 \bmod 35$,

— $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$,

— $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$.

Intéressons-nous à chacune de ces éventualités :

— si $a \equiv 1 \bmod 35$, alors R commute avec K et $\mathrm{G} \simeq \mathrm{K} \times \mathrm{R} \simeq \mathbb{Z}/35\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/70\mathbb{Z}$.

— si $a \equiv -1 \bmod 35$, alors s commute avec S mais pas avec T ainsi S commute avec T et R donc avec le sous-groupe RT qui est d'ordre 14. Puisqu'il est non abélien RT doit être isomorphe à D_{14}. Par conséquent $\mathrm{G} \simeq \mathrm{S} \times \mathrm{RT} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathrm{D}_{14}$.

— le cas $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$ se traite de la même façon que le cas précédent et on obtient $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathrm{D}_{10}$.

— si $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$ alors $\mathrm{G} \simeq \mathrm{D}_{70}$.

Exercice 407

1. Soit G un groupe fini d'ordre n. Soit p un facteur premier de n. Soit n_p le nombre de p-Sylowde G. Montrer que si n ne divise pas $n_p!$, alors le groupe G n'est pas simple.
2. Soit G un groupe fini d'ordre n. Montrer que si n est de la forme $p^\alpha q^\beta$ et si n ne divise pas $p^\alpha!$ ou $q^\beta!$, alors G n'est pas simple.
3. Montrer qu'il n'existe pas de groupe simple d'ordre 72.

Éléments de réponse 407

1. Si $n_p = 1$, alors l'unique p-Sylowde G est distingué. Sinon G opère transitivement sur l'ensemble à $n_p > 1$ éléments de ses p-Sylow. On obtient aussi un morphisme
$$\varphi \colon \mathrm{G} \to \mathfrak{S}_{n_p}$$
qui n'est pas trivial (*i.e.* n'envoie pas G sur $\{\mathrm{id}\}$) car l'opération est transtive et $n_p > 1$. Puisque n ne divise pas $n_p!$, le morphisme φ ne peut être injectif. Son noyau $\ker \varphi$ est donc un sous-groupe distingué non trivial de G.
2. Supposons par exemple que n ne divise pas $q^\beta!$. D'après les théorèmes de Sylow n_p divise q^β donc est plus petit que q^β. Comme n ne divise pas $q^\beta!$ il ne divise pas non plus [15] $n_p!$ et on conclut par 1.
3. Soit G un groupe d'ordre 72. Notons que $72 = 2^3 \times 3^2$. Soit n_3 le nombre de 3-Sylow. D'après les théorèmes de Sylow d'une part n_3 divise $2^3 = 8$, d'autre part $n_3 \equiv 1 \bmod 3$. Par suite n_3 vaut 1 ou 4. Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué ; en particulier G n'est pas simple. Si $n_3 = 4$, alors 72 ne divise pas $n_3! = 24$ et G n'est pas simple d'après 1.

15. Si $a < b$, alors $a!$ divise $b!$.

Exercice 408 Soit G un groupe fini simple non abélien.

1. Soit H un sous-groupe propre de G. Montrer que |G| divise [G : H]! (indication : montrer que G est isomorphe à un sous-groupe du groupe alterné $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$). Puisque H est distinct de G on peut même dire que G divise $\frac{1}{2}[\mathrm{G} : \mathrm{H}]!$.
2. Soit p un diviseur premier de |G|. Désignons par n_p le nombre de p-Sylow de G. L'entier |G| divise alors $n_p!$.

Éléments de réponse 408

1. Notons φ le morphisme de G dans $\mathfrak{S}_{\mathrm{G}/\mathrm{H}}$ induit par l'action de G sur l'ensemble G/H des classes à droite de G modulo H. Le noyau de cette action est exactement l'intersection des conjugués de H dans G. C'est un sous-groupe propre de G car H l'est par hypothèse. Puisque G est simple $\ker\varphi = \{\mathrm{id}\}$, *i.e.* φ est injectif.

   Intéressons-nous alors au morphisme $\mathrm{sgn}\circ\varphi\colon \mathrm{G}\to\{-1,1\}$ obtenu à partir de φ par composition par la signature $\mathrm{sgn}\colon \mathfrak{S}_{\mathrm{G}/\mathrm{H}}\to\{-1,1\}$. Si $\mathrm{sgn}\circ\varphi$ pouvait prendre la valeur -1, le groupe G possèderait un sous-groupe distingué d'indice 2 et ne serait pas simple non abélien. Par conséquent le morphisme $\mathrm{sgn}\circ\varphi$ est trivial et φ plonge donc G dans $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$. En particulier |G| divise $|\mathfrak{S}_{\mathrm{G}/\mathrm{H}}| = [\mathrm{G} : \mathrm{H}]!$.
2. Soit P un p-Sylow de G. Puisque G est simple non abélien, le normalisateur [16] $N_{\mathrm{G}}(\mathrm{P})$ de P dans G est un sous-groupe propre de G. D'après le 1. nous avons donc : |G| divise $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]!$. Les théorèmes de Sylowassure que $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]! = n_p!$ d'où le résultat.

1.9. Structure des groupes abéliens de type fini

Exercice 409

Soit G un groupe de type fini.

Un sous-groupe H de G est-il nécessairement de type fini ? Justifiez votre réponse.

Éléments de réponse 409

Soit G est un groupe de type fini ; G peut contenir un sous-groupe H qui n'est pas de type fini.

Considérons le sous-groupe G de $\mathrm{GL}(2,\mathbb{Q})$ engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

16. dans un groupe G, le normalisateur d'une partie X est l'ensemble, noté $N_{\mathrm{G}}(X)$, des éléments g de G qui normalisent X, c'est-à-dire qui vérifient $gXg^{-1} = X$: $N_{\mathrm{G}}(X) = \left\{g\in\mathrm{G}\,|\,gXg^{-1}=X\right\} = \left\{g\in\mathrm{G}\,|\,gX=Xg\right\}$

Soit H le sous-groupe de G formé des matrices de G avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que H soit de type fini, *i.e.* $\mathrm{H} = \langle M_1, M_2, \ldots, M_r \rangle$ avec $M_i = \begin{pmatrix} 1 & m_i \\ 0 & 1 \end{pmatrix}$. Puisque $M_i^{-1} = \begin{pmatrix} 1 & -m_i \\ 0 & 1 \end{pmatrix}$ et $M_i M_j = \begin{pmatrix} 1 & m_i + m_j \\ 0 & 1 \end{pmatrix}$, il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}(2, \mathbb{Q})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or $A^{-N} B A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$: contradiction ($2^N > N$). Ainsi H n'est pas de type fini alors que G l'est.

Considérons par exemple le groupe libre G sur deux générateurs a et b. Soit H le sous-groupe engendré par tous les éléments de la forme ab^n avec $n \in \mathbb{N}$. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H le nombre de b consécutifs soit toujours strictement inférieur à N. Or ab^N appartient à H : contradiction. Le sous-groupe H de G n'est donc pas de type fini.

Exercice 410

Soit G un groupe abélien.

Montrer que $T(\mathrm{G}) = \{g \in \mathrm{G} \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Donner un exemple explicite pour lequel $T(\mathrm{G})$ n'est pas un sous-groupe de G si G n'est pas abélien.

Éléments de réponse 410

Soit G un groupe abélien.

Montrons que $T(\mathrm{G}) = \{g \in G \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Clairement $T(\mathrm{G})$ est contenu dans G. On a

- $o(e) = 1 < \infty$ donc $e \in T(\mathrm{G})$;
- soient g et h dans $T(\mathrm{G})$. Notons n (respectivement m) l'ordre de g (respectivement h). Par hypothèse $n < \infty$ et $m < \infty$. On a bien sûr $o(h^{-1}) = m$. Puisque G est abélien on a

  $$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn}$$

  Par suite $(gh^{-1})^{mn} = (g^n)^m((h^{-1})^m)^n = e^m e^n = e$. Ainsi $o(gh^{-1}) \leq mn < \infty$ et gh^{-1} appartient à $T(\mathrm{G})$.

Ainsi $T(\mathrm{G})$ est un sous-groupe de G.

Montrons que si G n'est pas abélien, alors $T(\mathrm{G})$ n'est pas forcément un sous-groupe de G.

Considérons $\mathrm{G} = \mathrm{O}(2)$. Soit ρ la rotation d'angle θ où θ/π est irrationnel. Alors ρ n'appartient pas à $T(\mathrm{G})$. Mais $\rho = s_2 \circ s_1$ avec s_1, s_2 réflexions ; en particulier $o(s_1) = o(s_2) = 2$ et donc s_1, s_2 appartiennent à $T(\mathrm{G})$.

Exercice 411

Soit $n \in \mathbb{N}$, $n \geq 2$. Trouver le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 411

Soit $n \in \mathbb{N}$, $n \geq 2$. Déterminons le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} T\left(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right) &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, o(a,b) < \infty\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, \exists\, k \in \mathbb{N}^*,\ o(a,b) = k\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, (ka, kb) = (0, \bar{0})\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, a = 0 \text{ et } b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \{0\} \times \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Montrons que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Soient $(1,1)$ et $(-1,0)$ deux éléments de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ils sont d'ordre infini mais $(1,1) + (-1,0) = (0,1)$ est d'ordre fini.

Exercice 412

a) Donner un exemple de groupe abélien qui n'est pas de type fini.

b) Si p est un nombre premier, quel est le groupe sous-jacent au corps $\mathbb{F}_{p^n}$?

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$.
Montrer que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

d) Montrer qu'un groupe abélien de type fini et de torsion est fini (ceci n'est plus vrai pour les groupes non-abéliens : voir par exemple [Calais, p. 294]).

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Éléments de réponse 412

a) $(\mathbb{Q}, +)$ est un groupe abélien qui n'est pas de type fini (pour le vérifier raisonner par l'absurde).

b) Soit p un nombre premier.
Si $n = 1$, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et le groupe sous-jacent est $\mathbb{Z}/p\mathbb{Z}$.
Si $n = 2$, alors le groupe sous-jacent à $\mathbb{F}_{p^2}$ est $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ car $\mathbb{Z}/p^2\mathbb{Z}$ possède un élément d'ordre p^2 alors que $\mathbb{F}_{p^2}$ est de caractéristique p donc sans élément d'ordre p^2.
De même pour n quelconque le groupe sous-jacent à $\mathbb{F}_{p^n}$ est $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$. Montrons que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

Écrivons les décompositions de m et n en nombre premiers :

$$m = \prod_i p_i^{\alpha_i} \qquad\qquad n = \prod_i p_i^{\beta_i}$$

Alors

$$\delta = \prod_i p_i^{\min(\alpha_i,\beta_i)} \qquad\qquad \mu = \prod_i p_i^{\max(\alpha_i,\beta_i)}$$

D'une part

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d'autre part

$$\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

Si $\min(\alpha_i,\beta_i) = \alpha_i$, alors $\max(\alpha_i,\beta_i) = \beta_i$; réciproquement si $\min(\alpha_i,\beta_i) = \beta_i$ alors $\max(\alpha_i,\beta_i) = \alpha_i$. Par conséquent tous les α_i et β_i apparaissent une fois et une seule dans le produit

$$\prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

qui est donc isomorphe à

$$\prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d) Montrons qu'un groupe abélien de type fini et de torsion est fini.

Soit G un groupe abélien de type fini et sans torsion. Puisque G est abélien de type fini on a

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

où $r \geq 0$, $n_j \geq 0$ pour tout $1 \leq j \leq s$ et n_{i+1} divise n_i pour tout $1 \leq i \leq s-1$.

De plus G est de torsion, *i.e.* tout élément est d'ordre fini. Il en résulte que $r = 0$, c'est-à-dire que

$$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

En particulier $|\mathrm{G}| = n_1 n_2 \ldots n_s < \infty$.

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Soient G un groupe abélien et $(\mathrm{H}_i)_{1\leq i\leq r}$ une famille de sous-groupes d'ordre 2 à 2 premiers entre eux. Alors ces groupes sont en somme directe dans G. En effet soit d_i l'ordre de H_i. Rappelons que dans un groupe abélien si G est d'ordre m et h d'ordre n avec n, m premiers entre eux, alors gh est d'ordre mn. Ainsi pour tout i l'ordre de tout

élément de $\sum_{j\neq i} \mathrm{H}_j$ divise $\mathrm{ppcm}_{j\neq i}(d_j)$ donc est premier avec d_i. Il en résulte que nous avons pour tout i

$$\mathrm{H}_i \cap \Big(\sum_{j\neq i} \mathrm{H}_j\Big) = \{1\}$$

Par conséquent les H_i, $1 \leq i \leq r$, sont en somme directe.

D'après ce qui précède les différents p-Sylow d'un groupe abélien fini G sont en somme directe. L'égalité des cardinaux assure que G est la somme directe de ses sous-groupes de Sylow.

Exercice 413

Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G.

Éléments de réponse 413

Soit G un groupe abélien fini. Montrons qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G. Le théorème de structure assure que

$$\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{d_2\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{d_r\mathbb{Z}}$$

où d_i divise d_{i+1} pour tout $1 \leq i \leq r-1$.

L'exposant de G est d_r et $(0, 0, \ldots, 0, 1)$ est d'ordre d_r.

Exercice 414

Montrer qu'il existe exactement 20 groupes abéliens d'ordre ≤ 15 à isomorphisme près. On donnera leur forme canonique successivement sous forme « facteurs invariants » et sous forme « facteurs élémentaires ».

Éléments de réponse 414

Il y a 15 groupes cycliques d'ordre $n \leq 15$. Pour chacun

- ◇ la décomposition en facteurs invariants consiste juste à écrire ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$;
- ◇ la décomposition en facteurs élémentaires consiste à écrire la décomposition en facteurs premiers de n.

Par exemple

Exercice 415

a) Donner la décomposition primaire du groupe ${}^{\mathbb{Z}}\!/_{8\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{24\mathbb{Z}}$. En déduire ses facteurs invariants.

b) Donner la décomposition primaire du groupe ${}^{\mathbb{Z}}\!/_{54\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{26\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{15\mathbb{Z}}$. En déduire ses facteurs invariants.

Éléments de réponse 415

a) Donnons la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

Notons que $8 = 2^3$, $12 = 2^2 \times 3$ et $24 = 2^3 \times 3$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2^3, 2^2, 3, 2^3 et 3.

Déterminons les facteurs invariants de G. Réordonnons les diviseurs élémentaires comme suit

$$\begin{array}{r} 2^2 \mid 2^3 \mid 2^3 \\ 3 \mid 3 \end{array}$$

Les facteurs invariants de G sont donc $2^2 \times 1 = 4$, $2^3 \times 3 = 24$ et $2^3 \times 3 = 24$.

Par conséquent

$$\mathrm{G} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}.$$

b) Donnons la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

Notons que $54 = 2 \times 3^3$, $26 = 2 \times 13$ et $15 = 3 \times 5$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2, 3^3, 2, 13, 3 et 5.

Donnons ses facteurs invariants. On ordonne les diviseurs élémentaires comme suit

$$\begin{array}{r} 2 \mid 2 \\ 3 \mid 3^3 \\ 5 \\ 13 \end{array}$$

Les facteurs invariants de G sont donc $2 \times 3 = 6$ et $2 \times 3^3 \times 5 \times 13 = 3510$.

Exercice 416

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathfrak{S}_n$.

Éléments de réponse 416

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Expliquons pourquoi. Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ et le nombre de groupes abéliens de cardinal 32 à isomorphisme près sont chacun en bijection avec l'ensemble des partitions de 5 (rappelons qu'une partition d'un entier est une décomposition de cet entier en une somme d'entiers strictement positifs à l'ordre près des termes).

b) Généralisons au nombre de classes de conjugaison dans $\mathfrak{S}_n$. Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphismes de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$. Considérons

$$\varphi\colon P_n \to G_n \qquad (n_1, n_2, \dots, n_r) \mapsto \text{ classe d'isomorphisme de } \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

et

$$\psi\colon P_n \to C_n \qquad (n_1, n_2, \dots, n_r) \mapsto \text{ classe de conjugaison de la permutation } (1, 2, \dots, n_1)(n_1+1, \dots, n_1+n_2)\dots(n_1+n_2+n_{r-1}+1, \dots, n)$$

φ et ψ sont des bijections donc $|C_n| = |G_n|$: il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 417

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1, 3)$ et $(2, 0)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1, 1)$ et $(1, -1)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

Éléments de réponse 417

◇ Déterminons la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$. On a

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Par suite $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/6\mathbb{Z}$.

◇ On a

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Par conséquent $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 418

Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2, 5)$, $(5, -1)$ et $(1, -2)$. Déterminer une base de H et décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

Éléments de réponse 418

On a

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 9 & 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}$$

donc $\mathrm{H} = \langle (0,9),\, (1,-2) \rangle$ est de rang 2.

De plus $\begin{pmatrix} 0 & 1 \\ 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 9 & 0 \end{pmatrix}$; par suite ${}^{\mathbb{Z}^2}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$.

Exercice 419

Trouver une base du groupe suivant :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases} \right\}$$

Éléments de réponse 419

Soit G le groupe donné par :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases} \right\}$$

On a

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 7x+12z=0 \end{cases} \right\}$$

Comme $7x+12z=0$ on écrit $x=12k$ et $z=-7k$. Alors $2x+3y+5z=0$ conduit à $3y=11k$. On pose donc $k=3l$ alors

$$x = 36\ell, \qquad y = 11\ell, \qquad z = -21\ell$$

Finalement

$$\mathrm{G} = \{\ell(36,11,-21) \,|\, \ell \in \mathbb{Z}\} = \mathrm{Vect}(36,11,-21)$$

et $\{(36,11,-21)\}$ est une base de G.

Exercice 420

Les groupes

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \qquad\qquad {}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$$

sont-ils isomorphes ? Justifier votre réponse.

Éléments de réponse 420

D'une part $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$ et $25 = 5^2$ donc

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5^2\mathbb{Z}};$$

d'autre part $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$ donc

$${}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2^2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3^2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5^2\mathbb{Z}}.$$

En particulier les groupes

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \qquad\qquad {}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$$

sont isomorphes.

Exercice 421

Soit G un groupe abélien fini.

Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Éléments de réponse 421

Raisonnons par l'absurde. Supposons que G ne soit pas cyclique. Alors G est isomorphe à $\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \ldots \times \mathbb{Z}/q_k\mathbb{Z}$ où $q_1|q_2|\ldots|q_k$ sont les facteurs invariants de G et $k \geq 2$. Il y a alors (au moins) deux sous-groupes distincts d'ordre q_1 : d'une part le facteur $\mathbb{Z}/q_1\mathbb{Z}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/q_2\mathbb{Z}$ associé au diviseur q_1 de q_2.

Exercice 422

Soit p un nombre premier. Soit G un groupe abélien fini d'ordre n tel que tous les éléments de G soient d'ordre une puissance de p.

1. Soit g un élément de $G \setminus \{id\}$. Soit $H = \langle g \rangle$ le sous-groupe cyclique engendré par g.
   Montrer que tous les éléments de G/H sont d'ordre une puissance de p.
2. En déduire par récurrence sur n que G est d'ordre une puissance de p.
   (Indication : prendre comme hypothèse de récurrence que tous les groupes d'ordre $< n$ dont tous les éléments sont d'ordre une puissance de p sont d'ordre une puissance de p).
3. Soit G un groupe fini abélien d'ordre 12.
   Montrer que si G ne contient pas d'élément d'ordre 3, il ne contient que des éléments d'ordre 1, 2 ou 4.
   En déduire que G possède un élément d'ordre 3.
4. Supposons désormais que G est un groupe abélien d'ordre 12 non cyclique. Soit $g \in G$ un élement d'ordre 3. Soit $H = \langle g \rangle$ le sous-groupe cyclique engendré par $\langle g \rangle$. Montrer que G/H ne peut être cyclique.
5. En déduire que $G/H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
6. Montrer que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Éléments de réponse 422

Exercice 423

1. Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?
   Montrer que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, alors il y a exactement $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1)$ sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que dans un groupe cyclique tous les sous-groupes sont caractéristiques [17].

17. Soit G un groupe. Un sous-groupe de G qui est stable par tout automorphisme de G est dit caractéristique.

3. Déduire de l'existence d'un p-Sylow dans un groupe G d'ordre $p^\alpha n$ (où p désigne un entier premier, n un entier premier avec p et $\alpha \geq 1$), le théorème de Cauchy, *i.e.* l'existence d'un élément d'ordre p.
4. Montrer qu'un groupe fini G a pour ordre une puissance d'un nombre premier p si et seulement si tout élément du groupe G a pour ordre une puissance de p.

Éléments de réponse 423

Exercice 424

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ sont-ils isomorphes ?
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont-ils isomorphes ?

Éléments de réponse 424

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ ne sont pas isomorphes. En effet posons
$$\mathrm{G}_1 = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}.$$
Nous avons $12 = 2^2 \times 3$, $72 = 2^3 \times 3^2$, $18 = 2 \times 3^2$ et $48 = 2^4 \times 3$. Les groupes G_1 et G_2 sont tous deux d'ordre $2^5 \times 3^3$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i$ pour $i = 1, 2$ où A_i est un groupe abélien d'ordre 2^5 et B_i un groupe abélien d'ordre 3^3. Le groupe A_1 est associé à la partition $(3, 2)$ de 5 et le groupe A_2 est associé à la partition $(4, 1)$ de 5 ; ils ne sont donc pas isomorphes. Par suite les groupes G_1 et G_2 ne sont pas isomorphes.
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont isomorphes. En effet posons
$$\mathrm{G}_1 = \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

Nous avons $72 = 2^3 \times 3^2$, $84 = 2^2 \times 3 \times 7$, $36 = 2^2 \times 3^2$ et $168 = 2^3 \times 3 \times 7$. Les groupes G_1 et G_2 sont donc de même ordre $2^5 \times 3^3 \times 7$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i \times \mathrm{C}_i$ où A_i est un groupe abélien d'ordre 2^5, B_i est un groupe abélien d'ordre 3^3 et C_i est un groupe abélien d'ordre 7. Les groupes A_1 et A_2 sont associés à la partition $(3, 2)$ de 5, ils sont isomorphes. Les groupes B_1 et B_2 sont associés à la partition $(2, 1)$ de 3 ; ils sont donc isomorphes. Les groupes C_1 et C_2 sont isomorphes. Il en résulte que G_1 et G_2 sont isomorphes.

Exercice 425

Trouver tous les couples d'entiers naturels (a, b) tels que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Éléments de réponse 425

Exercice 426

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrer que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Éléments de réponse 426

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.

Montrons que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Les nombres a, b, c et d étant premiers entre deux à deux nous avons

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

$$\mathbb{Z}/cd\mathbb{Z} \simeq \mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

$$\mathbb{Z}/ac\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$$

$$\mathbb{Z}/bd\mathbb{Z} \simeq \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

Par suite les deux groupes $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ et $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$ sont isomorphes.

Exercice 427

Soit $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Considérons les deux sous-groupes suivants de G :

$$\mathrm{H} = \mathbb{Z}/2\mathbb{Z} \times \{0\} \qquad\qquad \mathrm{K} = \{0\} \times \{0, 6\}.$$

Remarquons que $\mathrm{H} \simeq \mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z}$ mais avons-nous $\mathrm{G}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$?

Éléments de réponse 427

D'une part $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, d'autre part $\mathrm{G}/\mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \times \mathbb{Z}/3\mathbb{Z}$.

Les deux premiers facteurs ne sont pas isomorphes donc les deux groupes ne sont pas isomorphes.

Exercice 428

Soient G, H et K des groupes abéliens finis.

1. Montrer que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$.
2. Montrer que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

Éléments de réponse 428

Soient G, H et K des groupes abéliens finis. Montrons que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$et que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

La décomposition primaire de G est $\prod_{i=1}^{s} \mathrm{A}_i$, celle de $\mathrm{G} \times \mathrm{G}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \mathrm{A}_i$.

La décomposition primaire de H est $\prod_{i=1}^{t} \mathrm{B}_i$, celle de $\mathrm{H} \times \mathrm{H}$ est donc $\prod_{i=1}^{t} \mathrm{B}_i \times \mathrm{B}_i$.

La décomposition primaire de K est $\prod_{i=1}^{u} \mathrm{C}_i$, celle de $\mathrm{G} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \prod_{i=1}^{u} \mathrm{C}_i$ et celle de $\mathrm{H} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{B}_i \times \prod_{i=1}^{u} \mathrm{C}_i$.

Si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par suite $\mathrm{G} \simeq \mathrm{H}$.

Si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par conséquent $\mathrm{G} \simeq \mathrm{H}$.

Exercice 429

1. Exprimer tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.
2. Exprimer tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques.

Éléments de réponse 429

1. Exprimons tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.

   Les groupes abéliens d'ordre $99 = 3^2 \times 11$ sont isomorphes

   - soit à $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$,
   - soit à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

2. Exprimons tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques. Les groupes abéliens d'ordre $100 = 2^2 \times 5^2$ sont isomorphes

   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 430

Combien existe-t-il, à isomorphisme près, de groupes abéliens d'ordre 10^6 ?

Éléments de réponse 430

Nous avons $10^6 = 2^6 \times 5^6$. Les partitions de 6 sont

$$(6)$$
$$(5,1)$$
$$(4,2)$$
$$(4,1,1)$$
$$(3,3)$$
$$(3,2,1)$$
$$(3,1,1,1)$$
$$(2,2,2)$$
$$(2,2,1,1)$$
$$(2,1,1,1,1)$$
$$(1,1,1,1,1,1)$$

Elles sont donc au nombre de 11. Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 431

1. Soient G, H, G′ et H′ des groupes finis tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. Nous allons montrer qu'alors $H \simeq H'$.
   Étant donnés deux groupes finis G_1 et G_2, notons $m(G_1, G_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(G_1, G_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.
   a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(G_1, G_2) = \sum_{N \trianglelefteq G_1} i\Big({}^{G_1}\!/_{N}, G_2\Big). \tag{1.9.1}$$

   b) Montrer pour tout groupe fini L que

$$m(L, G) \cdot m(L, H) = m(L, G \times H).$$

   c) En déduire que pour tout groupe fini L on a l'égalité $m(L, H) = m(L, H')$.
   d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (3.6.2) que

$$i(L, H) = i(L, H'). \tag{1.9.2}$$

   e) Appliquer l'équation (1.16.4) à H pour en déduire que $H \simeq H'$.
   f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors en général H et H′ ne sont pas isomorphes.

2. Nous allons appliquer le résultat obtenu dans la partie 1. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
   Soit G un groupe abélien fini. Supposons que
   $$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$
   avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.
   a) Montrer que l'exposant de G est égal à n_1.
   b) Utiliser le résultat obtenu dans la partie 1. pour montrer que cette décomposition est unique.

Éléments de réponse 431

Exercice 432

Soit G un groupe abélien fini. Les assertions suivantes sont-elles vraies ou fausses ?

a) Pour tout d qui divise l'ordre de G, le groupe G admet un élément d'ordre d.

b) Pour tout d qui divise l'ordre de G, le groupe G admet un sous-groupe d'ordre d.

Éléments de réponse 432

Exercice 433

a) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12 et 72.

b) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Éléments de réponse 433

a) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 12.
   Nous avons $12 = 2^2 \times 3$. De plus les partitions de 2 sont

   2 1, 1

   Par conséquent il y a à isomorphisme près 2 groupes abéliens d'ordre 12 :
   $$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
   Déterminons à isomorphisme près tous les groupes abéliens d'ordre 72.
   Nous avons $72 = 2^3 \times 3^2$. De plus les partitions de 2 sont

   2 1, 1

   et celles de 3 sont

   3 2, 1 1, 1, 1

Par conséquent il y a à isomorphisme près $2 \times 3 = 6$ groupes abéliens d'ordre 72 :

$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

b) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Nous avons $10^6 = 2^6 \times 5^6$. De plus les partitions de 6 sont

6
5, 1
4, 2
4, 1, 1
3, 3
3, 2, 1
3, 1, 1, 1
2, 2, 2
2, 2, 1, 1
2, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 1

Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 434

a) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3 \mid 5g_1 - 2g_2 + 12g_3 = 3g_1 + 4g_3 = 0\rangle.$$

Déterminer la structure de ce groupe.

b) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3, g_4 \mid 2g_1 + 4g_2 - 4g_4 = 6g_1 - 12g_3 + 3g_4 = 0\rangle.$$

Déterminer la structure de ce groupe.

Éléments de réponse 434

Exercice 435

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Éléments de réponse 435

Nous utilisons le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}\right) \times \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}\right)$$

Notons que cette écriture est la décomposition en composantes p-primaires. En effet $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$, $25 = 5^2$, $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$.

Nous pouvons aussi écrire la décomposition en facteurs invariants de ces deux groupes, nous trouvons

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}.$$

Exercice 436

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Éléments de réponse 436

Montrons qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Soit G un groupe abélien fini non cyclique. Il est isomorphe à un produit

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_i \geq 2$ et $d_i \,|\, d_{i+1}$. Puisque G n'est pas cyclique, $r \geq 2$. Soit p un facteur premier de d_1 alors p disvise tous les d_i et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Le sous-groupe de p torsion de G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^r$ qui contient un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 437

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.

b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Éléments de réponse 437

a) La décomposition de 360 en facteurs premiers est $2^3 \times 3^2 \times 5$. Ainsi si G est un groupe de cardinal 360, alors le sous-groupe

$$T_2(\mathrm{G}) = \{g \in \mathrm{G} \,|\, \exists\, n \in \mathbb{N} \quad 2^n g = 0\}$$

de 2-torsion de G est un groupe abélien de cardinal 2^3, il y a donc trois classes d'isomorphisme de tels groupes : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. De même il y a exactement deux classes d'isomorphisme possibles pour $T_3(\mathrm{G})$ à savoir $\mathbb{Z}/9\mathbb{Z}$ et $\left(\mathbb{Z}/3\mathbb{Z}\right)^2$. Par ailleurs $T_5(\mathrm{G})$

est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Il y a donc exactement six classes d'isomorphisme de groupes abéliens d'ordre 360 donc les décompositions p-primaires et les décompositions en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/360\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times 4\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

b) Plus généralement, pour tout entier n, déterminons le nombre de groupes abéliens de cardinal n. Nous utilisons la classification des classes d'isomorphisme de groupes abéliens finis. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. La classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, d_2, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i \mid d_{i+1}$ et $d_1 d_2 \dots d_s = n$. Par suite chaque d_i se décompose comme suit : $d_i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \dots p_r^{\alpha_{r,i}}$ avec les contraintes suivantes : $\alpha_{i,j} \leq \alpha_{i+1,j}$ pour tout j, pour tout i et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$ et $\sum_{i=1}^{q} \alpha_{i,j} = \alpha_j$.

Il s'en suit que le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$ où $p(\alpha)$ désigne le nombre de partitions de α, *i.e.* le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 438

a) On considère $\mathrm{H} = \{(a,b) \in \mathbb{Z}^2 \mid a - b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$. Calculer le rang de H. Donner une base de H. Décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

b) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4, 8, 10)$ et $(6, 2, 0)$. Déterminer la structure du groupe H.

Éléments de réponse 438

a) Soit φ le morphisme de groupes donné par

$$\varphi \colon \mathbb{Z}^2 \to \mathbb{Z}/10\mathbb{Z}, \qquad (a,b) \mapsto a - b$$

Son noyau est H. En particulier H est un sous-groupe distingué de $\mathbb{Z}^2$.

D'une part H contient $(1,1)$ et $(0,10)$ donc $\operatorname{rg} \mathrm{H} \geq 2$. D'autre part $\mathrm{H} \subset \mathbb{Z}^2$ donc $\operatorname{rg} \mathrm{H} \leq 2$. Finalement $\operatorname{rg} \mathrm{H} = 2$.

Soit (a,b) dans H. Il existe n dans $\mathbb{Z}$ tel que $a = b + 10n$ et

$$(a,b) = (a, a-10n) = a(1,1) + (-n)(0,10).$$

Autrement dit $((1,1),(0,10))$ est une base de H.

Par ailleurs

$$\mathbb{Z}^2/\mathrm{H} = \langle (g_1,g_2) \,|\, g_1 + g_2 = 0,\ 10g_2 = 0 \rangle.$$

Puisque $\begin{pmatrix} 1 & 0 \\ 1 & 10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$ les facteurs invariants de $\mathbb{Z}^2/\mathrm{H}$ sont 1 et 10 et $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/10\mathbb{Z}$.

b) Notons H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminons la structure du groupe H. Nous avons

$$\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix}$$

Ainsi les facteurs invariants de $\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix}$ sont 2 et 10 et $\mathrm{H} \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Exercice 439

Soit $n \geq 1$ un entier. Montrer que tout système libre maximal dans $\mathbb{Z}^n$ est de cardinal n. Donner un exemple où un tel système n'est pas une base.

Éléments de réponse 439

Exercice 440

Soit $e_1 = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ un vecteur tel que le pgcd de ses coordonnées vaut 1. Montrer que l'on peut compléter e_1 en une base $(e_1, e_2, \ldots, e_n)$ de $\mathbb{Z}^n$.

Éléments de réponse 440

Exercice 441

Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

a) $\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}$;

b) $\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}$;

c) $\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}$.

Éléments de réponse 441

Nous pouvons procéder de deux manières différentes :

- soit en calculer le pgcd des coefficients de la matrice puis le pgcd des mineurs de taille 2, etc
- soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes.

Dans les deux cas nous obtenons ($\sim$ désigne l'équivalence des matrices à coefficients entiers) :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Les facteurs invariants sont donc respectivement $(1, 6)$, $(3, 9)$ et $(1, 2, 16)$.

Détaillons la première équivalence :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Détaillons la seconde équivalence :

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 12 & -27 \\ 69 & -153 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -27 \\ 9 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & 3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 12 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}.$$

Détaillons la dernière équivalence :

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -75 & 41 & -13 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -3 & 5 & -1 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -12 & 6 & -2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 0 & -14 & 2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -19 & 3 & -3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & -27 & 3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 3 & -5 & 1 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & -86 & 10 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 27 & -3 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & -2 \\ 0 & -2 & -2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -16 \\ 0 & -2 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -16 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Exercice 442

a) Soit G un groupe abélien de type fini. Soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme surjectif. Montrer que f est un isomorphisme.

Ceci est-il nécessairement vrai si on remplace surjectif par injectif ?

b) Soit G un groupe abélien libre de type fini et soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme. Définir le déterminant $\det(f) \in \mathbb{Z}$ de f. Montrer que f est injectif si et seulement si $\det(f) \neq 0$. Dans ce cas montrer que $|\det(f)| = |\mathrm{coker}(f)|$.

Éléments de réponse 442

Exercice 443

Le but de cet exercice est de redémontrer le théorème de structure des groupes abéliens finis. On rappelle qu'un caractère d'un groupe abélien fini G est un morphisme $\mathrm{G} \to \mathbb{C}^*$.

a) Si H est un sous-groupe d'un groupe abélien fini G, montrer que tout caractère de H se prolonge en un caractère de G.

b) Soit G un groupe abélien fini. On désigne par H un sous-groupe de G engendré par un élément de G d'ordre maximal. Montrer qu'on a l'isomorphisme $\mathrm{G} \simeq \mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

c) Conclure.

Éléments de réponse 443

Exercice 444 [Propriété d'annulation de groupes dans un produit direct (démonstration de Vipul Naik)]

A. Soient G, H, G′ et H′ des groupes finis tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. Nous allons montrer qu'alors $H \simeq H'$.
Étant donnés deux groupes finis G_1 et G_2, notons $m(G_1, G_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(G_1, G_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.

a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(G_1, G_2) = \sum_{N \trianglelefteq G_1} i\Big(G_1/N, G_2\Big). \tag{1.9.3}$$

b) Montrer pour tout groupe fini L que

$$m(L, G) \cdot m(L, H) = m(L, G \times H).$$

c) En déduire que pour tout groupe fini L on a l'égalité $m(L, H) = m(L, H')$.

d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (3.6.2) que

$$i(L, H) = i(L, H'). \tag{1.9.4}$$

e) Appliquer l'équation (1.16.4) à H pour en déduire que $H \simeq H'$.

f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors en général H et H′ ne sont pas isomorphes.

B. Nous allons appliquer le résultat obtenu dans la partie A. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
Soit G un groupe abélien fini. Supposons que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.

a) Montrer que l'exposant de G est égal à n_1.

b) Utiliser le résultat obtenu dans la partie A. pour montrer que cette décomposition est unique.

Éléments de réponse 444

Exercice 445

Soit $\Bbbk$ un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif $\Bbbk^\times = \Bbbk \setminus \{0\}$ de $\Bbbk$. Montrer que G est cyclique.

Éléments de réponse 445

Nous utilisons le théorème de structure des groupes abéliens finis. Si $|\mathrm{G}| > 1$, alors il existe une suite d'entiers $1 < a_1 \,|\, a_2 \,|\, \ldots \,|\, a_r$ tels que

$$\mathrm{G} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_r\mathbb{Z}$$

Montrons que $r = 1$. Puisque $a_r\mathrm{G} = \{0\}$ nous avons

$$\#\{z \in \Bbbk \,|\, z^{a_r} = 1\} \geq |\mathrm{G}| = a_1 a_2 \ldots a_r.$$

Par ailleurs le nombre de racines dans $\Bbbk$ du polynôme $X^{a_r} - 1 \in \Bbbk[X]$ est inférieur ou égal à son degré parce que $\Bbbk$ est commutatif. Il en résulte l'inégalité $a_1 a_2 \ldots a_r \leq a_r$ qui conduit à $r = 1$.

1.10. Produits semi-directs

Exercice 446

Soient N et H des groupes et soit $\phi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ un morphisme de groupes. Notons $\mathrm{N} \rtimes_\phi \mathrm{H}$ l'ensemble $\mathrm{N} \times \mathrm{H}$ muni de la loi de composition définie par

$$(n_1, h_1) \rtimes_\phi (n_2, h_2) = \big(n_1 \phi(h_1)(n_2), h_1 h_2\big).$$

1. Montrer que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe appelé produit semi-direct de H par N relativement à ϕ.
2. Montrer que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.
3. Identifier le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Éléments de réponse 446

1. Montrons que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe.
   - Commençons par montrer que la loi est associative.
     Soient n_1, n_2 et n_3 dans N. Soient h_1, h_2 et h_3 dans H. Par définition du produit nous avons

$$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = \big(n_1 \phi(h_1)(n_2), h_1 h_2\big) \rtimes_\phi (n_3, h_3) = \big(n_1 \phi(h_1)(n_2) \phi(h_1 h_2)(n_3), h_1 h_2 h_3\big).$$

     De même nous avons

$$(n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big) = (n_1, h_1) \rtimes_\phi \big(n_2 \phi(h_2)(n_3), h_2 h_3\big) = \big(n_1 \phi(h_1)(n_2 \phi(h_2)(n_3))\big), h_1 h_2 h_3\big).$$

     Or $\phi(h_1)$ et ϕ sont des morphismes donc

$$\phi(h_1)(n_2 \phi(h_2)(n_3)) = \phi(h_1)(n_2)(\phi(h_1) \circ \phi(h_2))(n_3) = \phi(h_1)(n_2)(\phi(h_1 h_2))(n_3)$$

dont on déduit que

$$((n_1,h_1)\rtimes_\phi(n_2,h_2))\rtimes_\phi(n_3,h_3)=(n_1,h_1)\rtimes_\phi((n_2,h_2)\rtimes_\phi(n_3,h_3)).$$

Par conséquent le produit $\rtimes_\phi$ est associatif.

- On voit tout de suite que l'élément $(e_{\mathrm{N}},e_{\mathrm{H}})$ est neutre pour la loi $\rtimes_\phi$.
- Montrons que tout élément admet un inverse.
  Soient $n\in\mathrm{N}$ et $h\in\mathrm{H}$. Pour tous $n'\in\mathrm{N}$ et $h'\in\mathrm{H}$ nous avons
  $$(n,h)\rtimes_\phi(n',h')=(e_{\mathrm{N}},e_{\mathrm{H}})$$
  si et seulement si
  $$(n\phi(n')(h'),hh')=(e_{\mathrm{N}},e_{\mathrm{H}})$$
  si et seulement si $h'=h^{-1}$ et $n'=\phi(h^{-1})(n^{-1})$. Le calcul de $(n',h')\rtimes_\phi(n,h)$ est similaire ce qui assure que (n,h) est inversible et que son inverse est $(n,h)^{-1}=(\phi(h^{-1})(n^{-1}),h^{-1})$.

Ainsi $\mathrm{N}\rtimes_\phi\mathrm{H}$ est bien un groupe.

2. Montrons que $\mathrm{N}\times\{e_{\mathrm{H}}\}\lhd\mathrm{N}\rtimes_\phi\mathrm{H}$ et $\{e_{\mathrm{N}}\}\times\mathrm{H}\subset\mathrm{N}\rtimes_\phi\mathrm{H}$.

   Les formules définissant le produit assurent que $\mathrm{N}\times\{e_{\mathrm{H}}\}$ et $\{e_{\mathrm{N}}\}\times\mathrm{H}$ sont bien des sous-groupes de $\mathrm{N}\rtimes_\phi\mathrm{H}$ car $\phi(h)(e_{\mathrm{N}})=e_{\mathrm{N}}$ pour tout $h\in\mathrm{H}$.

   Montrons que $\mathrm{N}\times\{e_{\mathrm{H}}\}$ est distingué dans $\mathrm{N}\rtimes_\phi\mathrm{H}$. Soient n, n' dans N et h' dans H. Alors

$$\begin{aligned}(n,h)\rtimes_\phi(n',e_{\mathrm{H}})\rtimes_\phi(n,h)^{-1} &= (n,h)\rtimes_\phi(n',e_{\mathrm{H}})\rtimes_\phi(\phi(h^{-1})(n^{-1}),h^{-1})\\ &= n\phi(h)(n'),h()\rtimes_\phi(\phi(h^{-1})(n^{-1}),h^{-1})\\ &= (n\phi(h)(n')\phi(h)(\phi(h^{-1})(n^{-1})),e_{\mathrm{H}})\\ &= (n\phi(h)(n')n^{-1},e_{\mathrm{H}})\in\mathrm{N}\times\{e_{\mathrm{H}}\}\end{aligned}$$

   Ainsi $\mathrm{N}\times\{e_{\mathrm{H}}\}$ est distingué dans $\mathrm{N}\rtimes_\phi\mathrm{H}$.

   Un calcul analogue montre que $\{e_{\mathrm{N}}\}\times\mathrm{H}$ n'est pas distingué en général.

3. Identifions le quotient de $\mathrm{N}\rtimes_\phi\mathrm{H}$ par $\mathrm{N}\times\{e_{\mathrm{H}}\}$.

   Considérons l'application naturelle $\pi\colon\mathrm{N}\rtimes_\phi\mathrm{H}\to\mathrm{H}$ donnée par la seconde projection, *i.e.* $\pi(n,h)=h$.

   Il est clair que π est surjective.

   La définition de la loi de groupes assure que π est un morphisme de groupes.

   Déterminons son noyau. Soient $n\in\mathrm{N}$ et $h\in\mathrm{H}$. Nous avons $\pi(n,h)=e_{\mathrm{H}}$ si et seulement si $h=e_{\mathrm{H}}$; ainsi $\ker\pi=\mathrm{N}\times\{e_{\mathrm{H}}\}$.

   Finalement l'application π passe au quotient par son noyau et induit un isomorphisme de groupes :
   $$\overline{\pi}\colon{}^{\mathrm{N}\rtimes_\phi\mathrm{H}}\!\diagup_{\mathrm{N}\times\{e_{\mathrm{H}}\}}\xrightarrow{\sim}\mathrm{H}$$

Exercice 447

Soit G un groupe. Soient N et H deux sous-groupes de G tels que $\mathrm{N} \cap \mathrm{H} = \{e\}$, $\mathrm{G} = \mathrm{NH}$ et $\mathrm{N} \triangleleft \mathrm{G}$.

1. Montrer que l'application
$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$
est un morphisme de groupes.
2. Montrer que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un isomorphisme de groupes.

On dit alors que G est le produit semi-direct de H par N.

Éléments de réponse 447

1. Montrons que l'application
$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$
est un morphisme de groupes.

   L'application i est bien définie car $\mathrm{N} \triangleleft \mathrm{G}$. On vérifie directement que c'est un morphisme de groupes.
2. Montrons que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un morphisme de groupes. Soient n, n' dans N et h, h' dans H. On a
$$f(n,h)f(n',h') = nhn'h'$$
et
$$f\big((n,h) \rtimes_i (n',h')\big) = f\big(ni(h)(n'), hh'\big) = f(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h'$$
ce qui assure que $f\big((n,h) \rtimes_i (n',h')\big) = f(n,h)f(n',h')$. Ainsi f est bien un morphisme de groupes.

   Montrons maintenant que f est un isomorphisme de groupes. L'hypothèse $\mathrm{NH} = \mathrm{G}$ assure que f est surjectif et l'hypothèse $\mathrm{N} \cap \mathrm{H} = \{e\}$ assure que le noyau de f est trivial. Par suite f est un isomorphisme.

Exercice 448

Montrer que le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Éléments de réponse 448

Le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si pour tous n, $n' \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (n',h') = (n', hh')$$

si et seulement si pour tous n, $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $\phi(h)(n') = nn'$ si et seulement si ϕ est le morphisme trivial.

Pour tous $n \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (e_\mathrm{N}, h') \rtimes_\phi (n,h)^{-1} = (n\phi(hh'h^{-1})(n^{-1}), hh'h^{-1}).$$

Ainsi le morphisme ϕ est trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Exercice 449

Soit

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

une suite exacte (courte).

1. Montrer que si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.
2. Réciproquement soit une telle suite exacte. Si p possède une section, c'est-à-dire s'il existe un morphisme de groupes $s\colon \mathrm{H} \to \mathrm{G}$ tel que $p \circ s = \mathrm{id}_\mathrm{H}$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.
3. Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Éléments de réponse 449

1. Supposons que $\mathrm{G} = \mathrm{N} \rtimes_\phi \mathrm{H}$. D'après l'Exercice **??** 3. on dispose d'un morphisme surjectif $\pi\colon \mathrm{G} \to \mathrm{H}$ dont le noyau est le sous-groupe $\mathrm{N} \rtimes_\phi \{e_\mathrm{H}\}$ qui est isomorphe à N. Par suite on a bien une suite exacte

   $$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

   où $i\colon \mathrm{N} \to \mathrm{G}$ est défini par $i(n) = (n, e_\mathrm{H})$. De plus on peut vérifier que l'application

   $$\mathrm{H} \to \mathrm{G} \qquad\qquad h \mapsto (e_\mathrm{N}, h)$$

   est une section de π.

2. C'est une conséquence de l'Exercice **??** appliqué aux sous-groupes $\mathrm{N}' = i(\mathrm{N})$ et $\mathrm{H}' = s(\mathrm{H})$ de G. Il suffit donc de vérifier que N' et G' satisfont les hypothèses de l'Exercice **??**. Le groupe N' est distingué dans G car $\mathrm{N}' = \ker p$. Soit $g \in \mathrm{G}$. Posons $h = s(\pi(g)) \in \mathrm{H}'$. Alors
$$\pi(h) = \pi(s(\pi(g))) = \pi(g)$$
donc $n = gh^{-1}$ appartient à $\ker \pi = \mathrm{N}'$. Finalement nous avons bien $\underbrace{g}_{\in \mathrm{G}} = \underbrace{n}_{\in \mathrm{N}'}\underbrace{h}_{\in \mathrm{H}'}$ ce qui assure que $\mathrm{G} = \mathrm{N}'\mathrm{H}'$. Soit $g \in \mathrm{N}' \cap \mathrm{H}'$. Puisque $g \in \mathrm{H}'$ il existe $h \in \mathrm{H}$ tel que $g = s(h)$. Comme $g \in \mathrm{N}'$ nous avons $\pi(g) = e_{\mathrm{H}}$. Par suite $\pi(s(h)) = e_{\mathrm{H}}$, *i.e.* $h = e_{\mathrm{H}}$, donc $g = s(e_{\mathrm{H}}) = e_{\mathrm{G}}$. Il s'en suit que $\mathrm{N}' \cap \mathrm{H}' = \{e_{\mathrm{G}}\}$. Nous pouvons donc bien appliquer l'Exercice **??** pour conclure.

3. Considérons la suite exacte courte
$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$
où p est la réduction modulo 2. C'est bien une suite exacte courte, en revanche p n'admet pas de section puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2 alors que tous ses antécédents par p sont d'ordre 4. Il s'en suit que $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

   Un autre exemple est donné par le groupe des quaternions $\mathbb{H}_8$ dont le centre $Z(\mathbb{H}_8)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $\mathbb{H}_8/Z(\mathbb{H}_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ce qui fournit une suite exacte
$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$
telle que p n'admet pas de section (on peut par exemple le voir en listant les éléments d'ordre 2 dans $\mathbb{H}_8$). Il en résulte que $\mathbb{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 450

Nous avons vu en cours que
$$\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*.$$
Ces produits semi-directs sont-ils directs ?

Éléments de réponse 450

On peut vérifier que les produits
$$\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$
ne sont pas directs (sauf pour $n = 2$) quelle que soit la section choisie. On peut en fait vérifier qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

Le cas $\mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*$ est moins évident pour $n \geq 2$. Si $x \mapsto x^n$ est un automorphisme de $\Bbbk^*$, on note $a\colon \Bbbk^\times \to \Bbbk^\times$ son inverse. L'application

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto A\mathrm{diag}(a(t),a(t),\dots,a(t))$$

est un isomorphisme.

Réciproquement supposons qu'il existe un isomorphisme de groupes

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto \phi(A)s(t).$$

Le sous-groupe dérivé de $\mathrm{SL}(n,\Bbbk) \times \Bbbk^*$ est $\mathrm{SL}(n,\Bbbk) \times \{1\}$ et celui de $\mathrm{GL}(n,\Bbbk)$ est $\mathrm{SL}(n,\Bbbk)$. Par conséquent ϕ est un automorphisme de $\mathrm{SL}(n,\Bbbk)$. De plus $\alpha(\Bbbk^*) = s(\Bbbk^*)$ commute avec tout élément de $\mathrm{GL}(n,\Bbbk)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}(n,\Bbbk)$ est formé des homothéties). Ainsi l'application $t \mapsto s(t)$ est un morphisme injectif de $\Bbbk^*$ vers $\mathrm{GL}(n,\Bbbk)$ de la forme $t \mapsto \mathrm{diag}(a(t),a(t),\dots,a(t))$.

Le noyau de det étant $\mathrm{SL}(n,\Bbbk)$ on a $a(t)^n = 1$ si et seulement si $a(t) = 1$. Puisque $t \mapsto a(t)$ est injectif, $t \mapsto a(t)^n$ l'est aussi. Or det est surjectif sur $\Bbbk^*$ donc $t \mapsto a(t)^n = a(t^n)$ est bijectif. Il en résulte que $x \mapsto x^n$ est bijectif et donc un automorphisme de $\Bbbk^*$.

Ainsi $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$ si et seulement si le morphisme $(\cdot)^n\colon \Bbbk^* \to \Bbbk^*$ est un automorphisme. En particulier

- si $\Bbbk = \mathbb{R}$ et n est impair, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$;
- si $\Bbbk$ est un corps fini de caractéristique p et si n est égal à une puissance de p, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$.

Exercice 451

Soit $\mathrm{G} = \mathrm{N} \rtimes \mathrm{H}$. Soit K un sous-groupe de G contenant N. Montrer que $\mathrm{K} = \mathrm{N} \rtimes (\mathrm{K} \cap \mathrm{H})$.

Éléments de réponse 451

On va appliquer ce qu'on a vu dans l'Exercice **??** :

— $\mathrm{N} \lhd \mathrm{G}$ et $\mathrm{N} \subset \mathrm{K}$ donc $\mathrm{N} \lhd \mathrm{K}$;

— $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{K} \subset \mathrm{G}$ donc $\mathrm{H} \cap \mathrm{K} \subset \mathrm{K}$;

— $\mathrm{N} \cap \mathrm{H} = \{e\}$ donc $\mathrm{N} \cap (\mathrm{K} \cap \mathrm{N}) = \{e\}$;

— $\mathrm{NH} = \mathrm{G}$ donc si $k \in \mathrm{K}$, alors $k = nh$ avec $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Puisque $\mathrm{N} \subset \mathrm{K}$ nous en déduisons que $h \in \mathrm{H} \cap \mathrm{K}$. D'où $\mathrm{N}(\mathrm{H} \cap \mathrm{K}) = \mathrm{K}$.

Exercice 452

Soient H et N des groupes. Soient φ, $\psi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ soient isomorphes.

1. S'il existe un automorphisme α de H tel que $\psi = \varphi \circ \alpha$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.

2. S'il existe un automorphisme u de N tel que
$$\forall\, h \in \mathrm{H} \qquad \phi(h) = u\psi(h)u^{-1}$$
montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.
3. Si H est cyclique et si $\varphi(\mathrm{H}) = \psi(\mathrm{H})$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.

Éléments de réponse 452

1. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (n, \alpha(h))$$
est un isomorphisme.
2. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (u(n), h)$$
est l'isomorphisme.
3. Le groupe H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{im}\varphi = \operatorname{im}\psi$ est isomorphe à $\mathbb{Z}/m\mathrm{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$
est surjective, il existe $d' \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ qui s'envoie sur d.

   La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait les conditions de 1. d'où le résultat.

Exercice 453

Soit p un nombre premier.

a) Quel est l'ordre d'un p-Sylow de $\mathfrak{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathfrak{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire
$$(p-1)! \equiv -1 \bmod p.$$

Éléments de réponse 453

a) L'ordre de $\mathfrak{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathfrak{S}_p$ est d'ordre p.

b) Une rédaction possible :

Pour déterminer le nombre de p-Sylow de $\mathfrak{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathfrak{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur Z_σ de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in Z_\sigma$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de Z_σ est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathfrak{S}_p$ car $\mathfrak{S}_p/Z_\sigma$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathfrak{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible :

Un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathfrak{S}_p$ [18]. Par ailleurs tout élément d'ordre p de $\mathfrak{S}_p$ vit dans un p-sous-groupe de Sylow ; réciproquement, comme p est premier et qu'un p-sous-groupe de Sylow de $\mathfrak{S}_p$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il existe exactement $p-1$ éléments d'ordre p dans chaque p-sous-groupe de Sylow de $\mathfrak{S}_p$ (puisque dans $\mathbb{Z}/p\mathbb{Z}$ tous les éléments non nuls sont générateurs). Ainsi, il y a $n_p = \frac{(p-1)!}{p-1} = (p-2)!$ p-sous-groupes de Sylow dans $\mathfrak{S}_p$.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 454

Montrer que tout groupe d'ordre 255 est cyclique.

Éléments de réponse 454

Soit G un groupe d'ordre $255 = 3 \times 5 \times 17$. Soit n_3 (respectivement n_5, respectivement n_{17}) le nombre de 3-Sylow (respectivement 5-Sylow, respectivement 17-Sylow) de G. Les théorèmes de Sylow assurent que

$$n_3 \in \{1, 85\}, \qquad n_5 \in \{1, 51\} \qquad n_{17} = 1.$$

On ne peut pas avoir $(n_3, n_5) = (85, 51)$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$.

18. Le nombre de k-cycles dans $\mathfrak{S}_p$ est le nombre d'arrangements de k parmi p divisé par k (car un k-cycle s'écrit de k façons différentes) ce qui donne : $\frac{p!}{k(p-k)!}$

Supposons que $n_3 = 1$ (le cas $n_5 = 1$ se résoud de manière analogue). Notons S_3 le seul 3-Sylow de G, S_{17} le seul 17-Sylow de G et S_5 un 5-Sylow quelconque. Nous avons

— $S_3S_{17} \simeq S_3 \times S_{17} \lhd \mathrm{G}$;

— $S_3S_{17} \cap S_5 = \{e\}$;

— $S_3S_{17}S_5 = \mathrm{G}$.

L'exercice **??** assure que $\mathrm{G} \simeq S_3S_{17} \rtimes S_5$. Soit $\phi\colon S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{16\mathbb{Z}}$ donc ϕ est trivial et le produit semi-direct. On conclut par le lemme chinois.

Exercice 455

Soit p un nombre premier impair.

1. Déterminer les p-Sylow de $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$.
2. Soient ϕ et ψ des morphismes non triviaux de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$. Pour tout entier k notons ϕ_k le morphisme ϕ_k défini par $\phi_k(x) = \phi(kx)$. Montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$ tels que $\psi = P\phi_k P^{-1}$.
3. Montrer qu'il existe un produit semi-direct non trivial $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^2 \rtimes {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.
4. Montrer que le centre de ce dernier groupe est isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. (On rappelle que si G est un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène, alors G est abélien.)
5. Supposons que G est un groupe fini. Notons p le plus petit nombre premier divisant le cardinal de G.

   Montrer que tout sous-groupe de G d'indice p est distingué (indication : commencer par montrer que tout sous-groupe H de G d'indice p agit trivialement sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$, en déduire que H est distingué dans G).
6. Soit G un groupe d'ordre p^3 non cyclique contenant un élément g d'ordre p^2. Montrer que $\langle g \rangle$ est distingué dans G et que G est un produit semi-direct de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ par $\langle g \rangle \simeq {}^{\mathbb{Z}}\!/_{p^2\mathbb{Z}}$.

Éléments de réponse 455

1. Les p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe
$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p \right\}$$
des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ et que tous sont conjugués, une matrice de $\mathrm{GL}(2, \mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre p^2 telles matrices (à la main...) et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). Remarquons que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2. Puisque les images de ψ et φ sont des p-Sylow de $\mathrm{GL}(2,\mathbb{F}_p)$ elles sont conjuguées par une matrice $P \in \mathrm{GL}(2,\mathbb{F}_p)$. Notons

$$\varphi_{(P)} \colon \mathbb{Z}/p\mathbb{Z} \to \psi\left(\mathbb{Z}/p\mathbb{Z}\right) \qquad\qquad x \mapsto P\varphi(x)P^{-1}$$

c'est un isomorphisme. Dès lors $(\varphi_{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, *i.e.* de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

3. Puisque $\mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\right) \simeq \mathrm{GL}(2,\mathbb{F}_p)$ le 1. assure l'existence d'un produit semi-direct non trivial $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

4. Comme le centre d'un p-groupe est non trivial, le centre de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ est d'ordre p, p^2 ou p^3. Si $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ était d'ordre p^2 ou p^3, alors $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ serait abélien (en effet si G est un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est monogène, alors G est abélien) : contradiction avec le fait que le produit semi-direct n'est pas trivial. Il s'en suit que $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

5. Notons p le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de G d'indice p. Posons $X = \mathrm{G}/\mathrm{H}$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi \colon \mathrm{G} \to \mathfrak{S}_X$. Intéressons-nous à la restriction de cette action au sous-groupe H, autrement dit au morphisme $\varphi \colon \mathrm{H} \to \mathfrak{S}_X$. Puisque H agit trivialement sur la classe x_0 de H dans $X = \mathrm{G}/\mathrm{H}$ l'action de H sur X induit une action de H sur $X' = X \smallsetminus \{x_0\}$ c'est-à-dire un morphisme de groupes $\psi \colon \mathrm{H} \to \mathfrak{S}_{X'}$. Or $|X'| = p - 1$ donc tous les facteurs premiers de $|\mathfrak{S}_{X'}|$ sont strictement inférieurs à p. Or les facteurs premiers de $|\mathrm{H}|$ sont par hypothèse tous supérieurs ou égaux à p. Par suite $|\mathrm{H}|$ et $|\mathfrak{S}_{X'}|$ sont premiers entre eux. Le morphisme ψ est donc trivial. Il en résulte que H agit trivialement sur X' et donc aussi sur X.

   Montrons que cela implique que G est distingué dans G. Soit $h \in \mathrm{H}$ et soit $g \in \mathrm{G}$. Puisque H agit trivialement sur X on a $h \cdot (g\mathrm{H}) = g\mathrm{H}$ donc $(g^{-1}hg)\mathrm{H} = \mathrm{H}$, par suite $g^{-1}hg$ appartient à H, *i.e.* H est distingué dans G.

6. Le sous-groupe $\langle g \rangle$ est d'indice p dans un groupe d'ordre p^3. D'après 5. le groupe $\langle g \rangle$ est donc distingué dans G.

   De plus le quotient $\mathrm{G}/\langle g \rangle$ est d'ordre p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

   Soit $y \in \mathrm{G} \smallsetminus \langle g \rangle$. Alors y^p appartient à $\langle g \rangle$ et $y^{p^2} = e$. Il existe donc $k \in \mathbb{Z}$ tel que $y^p = g^{pk}$. Comme $\langle g \rangle$ est distingué dans G il existe un entier $r \geq 0$ tel que $y^{-1}gy = g^r$. Alors pour tout $\ell \in \mathbb{N}$ nous avons $g^\ell y = yg^{\ell r}$. On cherche $z \in \mathrm{G} \smallsetminus \langle g \rangle$ d'ordre p ; plus précisément on cherche $z \in \mathrm{G} \smallsetminus \langle g \rangle$ d'ordre p sous la forme $z = yg^n$. Alors

$$z^p = (yg^n)^p = yg^nyg^n \dots yg^n;$$

une simple récurrence assure que

$$z^p = y^p g^{n(r^{p-1}+r^{p-2}+\ldots+r+1)} = g^{pk+n(r^{p-1}+r^{p-2}+\ldots+r+1)}.$$

Par suite z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + r^{p-2} + \ldots + r + 1) \equiv 0 \mod p^2. \tag{1.10.1}$$

On cherche donc à résoudre (1.17.1) dont l'inconnue est $n \in \mathbb{Z}$. Posons $S := r^{p-1} + r^{p-2} + \ldots + r + 1$. Alors $(r-1)S \equiv r - 1 \bmod p$ donc

— soit $r \not\equiv 1 \bmod p$ et $S \equiv 1 \bmod p$;

— soit $r \equiv 1 \bmod p$ et on vérifie que dans ce cas $S \equiv p \bmod p^2$ (utiliser que p est impair).

Dans les deux cas l'équation (1.17.1) admet une solution $n_0 \in \mathbb{Z}$. Ainsi $z_0 = yg^{n_0} \in \mathrm{G} \smallsetminus \langle g \rangle$ est d'ordre p. Les deux sous-groupes $\mathrm{N} = \langle g \rangle$ et $\mathrm{H} = \langle z \rangle$ satisfont les hypothèses de l'Exercice **??** ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^2\mathbb{Z}$.

1.11. Groupes libres

Exercice 456

Soient r et s deux entiers > 1 premiers entre eux. Quel est l'ordre du groupe de présentation $\langle a \,|\, a^r,\, a^s \rangle$?

Éléments de réponse 456

L'ordre de a est un diviseur de r et s qui sont premiers entre eux donc a est d'ordre 1. Puisque G est engendré par a, le groupe G est d'ordre 1. Ainsi $\mathrm{G} = \{e_\mathrm{G}\}$.

Exercice 457

Soit G le groupe de présentation

$$\langle a,\, b,\, c \,|\, a^3 = b^3 = c^4 = e_\mathrm{G},\, ac = ca^{-1},\, aba^{-1} = bcb^{-1} \rangle.$$

Montrer que $ab^3a^{-1} = bc^3b^{-1}$ puis que $c = e_\mathrm{G}$; en déduire G.

Éléments de réponse 457

Nous avons

$$\begin{aligned} ab^3a^{-1} &= ab(a^{-1}a)b(a^{-1}a)ba^{-1} \\ &= (aba^{-1})(aba^{-1})(aba^{-1}) \\ &= (bcb^{-1})(bcb^{-1})(bcb^{-1}) \\ &= bc(b^{-1}b)c(b^{-1}b)cb^{-1} \\ &= bc^3b^{-1} \end{aligned}$$

Puisque $b^3 = e$, nous avons $ab^3a^{-1} = aa^{-1} = e_\mathrm{G}$. Comme $bc^3b^{-1} = ab^3a^{-1}$ nous obtenons que $bc^3b^{-1} = e_\mathrm{G}$ et que $c^3 = e_\mathrm{G}$. Par suite $c = c^4(c^3)^{-1} = e_\mathrm{G}(e_\mathrm{G})^{-1} = e_\mathrm{G}$.

Puisque $c = e$, la relation $ac = ca^{-1}$ devient $a = a^{-1}$ ou encore $a^2 = e$. Comme $a^3 = e$ nous obtenons $a = e$.

Enfin puisque $a = c = e_{\mathrm{G}}$ la relation $aba^{-1} = bcb^{-1}$ se réduit à $b = e_{\mathrm{G}}$. Comme a, b et c engendrent G nous obtenons $\mathrm{G} = \{e_{\mathrm{G}}\}$.

Exercice 458

Montrer que tout élément non trivial d'un groupe libre est d'ordre infini.

Éléments de réponse 458

Soit G un groupe libre. Soit g un élément non trivial de G. Raisonnons par l'absurde, *i.e.* supposons que g soit d'ordre fini n ; alors $g^n = e$. Or g^n est un mot formé avec les générateurs de G, la relation $g^n = e$ fournit donc une relation entre ces générateurs ce qui contredit le fait que G est un groupe libre.

Exercice 459

Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$x^3 = y^2 = (xy)^2 = 1\,?$$

Quels sont les sous-groupes de G ?

Éléments de réponse 459

Supposons que G ne soit pas trivial. Ceci implique que $x \neq y$ (en effet si $x = y$ alors $x^3 = 1$ se réécrirait $y^3 = 1$ et combiné à $y^2 = 1$ on obtiendrait $x = y = 1$.

L'ordre de x est 3 ; celui de y est 2. Il en résulte que $|\mathrm{G}|$ est un multiple de $2 \times 3 = 6$. Le groupe G contient e, x, x^2, y, xy et xy^2. Montrons qu'il n'y a pas d'autres éléments dans G. Commençons à écrire la table de G en utilisant ces six éléments

	e	x	x^2	y	xy	x^2y
e	e	x	x^2	y	xy	x^2y
x	x	x^2	e	xy	x^2y	y
x^2	x^2	e	x	x^2y	y	xy
y	y	x^2y	xy	e	x^2	x
xy	xy	y	x^2y	x	e	x^2
x^2y	x^2y	xy	y	x^2	x	e

Par suite cette table est complète et le groupe G compte 6 éléments.

Les sous-groupes de G sont

- ◇ le sous-groupe trivial,
- ◇ le groupe G lui-même,
- ◇ un unique (théorème de Sylow) sous-groupe d'ordre 3 : $\langle x \rangle$,

◇ trois sous-groupes d'ordre 2 exactement (théorème de Sylow) : $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$.

Exercice 460

Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$xy^2 = y^3x \qquad\qquad yx^3 = x^2y\,?$$

Éléments de réponse 460

À partir de $xy^2 = y^3x$ nous obtenons

$$y^2 = x^{-1}y^3x \qquad\qquad y^3 = xy^2x^{-1}$$

et

$$y^4 = x^{-1}y^6x \qquad\qquad y^6 = xy^4x^{-1}.$$

Par suite d'une part

$$y^9 = (y^3)^3 = (xy^2x^{-1})^3 = xy^6x^{-1}$$

et d'autre part

$$xy^6x^{-1} = x(y^6)x^{-1} = x(xy^4x^{-1})x^{-1} = x^2y^4x^{-2}.$$

On en déduit que $y^9 = x^2y^4x^{-2}$. De plus

$$y^9 = y^{-1}(y^9)y = y^{-1}(x^2y^4x^{-2})y = y^{-1}(x^2y)y^4(y^{-1}x^{-2})y = y^{-1}(x^2y)y^4(x^2y)^{-1}y$$

Mais $yx^3 = x^2y$ donc

$$y^9 = y^{-1}(x^2y)y^4(x^2y)^{-1}y = y^{-1}(yx^3)y^4(yx^3)^{-1}y = x^3y^4x^{-3}$$

Puisque $y^9 = x^2y^4x^{-2}$ nous obtenons

$$x^2y^4x^{-2} = x^3y^4x^{-3}$$

soit $y^4 = xy^4x^{-1}$. Mais on a vu précédemment que $y^6 = xy^4x^{-1}$ donc $y^4 = y^6$ soit $y^2 = e$. À partir de $xy^2 = y^3x$ on a $y^3 = e$ et finalement $y = e$. De plus $yx^3 = x^2y$ se réécrit $x^3 = x^2$ d'où $x = e$. Finalement G est le groupe trivial.

Exercice 461

Le groupe de FIBONNACCI [19] G est engendré par les éléments a, b, c et d vérifiant les relations

$$ab = c \qquad bc = d \qquad cd = a \qquad da = b.$$

Quel est l'ordre de G ?

Éléments de réponse 461

À partir de $a = cd$ nous obtenons

$$a^2 = acd = cda = cb = ab^2$$

19. Les groupes de FIBONNACCI ont été introduits par John CONWAY en 1965.

d'où $a = b^2$.

De même nous obtenons que $c^2 = b$, $d^2 = c$ et $a^2 = d$.

Par suite

$$d = a^2 = b^4 = c^8 = d^{16}$$

et $d^{15} = e$.

De la même façon nous obtenons que $a^{15} = b^{15} = c^{15} = e$.

A partir de $ab = c$ nous obtenons que $ab = a^4$ d'où $aa^8 = a^4$ et $a^5 = e$. De même $b^5 = c^5 = d^5 = e$. Par conséquent $d = a^2$, $b = a^3$, $c = a^4$ et $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$.

Exercice 462

Exprimer comme produit direct de sous-groupes monogènes le sous-groupe multiplicatif de $\mathbb{Q}^*$ engendré par $\{-6, 6\}$.

Éléments de réponse 462

Le sous-groupe $\mathrm{H} = \langle 6\rangle$ de $\mathrm{G} = \langle 6, -6\rangle \subset \mathbb{Q}^*$ est monogène.

Le groupe ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est monogène engendré par $(-6)\mathrm{H}$.

Le sous-groupe H est distingué dans G : il suffit de vérifier que $(-6) \times 6 \times (-6)^{-1}$ appartient à H ce qui est vrai puisque ce nombre vaut 6

Ainsi G est produit direct de deux groupes monogènes : $\mathrm{G} \simeq \mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Exercice 463

Montrer que le groupe multiplicatif engendré par les matrices

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

est abélien.

Exprimer ce groupe, de deux façons différentes, comme produit direct de sous-groupes monogènes.

Éléments de réponse 463

Soit G le groupe multiplicatif engendré par les matrices

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

On peut vérifier que $AB = BA = -2\mathrm{id}$;

le groupe G est donc abélien. Le sous-groupe $\mathrm{H} = \langle A\rangle$ de G est monogène.

Le groupe ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est monogène engendré par $B\mathrm{H}$.

Notons que $BAB^{-1} = A$; en particulier BAB^{-1} appartient à H et H est un sous-groupe distingué de G.

Il en résulte que G est isomorphe au produit direct des deux groupes monogènes H et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Exercice 464 [Présentation de $\mathfrak{S}_n$]

Montrer que

$$\mathfrak{S}_n = \langle t_1, t_2, \ldots, t_{n-1} \,|\, t_i^2 = 1, (t_i t_{i+1})^3 = 1, [t_i, t_j] = 1 \text{ pour } 2 \leq |i-j| \rangle$$

(Indication : le groupe $\mathfrak{S}_n$ est engendré par (1 2), (2 3), ..., $(n-1\ n)$).

Éléments de réponse 464

Pour $1 \leq i \leq n-1$ posons $t_i = (i\ i+1)$. Le groupe $\mathfrak{S}_n$ est engendré par ces transpositions. Cet ensemble de transpositions vérifie les relations données car une transposition est d'ordre 2, deux transpositions disjointes commutent (et pour les transpositions considérées t_i et t_j sont disjointes si et seulement si $|i-j| > 1$), le produit $t_i t_{i+1}$ est égal au 3-cycles $(i\ i+1\ i+2)$ et est donc d'ordre 3. Par suite

$$\mathfrak{S}_n = \langle t_1, t_2, \ldots, t_{n-1} \,|\, t_i^2 = \mathrm{id}, (t_i t_{i+1})^3 = \mathrm{id}, [t_i, t_j] = \mathrm{id} \text{ pour } |i-j| > 1 \rangle$$

En effet soit H le sous-groupe de $\mathfrak{S}_n$ engendré par les t_i. Le groupe H est distingué dans $\mathfrak{S}_n$ car

$$\sigma t_i \sigma^{-1} = (\sigma(i)\ \sigma(i+1))$$

et toute transposition est dans H : si $|i-k| > 1$,

$$(i\ k) = (k-1\ k)(i\ k)(k-1\ k).$$

Ainsi H contient $\mathcal{A}_n$ car tout sous-groupe distingué non trivial de $\mathfrak{S}_n$ contient $\mathcal{A}_n$.

Mais H contient strictement $\mathcal{A}_n$ car les transpositions ne sont pas des permutations paires. L'indice de $\mathcal{A}_n$ dans $\mathfrak{S}_n$ étant 2 nous obtenons que l'indice de H dans $\mathfrak{S}_n$ est 1. Il s'ensuit que $\mathfrak{S}_n = \mathrm{H}$.

Exercice 465

Rappelons que le groupe des quaternions $\mathbb{H}_8$ est le sous-groupe du groupe des matrices 2×2 inversibles à coefficients complexes engendré par

$$A = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$$

Montrer que ce groupe admet les deux présentations suivantes

$$\langle A, B \,|\, A^2 = B^2 = (AB)^2 \rangle \qquad \langle R, S, T \,|\, R^2 = S^2 = T^2 = RST \rangle.$$

Éléments de réponse 465

On peut vérifier que $A^2 = B^2 = (AB)^2 = -\mathrm{id}$ d'où la première présentation pour $\mathbb{H}_8$ (en effet un groupe qui a cette présentation est d'ordre 8).

Posons $R = A$, $S = B$ et $T = AB$; alors $R^2 = S^2 = -\mathrm{id}$ d'après ce qu'on vient de voir. Par ailleurs $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ donc $T^2 = -\mathrm{id}$. Et $RST = ABAB = (AB)^2 = -\mathrm{id}$ d'où la deuxième présentation proposée.

Exercice 466 [Présentation de $\mathcal{A}_4$]

1. Soient $a = (2\ 3\ 4)$ et $b = (1\ 2)(3\ 4)$ deux éléments de $\mathcal{A}_4$. Montrer que
$$\langle a,\, b \,|\, a^3 = b^2 = (ab)^3 = e\rangle$$
est une présentation de $\mathcal{A}_4$.
2. Donner une seconde présentation de $\mathcal{A}_4$ en utilisant les deux 3-cycles $(2\ 3\ 4)$ et $(1\ 3\ 2)$.

Éléments de réponse 466

1. Rappelons que $\mathcal{A}_4$ est d'ordre 12. Le groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^2 = (ab)^3 = e\rangle$$
est d'ordre 12 ; en effet ses éléments sont
$$e,\ a,\ a^2,\ b,\ ab,\ a^2b,\ ba,\ ba^2,\ aba,\ a^2ba,\ aba^2,\ a^2ba^2.$$
Le morphisme φ de G dans $\mathcal{A}_4$ défini par
$$\varphi(a) = (1\ 2\ 3) \qquad\qquad \varphi(b) = (1\ 2)(3\ 4)$$
réalise un isomorphisme entre G et $\mathcal{A}_4$.
2. Posons $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2)$; alors $\alpha\beta = (1\ 4\ 2)$ et
$$\alpha^3 = \mathrm{id} \qquad\qquad \beta^3 = \mathrm{id} \qquad\qquad (\alpha\beta)^3 = \mathrm{id}$$
On peut vérifier que le groupe G de présentation
$$\langle \alpha,\, \beta,\, |\, \alpha^3 = \beta^3 = (\alpha\beta)^3 = e\rangle$$
est d'ordre 12. On en déduit que G et $\mathcal{A}_4$ sont isomorphes.

Exercice 467 [Présentation de $\mathfrak{S}_4$]
Nous allons montrer que le groupe $\mathfrak{S}_4$ est isomorphe au groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^4 = (ab)^2 = e\rangle.$$
1. En utilisant les éléments $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2\ 4)$ de $\mathfrak{S}_4$ montrer qu'il existe un morphisme de G sur $\mathfrak{S}_4$. Désignons par H le sous-groupe de G engendré par a et b^2.
2. Montrer que bab^{-1} est un élément de H ; en déduire que H est un sous-groupe distingué de G.
3. Montrer que G/H a au plus deux éléments : les classes H et bH.
4. Montrer que $(ab^2)^3 = e$.
5. Conclure en utilisant la présentation de $\mathcal{A}_4$ obtenue précédemment.

Éléments de réponse 467

1. Remarquons que les permutations α et β considérées vérifient les relations
$$\alpha^3 = \mathrm{id}, \qquad \beta^4 = \mathrm{id}, \qquad (\alpha\beta)^2 = \mathrm{id}.$$
Il existe donc un morphisme φ de G sur $\mathfrak{S}_4$ qui envoie a sur α et b sur β. C'est de plus un morphisme injectif.
2. Nous avons
$$bab^{-1} = bab^3 = (bab)b^2, \qquad bab = a^{-1} = a^2.$$
Donc $bab^{-1} = a^2b^2$ appartient à H. Puisque G est engendré par a et b, cette relation implique que H est distingué dans G.
3. Puisque G est engendré par a et b, G/H est engendré par aH et bH, donc par bH car aH = H. Or b^2H = H donc G/H contient au plus les deux éléments H et bH.
4. Nous avons $abba = b^3a^2a^2b^3 = b^3ab^3$ car $ab = b^{-1}a^{-1} = b^3a^2$ et $ba = a^{-1}b^{-1} = a^2b^3$. Il en résulte que
$$(ab^2)^3 = abbabbabb = b^3ab^3b^2ab^2 = b^3abab^2 = b^3(abab)b = b^4 = e.$$
5. Le sous-groupe H de G a pour présentation
$$\langle a,\, c \,|\, a^3 = c^2 = (ac)^3 \rangle$$
(poser $c = b^2$). Les groupes H et $\mathcal{A}_4$ ont même présentation et $\varphi(\mathrm{H}) \subset \mathcal{A}_4$ donc $\varphi(\mathrm{H}) = \mathcal{A}_4$; en particulier H et $\mathcal{A}_4$ sont isomorphes. Le sous-groupe H est d'indice 2 dans G et $\mathcal{A}_4$ est d'indice 2 dans $\mathfrak{S}_4$. Ainsi $|\mathrm{G}| = |\mathfrak{S}_4|$. Finalement φ est un morphisme injectif de G dans $\mathfrak{S}_4$ et $|\mathrm{G}| = |\mathfrak{S}_4|$ donc φ réalise un isomorphisme entre G et $\mathfrak{S}_4$.

Exercice 468 [Présentation d'un produit semi-direct de groupes cycliques]

Notation : $[a]_m$ désigne un élément de $\mathbb{Z}/m\mathbb{Z}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq m-1$. De même $[a]_n$ désigne un élément de $\mathbb{Z}/n\mathbb{Z}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq n-1$.

Soient m, n des entiers ≥ 2 et
$$\tau \colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$$
un morphisme. Désignons par G le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\tau \mathbb{Z}/m\mathbb{Z}$ défini par τ.

Posons
$$[i]_n = \tau([1]_m)([1]_n) \qquad h = ([1]_n, [0]_m) \qquad k = ([0]_n, [1]_m).$$
Vérifions que
$$i^m \equiv 1 (\mathrm{mod\ n}) \qquad h^n = k^m = ([0]_n, [0]_m) \qquad khk^{-1} = h^i.$$
En déduire que G admet pour présentation
$$\langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i \rangle.$$

Éléments de réponse 468

Un morphisme $\tau\colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est entièrement déterminé par l'image $\tau([1]_m)$ de $[1]_m$ dans $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Cette image est elle-même déterminée par l'image de $[1]_n$ par $\tau([1]_m)$. Par suite un morphisme $\tau\colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est entièrement déterminé par $[i]_n = \tau([1]_m)([1]_n)$. Comme $[1]_m$ est d'ordre m, on a $\tau([1]_m)^m = \mathrm{id}$. Ainsi $i^m \equiv 1 \pmod{n}$.

Clairement $h^n = k^m = ([0]_n, [0]_m)$. L'inverse de k dans G est $k^{-1} = ([0]_n, [m-1]_m)$. Il en résulte que

$$\begin{aligned} hk^{-1} &= ([1]_n, [0]_m)([0]_n, [m-1]_m) \\ &= ([1]_n + \tau([0]_m)([0]_n), [m-1]_m) \\ &= ([1]_n, [m-1]_m) \end{aligned}$$

et donc que

$$\begin{aligned} khk^{-1} &= ([0]_n, [1]_m)([1]_n, [m-1]_m) \\ &= ([0]_n + \tau([1]_m)([1]_n), [0]_m) \\ &= ([i]_n, [0]_m) \end{aligned}$$

En particulier $khk^{-1} = h^i$.

Le groupe G est engendré par $a = h$ et $b = k^{-1}$ qui vérifient $a^n = b^b a^i$. Une présentation de G est la suivante

$$\mathrm{G} = \langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i \rangle.$$

1.12. Représentations linéaires des groupes finis

Exercice 469

Montrer que tout groupe fini G admet une représentation fidèle sur tout corps $\Bbbk$.

Éléments de réponse 469

Première réponse possible : la représentation régulière de G sur $\Bbbk$ répond à la question.

Deuxième réponse possible : le théorème de Cauchy assure que G se plonge dans le groupe des permutations de G et ce dernier groupe se plonge dans un groupe linéaire via les matrices de permutations.

Exercice 470

Montrer que si G est un groupe d'ordre fini n, si ρ est une représentation de G sur $\mathbb{C}$, alors pour tout g dans G $\rho(g)$ est diagonalisable et son spectre est inclus dans μ_n.

Éléments de réponse 470

Soit G un groupe d'ordre fini n. Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie, une représentation de G.

Soit g un élément de G. L'ordre de g divise n ; en particulier g est d'ordre fini. L'automorphisme $\rho(g)$ est d'ordre fini puisque g l'est, *i.e.* il existe un entier k tel que $\rho(g)^k = \mathrm{Id}_V$. Alors :

$$X^k - 1 = \prod_{j=0}^{k-1} (X - \zeta^j) \in \mathbb{C}[X]$$

où ζ est une racine primitive $k$ième de l'unité, est un polynôme annulateur de $\rho(g)$ scindé à facteurs simples ; $\rho(g)$ est donc diagonalisable et ses valeurs propres sont les racines $k$ième de l'unité.

Exercice 471

Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrer que $\rho \circ \pi$ est une représentation de G.

b) Montrer que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

Éléments de réponse 471

Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrons que $\rho \circ \pi$ est une représentation de G.

La composée de deux morphismes de groupes étant un morphisme de groupes, $\rho \circ \pi$ est une représentation de G.

b) Montrons que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

- Commençons par montrer que si $\rho \circ \pi$ est irréductible alors ρ l'est.

  Plus généralement si $f\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes et si ρ est une représentation de G′, on a l'implication suivante

  si $\rho \circ f$ est irréductible (comme représentation) de G, alors ρ est irréductible.

  En effet tout sous-espace stable par G′ est stable par G puisque l'action de G se factorise par G′.

- Montrons que si ρ est irréductible, alors $\rho \circ \pi$ est irréductible.

  Soit W un sous-espace strict stable par G. Pour tout $\overline{x} \in {}^{\mathrm{G}}\!/_{\mathrm{H}}$ il existe $g \in \mathrm{G}$ tel que $\pi(g) = \overline{x}$ (ρ est surjective, si elle ne l'était pas l'implication serait fausse). Comme W est stable par g, il est stable par $\overline{x}$. Ainsi W est stable par tout élément de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. La représentation ρ étant irréductible $W = 0$ et $\rho \circ \pi$ est irréductible.

Exercice 472

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}(n, \mathbb{C})$ est le groupe des homothéties. Soit ρ l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$.

a) Montrer que la représentation ρ est irréductible.

b) Montrer que tout élément du centre de $\mathrm{GL}(n, \mathbb{C})$ est un morphisme de la représentation ρ.

c) Conclure en utilisant le Lemme de Schur.

Éléments de réponse 472

Puisque ρ est l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}(n, \mathbb{C})$ dans $\mathrm{GL}(n, \mathbb{C})$.

a) Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}(n, \mathbb{C})$, alors il est évident que $V = \{0\}$ ou $V = \mathbb{C}^n$, c'est-à-dire que ρ est irréductible.

b) Soit h un élément du centre de $\mathrm{GL}(n, \mathbb{C})$. Donc pour tout $M \in \mathrm{GL}(n, \mathbb{C})$ on a $\rho(M) \circ h = Mh = hM = h \circ \rho(M)$, donc h est bien un morphisme de la représentation ρ.

c) Comme ρ est irréductible, d'après le Lemme de Schur, on a $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, c'est-à-dire que h est une homothétie.

Exercice 473

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Soit G un groupe abélien.

a) Si $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ est une représentation de G, montrer que tout élément g de G définit un G-morphisme $V \to V$.

b) En déduire que toute représentation irréductible de G est de dimension 1.

c) Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 473

Comme souvent on note $g \cdot x$ pour $\rho(g)(x)$.

a) Pour tous g, h, $x \in \mathrm{G}$, nous avons

$$g \cdot (h \cdot x) = (gh) \cdot x = (hg) \cdot x = h \cdot (g \cdot x)$$

c'est-à-dire l'application $\rho(g)\colon x \mapsto g \cdot x$ est un G-morphisme pour tout $g \in \mathrm{G}$.

b) On suppose que V est une représentation irréductible de G. Si $g \in \mathrm{G}$, alors d'après la question précédente et le Lemme de Schur, $\rho(g) = \lambda \mathrm{id}$. De plus, comme $\rho(g) \in \mathrm{GL}(V)$, on a $\lambda \neq 0$. Donc tout sous-espace vectoriel de V est stable par G, et est donc une sous-représentation de G. Comme V est irréductible, on a nécessairement $\dim(V) = 1$.

c) D'après la question précédente, une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes $\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*$. Comme tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n, l'élément $\rho(k)$ sera aussi d'ordre divisant n, c'est-à-dire $\rho(k)^n = 1$. Réciproquement, pour toute racine $n$ème de l'unité ω, l'application

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$

est une représentation de $\mathbb{Z}/n\mathbb{Z}$, donc on les obtient toutes ainsi. On voit ainsi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 474

Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V,ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrer que (V,ρ) est isomorphe à la représentation régulière de G.

Éléments de réponse 474

Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V,ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrons que (V,ρ) est isomorphe à la représentation régulière de G.

Soit W un espace vectoriel de base $\{e_j\}_{g\in\mathrm{G}}$; prendre par exemple $W = \mathbb{C}^G$ et $e_g =$ indicatrice de g. Rappelons que la représentation régulière ρ_R de G opère sur W par

$$\rho_R(h)(e_g) = e_{hg}$$

Considérons l'application linéaire ϕ définie sur la base (e_g) oar

$$\phi\colon W \to V, \qquad e_g \mapsto \rho(g)v$$

Puisque par hypothèse $(\rho(g)(v))_{g\in\mathrm{G}}$ est une base de V ϕ est un isomorphisme de $\mathbb{C}$-espaces vectoriels. Par définition ϕ est G-équivariante, *i.e.* $\phi \circ \rho_R(g) = \rho(g) \circ \phi$. En effet d'une part

$$(\phi \circ \rho_R(g))(e_h) = \phi(e_{gh}) = \rho(gh)(v)$$

et d'autre part

$$(\rho(g) \circ \phi)(e_h) = \rho(g)(\phi(e_h)) = \rho(g)(\rho(h)(v)) = \rho(gh)(v)$$

Ainsi ϕ est un isomorphisme entre ρ et ρ_R.

Exercice 475

Soit $\mathrm{G} = \mathfrak{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrer que T est une représentation de G.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad\qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrer que W est une sous-G-représentation de V. W est-il irréductible ?

c) Déterminer la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Éléments de réponse 475

Soit $\mathrm{G} = \mathfrak{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrons que T est une représentation de G.

T est un morphisme de G dans $\mathrm{GL}(V)$: soient g et g' dans G on a d'une part

$$T(gg')(e_\tau) = e_{(gg')\tau(gg')^{-1}} = e_{gg'\tau g'^{-1}g^{-1}}$$

et d'autre part

$$T(g) \circ T(g')(e_\tau) = T(g)(e_{g'\tau g'^{-1}}) = e_{gg'\tau g'^{-1}g^{-1}}$$

d'où $T(gg') = T(g) \circ T(g')$.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad\qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrons que W est une sous-G-représentation de V.

Le groupe $\mathfrak{S}_3$ est engendré par (1 2) et (1 2 3). Il suffit donc de montrer que l'espace engendré par α et β est stable par $T((1\ 2))$ et $T((1\ 2\ 3))$. Un calcul montre que

$$T((1\ 2))(\alpha) = \beta, \qquad T((1\ 2\ 3))(\alpha) = j\alpha, \qquad T((1\ 2))(\beta) = \alpha, \qquad T((1\ 2\ 3))(\beta) = j^2\beta$$

W est-il irréductible ?

Un calcul montre qu'aucun sous-module de W de dimension 1 n'est stable par $\mathfrak{S}_3$ donc W est irréductible.

c) Déterminons la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Remarquons que si C est une classe de conjugaison dans $\mathfrak{S}_3$, alors $\sum_{g\in C} e_g$ est stable par T (c'est par définition même de T). On trouve ainsi trois sous-espaces stables sous $\mathfrak{S}_3$ qui sont les droites

$$W_1 = \mathbb{C}\mathrm{id}, \qquad W_2 = \mathbb{C}(e_{(1\ 2)} + e_{(1\ 3)} + e_{(2\ 3)}), \qquad W_3 = \mathbb{C}(e_{(1\ 2\ 3)} + e_{(1\ 3\ 2)})$$

Enfin si on note sgn la signature on obtient

$$T(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) = \mathrm{sgn}(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$$

En effet d'une part

$$\begin{aligned} T((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2)(1\ 2\ 3)(1\ 2)} - e_{(1\ 2)(1\ 3\ 2)(1\ 2)} \\ &= e_{(1\ 3\ 2)} - e_{(1\ 2\ 3)} \\ &= -(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

d'autre part

$$\begin{aligned} T((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3)^{-1}} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)^{-1}} \\ &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 3\ 2)} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 3\ 2)} \\ &= (e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

L'espace $W_4 = \mathbb{C}(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$ est donc stable par $\mathfrak{S}_3$.

On a finalement $V = W_1 \oplus W_2 \oplus W_3 \oplus W_4 \oplus W$ où W désigne l'unique représentation irréductible de dimension 2.

Exercice 476

Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrer que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Éléments de réponse 476

Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrons que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Le groupe G admet un sous-groupe distingué H d'indice p. Par conséquent ${}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Le corps $\Bbbk$ est algébriquement clos de caractéristique $\neq p$. Par suite le polynôme $X^p - 1$ est scindé à racines simples. Ainsi les racines p-ième de l'unité dans $\Bbbk^*$ forment un sous-groupe cyclique d'ordre p isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ d'où une injection de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\Bbbk^*$. Le morphisme

$$\mathrm{G} \longrightarrow {}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \longrightarrow \Bbbk^*$$

est donc une représentation non triviale de dimension 1 de G sur $\Bbbk$.

Exercice 477

Soit G un groupe fini et soit χ le caractère d'une représentation ρ de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrer que χ est un multiple entier du caractère de la représentation régulière de G.

Éléments de réponse 477

Soit G un groupe fini et soit χ le caractère d'une représentation ρ de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrons que χ est un multiple entier du caractère de la représentation régulière de G.

Rappel : le caractère de la représentation régulière est donné par

$$\chi_{\rho_R}(g) = \begin{cases} |\mathrm{G}| \text{ si } g = e \\ 0 \text{ sinon} \end{cases}$$

Il suffit de montrer que $|\mathrm{G}|$ divise $\chi(e)$. Notons χ_{triv} le caractère de la représentation triviale de G. On a

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi(g) \overline{\chi_{\mathrm{triv}}(g)}$$

Comme $\chi(g) = 0$ pour tout $g \neq e$ on a $\displaystyle\sum_{g \in \mathrm{G}} \chi(g)\overline{\chi_{\mathrm{triv}}(g)} = \chi(e)\overline{\chi_{\mathrm{triv}}(e)} = \chi(e)$ autrement dit

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|}\chi(e)$$

et

$$|\mathrm{G}|\langle \chi, \chi_{\mathrm{triv}} \rangle = \chi(e).$$

Remarquons

- ◇ d'une part que $\chi(e)$ est un entier : pour toute représentation ρ nous avons $\chi_\rho(e) = \mathrm{tr}(\rho(e)) = \mathrm{tr}(\mathrm{id}_{\mathrm{GL}(V)}) = \dim V$;
- ◇ d'autre part que $\langle \chi, \chi_{\mathrm{triv}} \rangle$ est un entier : la représentation ρ s'écrit $\rho = \oplus \rho_i^{n_i}$ où les ρ_i désignent les représentations irréductibles de G et les n_i des entiers naturels uniquement déterminés par ρ. Quitte à réindicer les ρ_i on peut supposer $\rho_1 = \rho_{\mathrm{triv}}$, *i.e.* $\rho = \rho_{\mathrm{triv}}^{n_1} \oplus \Big(\bigoplus_i \rho_i^{n_i}\Big)$. Ainsi $\langle \chi, \chi_{\mathrm{triv}} \rangle = n_1 \in \mathbb{N}$.

Il en résulte que χ est un multiple entier du caractère de la représentation régulière de G.

Exercice 478

Décrire les représentations irréductibles du groupe $\mathrm{GL}(3, \mathbb{F}_2)$ et écrire sa table de caractères.

Éléments de réponse 478

Exercice 479

a) Décrire les représentations irréductibles du groupe diédral D_{2n} et écrire sa table de caractères.

b) Déterminer les sous-groupes distingués de D_8 à l'aide de sa table de caractères.

Éléments de réponse 479

Exercice 480

Soit $\mathbb{H}_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions. Ecrire la table de caractères de $\mathbb{H}_8$ et décrire les représentations irréductibles.

Indication : On rappelle que $\mathbb{H}_8$ s'identifie à un sous-groupe de $\mathrm{SU}(2,\mathbb{C})$ en posant : $I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ et $K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Éléments de réponse 480

On peut vérifier que $\mathbb{H}_8$ admet cinq classes de conjugaison qui sont

$$\{1\}, \quad \{-1\}, \quad \{\pm i\}, \quad \{\pm j\}, \quad \{\pm k\}$$

Le groupe dérivé $D(\mathbb{H}_8)$ de $\mathbb{H}_8$ est donné par : $D(\mathbb{H}_8) = \{\pm 1\}$. Par conséquent a

$$\mathbb{H}_8/D(\mathbb{H}_8) = \langle \bar{i}, \bar{j} \,|\, \bar{i}^2 = \bar{j}^2 = 1, \bar{i}\bar{j} = \bar{j}\bar{i} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ainsi $\mathbb{H}_8$ admet quatre représentations de dimension 1 correspondant aux quatre morphismes de groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^*$. Il s'en suit que la cinquième représentation irréductible de $\mathbb{H}_8$ est de dimension 2. Son caractère se déduit des caractères praécédents par orthogonalité.

La table des caractères de $\mathbb{H}_8$ est

$\mathbb{H}_8$	1	1	2	2	2
	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_3 = \chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

Notons que les tables de $\mathbb{H}_8$ et D_8 sont les mêmes. La table de caractères ne détermine donc pas la classe d'isomorphisme d'un groupe fini.

Exercice 481

Décrire les représentations irréductibles du groupe symétrique $\mathfrak{S}_3$ et écrire sa table de caractères.

Éléments de réponse 481

Les classes de conjugaison de $\mathfrak{S}_3$ sont (Proposition **??**)

$$C_1 = \{\mathrm{id}\}, \qquad C_2 = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}, \qquad C_3 = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Ainsi $\mathfrak{S}_3$ a trois représentations irréductibles à équivalence près. Il y a la représentation triviale ρ_{triv} qui est irréductible. On a aussi la représentation signature

$$\mathrm{sgn}\colon \mathfrak{S}_3 \to \mathrm{GL}(1,\mathbb{C}) \simeq \mathbb{C}^*, \qquad \sigma \mapsto \mathrm{sgn}(\sigma)$$

qui est de degré 1 ; elle est irréductible car

$$\langle \chi_{\mathrm{sgn}}, \chi_{\mathrm{sgn}} \rangle = \frac{1}{6}\Big(\underbrace{1}_{\#C_1} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((\mathrm{id}))} \times \overline{1} + \underbrace{3}_{\#C_2} \times \underbrace{(-1)}_{\chi_{\mathrm{sgn}}((1\ 2))} \times \overline{(-1)} + \underbrace{2}_{\#C_3} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((1\ 2\ 3))} \times \overline{1} \Big) = 1$$

Enfin on a la représentation décrite dans l'Exemple **??** dite représentation standard et notée ρ_S. Notons que

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = 1^2 + 1^2 + 2^2 = 6$$

autrement dit $(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = |\mathfrak{S}_3|$.

Ainsi la table de caractères de $\mathfrak{S}_3$ est

	C_1	C_2	C_3
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1
sgn	1	-1	1
χ_{ρ_S}	2	0	-1

A noter que les colonnes sont bien orthogonales.

Exercice 482 [Table de caractères du groupe symétrique $\mathfrak{S}_4$]

a) Décrire les représentations irréductibles de $\mathfrak{S}_4$ et dresser sa table des caractères.

b) Déterminer les sous-groupes distingués de $\mathfrak{S}_4$ à partir de sa table des caractères.

c) On rappelle que $\mathfrak{S}_4$ s'identifie au groupe des isométries directes d'un cube (ou d'un octaèdre) et également au groupe des isométries (directes et indirectes) d'un tétraèdre. Que pensez-vous des représentations de dimension 3 associées ?

Éléments de réponse 482

Le groupe symétrique $\mathfrak{S}_4$ possède cinq classes de conjugaison (Proposition **??**) :

$$\begin{aligned}
C_1 &= \{\mathrm{id}\},\\
C_2 &= \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\},\\
C_3 &= \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},\\
C_4 &= \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\},\\
C_5 &= \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}.
\end{aligned}$$

Il y a donc cinq représetntations irréductibles à équivalence près. On peut déjà donner deux représentations de degré 1

- ◇ la représentation triviale ρ_{triv} ;
- ◇ la représentation signature sgn.

Intéressons-nous à la représentation par permutations. Notons $\mathcal{B} = (e_1, e_2, e_3, e_4)$ la base canonique de $\mathbb{C}^4$. On définit la représentation par permutations par

$$\rho_P \colon \mathfrak{S}_4 \to \mathrm{GL}(\mathbb{C}^4) \qquad\qquad \sigma \mapsto (e_i \mapsto e_{\sigma(i)}).$$

Cette représentation laisse stable $\mathrm{Vect}(1,1,1,1)$ dont

$$H = \{x = (x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$$

est un supplémentaitre stable. Elle induit une représentation ρ_S appelée représentation standard sur H. Comme ρ_P induit la représentation triviale sur $\mathrm{Vect}(1,1,1,1)$ nous avons la relation $\chi_{\rho_P} = \chi_{\rho_{\mathrm{triv}}} + \chi_{\rho_S}$. Reste à savoir si χ_{ρ_S} est irréductible, *i.e.* si $\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle = 1$. Mais $\chi_{\rho_P}(\sigma)$ est le nombre de 1 sur la diagonale de la matrice de permutations σ, c'est-à-dire le nombre de points fixes de σ (Exemple **??**). Ainsi

$$\chi_{\rho_P}(\mathrm{id}) = 4, \quad \chi_{\rho_P}((1\ 2)) = 2, \quad \chi_{\rho_P}((1\ 2)(3\ 4)) = 0, \quad \chi_{\rho_P}((1\ 2\ 3)) = 1, \quad \chi_{\rho_P}((1\ 2\ 3\ 4)) = 0$$

(en effet $\mathrm{Fix}(\mathrm{id}) = \{1, 2, 3, 4\}$, $\mathrm{Fix}((1\ 2)) = \{3, 4\}$, $\mathrm{Fix}((1\ 2)(3\ 4)) = \emptyset$, $\mathrm{Fix}((1\ 2\ 3)) = \{4\}$ et $\mathrm{Fix}((1\ 2\ 3\ 4)) = \emptyset$) d'où (puisque $\chi_{\rho_S}(g) = \chi_{\rho_P}(g) - \chi_{\rho_{\mathrm{triv}}}(g) = \chi_{\rho_P}(g) - 1$)

$$\chi_{\rho_S}(\mathrm{id}) = 3, \quad \chi_{\rho_S}((1\ 2)) = 1, \quad \chi_{\rho_S}((1\ 2)(3\ 4)) = -1, \quad \chi_{\rho_S}((1\ 2\ 3)) = 0, \quad \chi_{\rho_S}((1\ 2\ 3\ 4)) = -1.$$

Il en résulte que

$$\begin{aligned}
\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle &= \frac{1}{|\mathfrak{S}_4|}\Big(1 \times 3 \times \overline{3} + 6 \times 1 \times \overline{1} + 3 \times (-1) \times \overline{(-1)} + 8 \times 0 \times \overline{0} + 6 \times (-1) \times \overline{(-1)}\Big)\\
&= \frac{1}{24}(9 + 6 + 3 + 6)
\end{aligned}$$

Nous en déduisons que ρ_S est une représentation irréductible de degré 3. Nous la notons ρ_4.

Déterminons les deux autres représentations irréductibles de $\mathcal{A}_4$ notées ρ_3 et ρ_5. Commençons par déterminer leurs degrés : l'identité

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_3^2)^2 + (\deg \rho_4^2)^2 + (\deg \rho_5^2)^2 = |\mathfrak{S}_4|$$

conduit à

$$24 - (\deg \rho_{\mathrm{triv}})^2 - (\deg \mathrm{sgn})^2 - (\deg \rho_4)^2 = (\deg \rho_3)^2 + (\deg \rho_5)^2$$

soit $13 = (\deg\rho_3)^2 + (\deg\rho_5)^2$. Nous en déduisons que $\{\deg\rho_3, \deg\rho_5\} = \{2, 3\}$.

Considérons la représentation

$$\rho_5 \colon \mathfrak{S}_4 \to \mathrm{GL}(H), \qquad \sigma \mapsto \mathrm{sgn}(\sigma)\rho_4(\sigma).$$

Alors $\chi_{\rho_5} = \mathrm{sgn}\chi_{\rho_4}$ d'où

$$\begin{aligned}
&\chi_{\rho_S}(\mathrm{id}) = 1 \times 3 = 3, && \chi_{\rho_S}((1\ 2)) = (-1) \times 1 = -1,\\
&\chi_{\rho_S}((1\ 2)(3\ 4)) = 1 \times (-1) = -1, && \chi_{\rho_S}((1\ 2\ 3)) = 1 \times 0 = 0,\\
&\chi_{\rho_S}((1\ 2\ 3\ 4)) = (-1) \times (-1) = 1.
\end{aligned}$$

En particulier

$$\langle\chi_{\rho_5}, \chi_{\rho_5}\rangle = \frac{1}{24}\Big(1{\times}3{\times}3{+}6{\times}(-1){\times}(-1){+}3{\times}(-1){\times}(-1){+}8{\times}0{\times}0{+}6{\times}1{\times}1\Big) = \frac{1}{24}\Big(9{+}6{+}3{+}6\Big) = 1.$$

Il s'ensuit que ρ_5 est irréductible. De plus $\deg\rho_5 = \dim H = 3$.

Remarque — On peut donner une interprétation géométrique de ρ_5 : c'est la représentation de $\mathfrak{S}_4$ comme $\mathrm{Isom}^+(C_6)$ (Proposition **??**).

Commençons à écrire la table de caractères de $\mathfrak{S}_4$:

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	?	?	?	?
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

où $C(g)$ désigne la classe de conjugaison de $g \in \mathfrak{S}_4$.

En utilisant que les colonnes de la table de $\mathfrak{S}_4$ sont orthogonales nous obtenons

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	0	2	-1	0
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

Rappelons que les sous-groupes distingués de $\mathfrak{S}_4$ sont les intersections $\bigcap_{i\in I}\ker\chi_{\rho_i}$ où $I\subset$ [triv, sgn, 3, 4, 5]. La table des caractères de $\mathfrak{S}_4$ assure que

$$\begin{aligned}
&\ker\chi_{\rho_{\text{triv}}}=\mathfrak{S}_4\\
&\ker\chi_{\rho_{\text{sgn}}}=\{\text{id},\,C((1\ 2)(3\ 4)),\,C(1\ 2\ 3)\}=\mathcal{A}_4\\
&\ker\chi_{\rho_3}=\{\text{id},\,C((1\ 2)(3\ 4))\}\simeq\mathcal{K}\\
&\ker\chi_{\rho_4}=\{\text{id}\}\\
&\ker\chi_{\rho_5}=\{\text{id}\}
\end{aligned}$$

Par suite les sous-groupes distingués de $\mathfrak{S}_4$ sont

$$\mathfrak{S}_4,\qquad \{\text{id}\},\qquad \mathcal{A}_4,\qquad \{\text{id},\,(1\ 2)(3\ 4),\,(1\ 3)(2\ 4),\,(1\ 4)(2\ 3)\}\simeq\mathcal{K}$$

(on rappelle que $\mathcal{K}$ désigne le groupe de Klein).

Explicitons ρ_3. Nous avons la décomposition en produit semi-direct

$$\mathfrak{S}_4\simeq\mathcal{K}\rtimes\mathfrak{S}_3.$$

À cette décomposition correspond un morphisme surjectif de groupes

$$\pi\colon\mathfrak{S}_4\to{}^{\mathfrak{S}_4}\!/_{\mathcal{K}}\simeq\mathfrak{S}_3$$

d'où par composition avec la représentation standard $\widetilde{\rho_S}$ de $\mathfrak{S}_3$ une représentation de degré 2

$$\rho_3\colon\mathfrak{S}_4\xrightarrow{\pi}\mathfrak{S}_3\xrightarrow{\widetilde{\rho_S}}\mathrm{GL}(\widetilde{H})$$

où $\widetilde{H}$ désigne l'hyperplan de $\mathbb{C}^3$ d'équation $x_1+x_2+x_3=0$, $\mathcal{B}=(e_1,e_2,e_3)$ la base canonique de $\mathbb{C}^3$ et $\widetilde{\rho_S}\colon\mathfrak{S}_3\to\mathrm{GL}(\widetilde{H})$ la représentation standard de $\mathfrak{S}_3$ induite par la représentation par permutation

$$\widetilde{\rho_P}\colon\mathfrak{S}_3\to\mathrm{GL}(\mathbb{C}^3),\qquad\qquad \sigma\mapsto(e_i\mapsto e_{\sigma(i)}).$$

Pour tout σ dans $\mathfrak{S}_4$ nous avons

$$\chi_{\rho_3}(\sigma)=\chi_{\widetilde{\rho_S}}(\pi(\sigma))$$

soit

$$\begin{aligned}
&\chi_{\rho_3}(\text{id})=2\\
&\chi_{\rho_3}((1\ 2))=0\\
&\chi_{\rho_3}((1\ 2)(3\ 4))=2\\
&\chi_{\rho_3}((1\ 2\ 3))=-1\\
&\chi_{\rho_3}((1\ 2\ 3\ 4))=\chi_{\rho_3}((1\ 4)(1\ 2\ 3))=0
\end{aligned}$$

De plus

$$\langle\chi_{\rho_3},\,\chi_{\rho_3}\rangle=\frac{1}{24}\Big(1\times2\times2+6\times0\times0+3\times2\times2+8\times(-1)\times(-1)+6\times0\times0\Big)=\frac{1}{24}\Big(4+12+8\Big)=1$$

autrement dit χ_{ρ_3} est irréductible.

Exercice 483

Déterminer, à isomorphisme près, le groupe dont la table des caractères est :

	e	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Éléments de réponse 483

Exercice 484

Décrire les représentations irréductibles du groupe $\mathcal{A}_4$ et écrire sa table de caractères.

Éléments de réponse 484

Nous allons établir la table des caractères de $\mathcal{A}_4$. Il y a plusieurs façons d'arriver au résultat. La manière la plus systématique consiste à déterminer les classes de conjugaison de $\mathcal{A}_4$, construire toutes les représentations irréductibles de $\mathcal{A}_4$ et calculer la valeur de leurs caractères sur les classes de conjugaison. C'est ce que nous allons faire avant de montrer que certains des résultats démontrés précédemment permettent quelques raccourcis.

a) Désignons par t le 3-cycle (1 2 3). Notons que $t^2 = (1\ 3\ 2)$ et que comme t est d'ordre 3, le sous-groupe $\mathrm{T} = \langle t \rangle = \{\mathrm{id}, t, t^2\}$ de $\mathcal{A}_4$ engendré par t est d'ordre 3.

b) Le sous-groupe $\mathrm{H} = \{\mathrm{id}, s_2, s_3, s_4\}$ de $\mathcal{A}_4$ est abélien et distingué dans $\mathcal{A}_4$. En effet un 2-Sylow de $\mathcal{A}_4$ est d'ordre 4 et comme H est d'ordre 4 et contient tous les éléments de $\mathcal{A}_4$ d'ordre divisant 4 cela montre qu'il n'y a qu'un seul 2-Sylow qui est par conséquent distingué dans $\mathcal{A}_4$ et que ce 2-Sylow est H.

De plus tous les éléments de H sont d'ordre divisant 2 donc H est abélien [20].

c) Tout élément de $\mathcal{A}_4$ peut s'écrire de manière unique sous la forme $t^\ell h$ avec $\ell \in \{0, 1, 2\}$ et $h \in \mathrm{H}$.

Considérons

$$\varphi\colon \mathrm{T} \times \mathrm{H} \to \mathcal{A}_4, \qquad (c, h) \mapsto ch.$$

20. En effet soit G un groupe dont tous les éléments sont d'ordre divisant 2 ; si g et h sont deux éléments de G, alors d'une part $(gh)^2 = e$ et d'autre part $g^2h^2 = e$ d'où $(gh)^2 = g^2h^2$ soit $ghgh = gghh$ et $gh = gh$.

C'est une injection de $\mathrm{T}\times\mathrm{H}$ dans $\mathcal{A}_4$. En effet soient (c_1,h_1) et (c_2,h_2) dans $\mathrm{T}\times\mathrm{H}$ tels que $c_1h_1=c_2h_2$. Alors $c_2^{-1}c_1=h_2h_1^{-1}$; en particulier puisque $c_2^{-1}c_1$ appartient à T et $h_2h_1^{-1}$ appartient à H, les éléments $c_2c_1^{-1}$ et $h_2h_1^{-1}$ appartiennent à $\mathrm{T}\cap\mathrm{H}$. Or $\mathrm{T}\cap\mathrm{H}=\{\mathrm{id}\}$ donc $(c_1,h_1)=(c_2,h_2)$. Remarquons que $|\mathrm{T}\times\mathrm{H}|=|\mathcal{A}_4|$; il en résulte que φ est une bijection ce qui permet de conclure.

d) On peut vérifier que les 3-cycles t et t^2 ne commutent à aucun élément de $\mathrm{H}\smallsetminus\{\mathrm{id}\}$ par un calcul direct.

e) Montrons que les classes de conjugaison de $\mathcal{A}_4$ sont

$$C_1=\{\mathrm{id}\},\qquad C_2=\mathrm{H}\smallsetminus\{\mathrm{id}\},\qquad C_3=t\mathrm{H},\qquad C_4=t^2\mathrm{H}.$$

Comme dans tout groupe la classe de conjugaison de l'élément neutre a un seul élément C_1 appartient à l'ensemble $\mathrm{conj}(\mathcal{A}_4)$ des classes de conjugaison de $\mathcal{A}_4$.

Si s appartient à C_2 et si t^ah, avec $a\in\{0,\,1,\,2\}$ et $h\in\mathrm{H}$, commute à s, alors $t^ahs=st^ah$ donc $t^ahsh=st^ah^2$. Comme H est abélien et $h^2=\mathrm{id}$ nous obtenons $t^as=st^a$ ce qui entraîne $a=0$. Le centralisateur de s est donc G et le cardinal de la classe de conjugaison de s est égal à $\frac{|\mathcal{A}_4|}{|\mathrm{H}|}=3$. Puisqu'un conjugué de s est d'ordre 2, cette classe de conjugaison est incluse dans C_2 et lui est égale pour des raisons de cardinal.

Enfin le centralisateur de t et t^2 est T ; en effet si $t^aht=tt^ah$ alors $ht=th$ et donc $h=\mathrm{id}$. Il s'ensuit que la classe de conjugaison de t est de cardinal $\frac{|\mathcal{A}_4|}{|\mathrm{T}|}=4$. Or

$$(t^ah)t(t^ah)^{-1}=t^ahth^{-1}t^{-a}=t(t^{a-1}ht^{1-a})(t^ah^{-1}t^{-a})\in t\mathrm{H}$$

car H est distingué dans $\mathcal{A}_4$. Donc $t^{a-1}ht^{1-a}$ et $t^ah^{-1}t^{-a}$ appartiennent à H. La classe de conjugaison de t est donc contenue dans C_3 et lui est égale pour des raisons de cardinalité. On obtient de la même façon que la classe de conjugaison de t^2 est C_4.

f) Soit $\zeta=\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ une racine primitive 3ième de l'unité. Rappelons que μ_n désigne l'ensemble des racines $n$ième de l'unité. Pour $0\leq j\leq 2$ on définit $\eta^j:\mathcal{A}_4\to\mu_3$ par $\eta^j(t^ah)=\zeta^{ja}$ si $0\leq a\leq 2$ et $h\in\mathrm{H}$. Alors $\eta^0=\mathrm{id}$, η et η^2 sont des caractères linéaires distincts de $\mathcal{A}_4$.

En effet si $0\leq a,\,b\leq 2$ et si h, g appartiennent à H, alors $t^aht^bg=t^{a+b}(t^{-b}ht^b)g$. Puisque H est distingué dans $\mathcal{A}_4$, on a $t^{-b}ht^b$ appartient à H et donc $(t^{-b}ht^b)g$ appartient à H. De plus $\eta^j(t^aht^bg)=\zeta^{j(a+b)}=\zeta^{ja}\zeta^{jb}=\eta^j(t^ah)\eta^j(t^bg)$.

g) Soit V la représentation de permutation associée à l'action naturelle de $\mathcal{A}_4$ sur $\{1,\,2,\,3,\,4\}$. Rappelons que cette représentation est $\mathbb{C}^4$ muni de l'action de $\mathcal{A}_4$ définie dans la base canonique $(e_1,\,e_2,\,e_3,\,e_4)$ par $g(e_i)=e_{g(i)}$. L'hyperplan W d'équation $x_1+x_2+x_3+x_4=0$ est stable par $\mathcal{A}_4$ et la représentation obtenue est irréductible de caractère :

$$\chi_W(\mathrm{id})=3,\qquad \chi_W(g)=-1\text{ si }g\in\mathrm{H}\smallsetminus\{\mathrm{id}\},\qquad \chi_W(g)=0\text{ si }g\notin\mathrm{H}.$$

En effet la représentation V se décompose sous la forme $V'\oplus W$ où V' est la droite engendrée par $e_1+e_2+e_3+e_4$. Puisque V est une repésentation de permutation $\chi_V(g)$

est le nombre de points fixes de g agissant sur $\{1, 2, 3, 4\}$. Nous avons donc

$$\chi_V(\mathrm{id}) = 4, \qquad \chi_V(g) = 0 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_V(g) = 1 \text{ si } g \notin \mathrm{H}.$$

Nous en déduisons le caractère de W car $\chi_V = \chi_{V'} + \chi_W$ et $\chi_{V'}(g) = 1$ pour tout $g \in \mathcal{A}_4$ (en effet $e_1 + e_2 + e_3 + e_4$ est fixe par $\mathcal{A}_4$ donc $\chi_{V'} \simeq \chi_{\rho_{\mathrm{triv}}}$). Par suite

$$\chi_W(\mathrm{id}) = 3, \qquad \chi_W(g) = -1 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_W(g) = 0 \text{ si } g \notin \mathrm{H}.$$

Montrons que W est irréductible. Commençons par constater que si g appartient à $\mathcal{A}_4$ et si $v = (x_1, x_2, x_3, x_4)$ appartient à $\mathbb{C}^4$, alors

$$g \cdot v = x_1 e_{g(1)} + x_2 e_{g(2)} + x_3 e_{g(3)} + x_4 e_{g(4)} = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}, x_{g^{-1}(4)}).$$

Supposons que v appartienne à $W \smallsetminus \{0\}$; soit W' le sous-espace de W engendré par les $g \cdot v$ pour $g \in \mathcal{A}_4$. Montrons que $W = W'$ quel que soit v. Il existe donc $i \neq j$ tel que $x_i \neq x_j$; sans perdre de généralité on peut supposer que $x_1 \neq x_2$. L'image de v par le 3-cycle t est alors (x_3, x_1, x_2, x_4) ; il s'ensuit que W' qui contient $t \cdot v$ et v contient $w = t \cdot v - v = (x_3 - x_1, x_1 - x_2, x_2 - x_3, 0)$. Le sous-espace W' contient aussi $w + g \cdot w$ si $g = (1\ 3)(2\ 4)$, et comme

$$w + g \cdot w = (x_1 - x_2)(e_2 + e_4 - e_1 - e_3)$$

et $x_1 - x_2 \neq 0$ il contient le vecteur $f_1 = e_1 - e_2 + e_3 - e_4$. Il contient donc aussi les images $f_2 = e_1 + e_2 - e_3 - e_4$ et $f_3 = e_1 - e_2 - e_3 + e_4$ de f_1 par les 3-cycles $(2\ 4\ 3)$ et $(2\ 3\ 4)$. Puisque f_1, f_2 et f_3 forment une base de W nous avons l'égalité recherchée $W = W'$.

h) Le groupe $\mathcal{A}_4$ compte quatre classes de conjugaison, il a donc quatre représentations irréductibles à isomorphismes près qui sont les trois caractères linéaires ρ_{triv}, η et η^2 et la représentation W de dimension 3. Les valeurs des caractères de ces représentations ont été calculées ci-dessus d'où la table des caractères de $\mathcal{A}_4$:

	C_1	C_2	C_3	C_4
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1
χ_η	1	1	ζ	ζ^2
χ_{η^2}	1	1	ζ^2	ζ
χ_W	3	-1	0	0

Exercice 485

a) Soit G un groupe fini abélien et soit χ un caractère de G sur $\mathbb{C}$.

Montrer que

$$\sum_{a \in \mathrm{G}} |\chi(a)|^2 \geq |\mathrm{G}| \cdot \chi(1).$$

b) Soit G un groupe fini et soit H un sous-groupe abélien de G d'indice $n \geq 1$.

Montrer que si χ est un caractère irréductible de G, on a $\chi(1) \leq n$. Que peut-on dire si $\chi(1) = n$?

Éléments de réponse 485

Exercice 486

Soit G un groupe fini. Soient ϕ et ψ des caractères de G dans $\mathbb{C}$.

a) Montrer que si ψ est de degré 1, alors $\phi\psi$ est irréductible si et seulement si ϕ est irréductible.

b) Montrer que si ψ est de degré strictement supérieur à 1, alors le caractère $\psi\overline{\psi}$ n'est pas irréductible.

c) Soit ϕ un caractère irréductible de G. On suppose que ϕ est le seul caractère irréductible de son degré. Montrer que s'il existe un caractère ψ de degré 1 et $g \in \mathrm{G}$ tel que $\psi(g) \neq 1$, alors $\phi(g) = 0$.

Éléments de réponse 486

Exercice 487

Soit p un nombre premier. Soit $n \geq 1$ un entier. On pose $q = p^n$. Soit G le groupe donné par

$$\mathrm{G} = \{x \mapsto ax + b \,|\, a \in \mathbb{F}_q^x,\, b \in \mathbb{F}_q\}.$$

a) Déterminer la table des caractères de G sur $\mathbb{C}$.

b) Déterminer les représentations irréductibles de G sur $\mathbb{C}$.

Éléments de réponse 487

Exercice 488

Soient p un nombre premier, G un p-groupe fini et $\Bbbk$ un corps de caractéristique p.

a) Montrer que toute représentation linéaire de G sur un $\Bbbk$-espace vectoriel non nul admet des vecteurs fixes non nuls.

b) Montrer que toute représentation irréductible de G à coefficients dans $\Bbbk$ est isomorphe à la représentation triviale.

Éléments de réponse 488

Exercice 489

a) Soient G un groupe abélien (éventuellement infini) et (V, ρ) une représentation complexe irréductible de G (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle de dimension 1 ? Est-ce toujours le cas ?

b) Soient $\Bbbk$ un corps de caractéristique nulle, G un groupe (éventuellement infini) et (V, ρ) une représentation de G sur $\Bbbk$ (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle somme directe de sous-représentations irréductibles ? Est-ce toujours le cas ?

Éléments de réponse 489

Exercice 490

Montrer que deux représentations de degré 1 d'un groupe G sont équivalentes si et seulement si elles coïncident.

Éléments de réponse 490

Exercice 491

Soit G un groupe.

a) Soient ρ_1 et ρ_n des représentations complexes de G de degré respectivement 1 et n. Montrer que

$$\rho_1 \cdot \rho_n \colon \mathrm{G} \longrightarrow \mathrm{GL}(n, \mathbb{C}), \qquad g \longmapsto \rho_1(g) \cdot \rho_n(g)$$

est une représentation de G.

b) Si ρ_n est irréductible, montrer que $\rho_1 \cdot \rho_n$ l'est aussi.

Éléments de réponse 491

Exercice 492

Soient G un groupe fini et H un sous-groupe distingué de G. Montrer que l'ensemble des représentations du groupe quotient G/H s'identifie naturellement aux représentations de G dont la restriction à H est triviale.
En déduire une injection de l'ensemble des représentations irréductibles de G/H dans l'ensemble des représentations irréductibles de G.

Éléments de réponse 492

Exercice 493

Soit $\rho \colon \mathrm{G} \longrightarrow \mathrm{GL}(V)$ une représentation irréductible d'un groupe abélien fini G dans un $\mathbb{C}$-espace vectoriel de dimension finie.

a) Utiliser le lemme de Schur pour montrer que $\rho(g)$ est une homothétie, pour tout $g \in \mathrm{G}$.

b) En déduire que chaque sous-espace vectoriel de V est ρ-invariant.

c) Conclure que le degré de ρ est égal à 1.

Éléments de réponse 493

Exercice 494

Soit ρ la représentation du groupe symétrique $\mathfrak{S}_n$ dans $V = \mathbb{C}^n$ agissant par permutations des coordonnées (*i.e.* $\sigma \cdot (x_1, \ldots, x_n) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$). Montrer que l'hyperplan H d'équation $\sum_{1 \leq i \leq n} x_i = 0$ est stable pour cette action et que la représentation associée est irréductible.

Éléments de réponse 494

Exercice 495

Montrer que tout groupe fini est isomorphe (par exemple via la représentation régulière) à un sous-groupe de $\mathrm{GL}(V)$ où V désigne un espace vectoriel approprié de dimension finie.

Éléments de réponse 495

Exercice 496

Soient G un groupe fini et $\rho\colon \mathrm{G} \to \mathrm{GL}(n, \mathbb{C})$ une représentation de G dans $\mathbb{C}^n$. Construire un produit scalaire hermitien $< \cdot, \cdot >_G$ sur $\mathbb{C}^n$ invariant par G, i.e.

$$\langle \rho(g)(x), \rho(g)(y) \rangle_{\mathrm{G}} = \langle x, y \rangle_{\mathrm{G}}, \qquad \forall\, x, y \in \mathbb{C}^n, \forall\, g \in \mathrm{G}.$$

Retrouver le lemme de Maschke : toute sous-représentation de ρ admet un supplémentaire stable par G.

Éléments de réponse 496

Exercice 497

Soient X un ensemble fini et G un groupe fini opérant sur X. Notons V la représentation de permutation de G sur $\mathbb{C}^X$ et χ_V son caractère.
Soit c le nombre d'orbites de l'action de G sur X. Montrer que c est égal au nombre de fois que V contient la représentation triviale 1. En déduire la formule de Burnside :

$$c = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|.$$

Éléments de réponse 497

Exercice 498

Soit G un groupe fini. Soit H un sous-groupe de G. Soit π une représentation de G de caractère χ.

a) Montrer que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$.

b) Si π est irréductible, est-ce que $\chi_{|\mathrm{H}}$ est un caractère irréductible ?

Éléments de réponse 498

a) Montrons que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$. Pour tout $h \in H$ on a

$$\chi_{\pi_{|\mathrm{H}}}(h) = \mathrm{tr}(\pi_{|\mathrm{H}}(h)) = \mathrm{tr}(\pi(h)) = \chi(h) = \chi_{|\mathrm{H}}(h).$$

b) Si π est irréductible, $\chi_{|\mathrm{H}}$ n'est pas nécessairement un caractère irréductible. En effet soit G un groupe fini non abélien. Soit $H = \{e_{\mathrm{G}}\}$ le sous-groupe trivial de G et soit π une représentation complexe irréductible de G de dimension ≥ 2 (une telle représentation existe). Alors toute droite de π est un sous-espace strict non nul de π stable par H donc $\chi_{|\mathrm{H}}$ n'est pas irréductible.

Exercice 499

Soit G un groupe fini. Soit H un sous-groupe de G. Soit (π, V) une représentation de H. On pose

$$W = \{f\colon \mathrm{G} \to V \mid \forall\, x \in \mathrm{G}\, \forall\, h \in H \quad f(hx) = \pi(h)f(x)\}$$

avec une action de G donnée par $g(f)\colon x \mapsto f(xg)$.

a) Montrer que W est une représentation de G. Quelle est sa dimension ?

b) Si π est irréductible, W est-elle une représentation irréductible de G ?

Éléments de réponse 499

a) Montrons que W est une représentation de G. On peut vérifier que

- W est un sous-espace vectoriel de V^{G} ;
- la formule $(g, f) \mapsto g(f)$ définit une action de groupes linéaire de G sur W ;
- pour tout $g \in \mathrm{G}$ et pour tout $f \in W$, on a $f(g)$ appartient à W. En effet, pour tout $h \in H$ et pour tout $x \in \mathrm{G}$ on a

$$g(f)(hx) = f(h(xg)) = \pi(h)f(xg) = \pi(h)g(f)(x).$$

Ces trois points assurent que W est naturellement une représentation de G.

Précisons la dimension de W.

Si $R \subset G$ désigne l'ensemble des représentants de G modulo H l'application

$$W \to V^R \qquad\qquad f \mapsto f_{|R}$$

est une application linéaire. C'est un isomorphisme par définition de W : un élément de W est entièrement déterminé par l'image des éléments de R. Par suite $\dim W = |R| \dim V$, *i.e.* $\dim W = [\mathrm{G} : \mathrm{H}] \dim V$.

b) Si π est irréductible, W n'est pas nécessairement une représentation irréductible de G. Considérons un groupe G non trivial et $H = \{e_G\}$ le sous-groupe trivial. La représentation triviale de H, notée triv, est irréductible. On peut vérifier que $W(\text{triv}) \simeq K[G]$ où $K[G]$ désigne la représentation régulière de G. Or cette dernière est irréductible si et seulement si $|G| = 1$ ce que l'on a exclu.

Exercice 500 [Représentations et sous-groupes distingués, Peyre, l'algèbre discrète de la transformée de Fourier, pages 231-232]

Soit G un groupe fini dont e_G est l'élément neutre. Soient ρ_1, ρ_2, …, ρ_r un ensemble de représentants des classes d'isomorphies de représentations irréductibles. Soient χ_1, χ_2, …, χ_r les caractères irréductibles associés. Posons

$$K_{\chi_i} = \{g \in G \,|\, \chi_i(g) = \chi_i(e_G)\}$$

a) Soit $\rho\colon G \to GL(V)$ une représentation de caractère χ_V sur un $\mathbb{C}$-espace V de dimension d. Soit g un élément d'ordre k de G. Alors

(i) $\rho(g)$ est diagonalisable ;

(ii) χ_V est somme de $\chi_V(1) = \dim V = d$ racines $k$ième de l'unité ;

(iii) $|\chi_V(g)| \leq \chi_V(e_G) = d$;

(iv) $K_{\chi_V} = \{x \in G, \,|\, \chi_V(x) = \chi_V(e_G)\}$ est un sous-groupe distingué de G. On l'appelle noyau de la représentation.

b) Soit $N \lhd G$ un sous-groupe distingué de G. Soit ρ_U une représentation de G/N sur un espace vectoriel U.

Il existe une représentation canonique de G sur U telle que les sous-représentations de U sous l'action de G/N soient exactement celles de U sous l'action de G.

c) Soit V un espace vectoriel de dimension égale à l'ordre de G. Soit $(b_t)_{t\in G}$ une base de V. La représentation régulière de G est la représentation

$$\begin{array}{rcl} \rho_{\text{reg}}\colon G & \to & GL(V) \\ g & \mapsto & \rho_{\text{reg}}(g)\colon V \to V \\ & & \qquad b_t \mapsto b_{gt} \end{array}$$

Soit $\rho\colon G \to GL(V)$ une représentation de G. La représentation est fidèle si ρ est injectif.

Montrer que la représentation régulière est fidèle.

d) Montrer que les sous-groupes distingués de G sont les

$$\bigcap_{i\in I} K_{\chi_i}$$

où $I \subset \{1, 2, 3, \ldots, r\}$.

e) Montrer que G est simple si et seulement si

$$\forall\, i \neq 1,\, \forall\, g \in \mathrm{G} \qquad \chi_i(g) \neq \chi_i(e_{\mathrm{G}}).$$

Éléments de réponse 500

a) (i) Puisque $g^k = 1$, on a $\rho(g)^k = \mathrm{id}$. Le polynôme minimal de $\rho(g)$ divise donc $X^k - 1$ qui est scindé à racines simples.

(ii) Soient λ_1, λ_2, …, λ_d les valeurs propres de $\rho(g)$ qui sont des racines $k$ièmes de l'unité. On a $\chi_V(g) = \lambda_1 + \lambda_2 + \ldots + \lambda_d$.

(iii) On a $|\chi_V(g)| \leq |\lambda_1| + |\lambda_2| + \ldots + |\lambda_d| = d$.

(iv) Si $|\chi_V(g)| = d$, alors d'après (iii) les nombres complexes λ_i sont positivement liés sur $\mathbb{R}$; comme ils sont de module 1, ils sont tous égaux. Si $\chi_V(g) = d$, alors nécessairement $\lambda_i = 1$ donc $\rho(g) = \mathrm{id}$. Ainsi $K_{\chi_V} = \ker\rho$ est bien un sous-groupe distingué.

b) Désignons par $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{N}}$ la projection canonique. La représentation $\widetilde{\rho}_U$ définie par

$$\forall\, g \in \mathrm{G} \qquad \widetilde{\rho}_U(g) = \rho_U \circ \pi(g)$$

convient.

c) Direct.

d) Soit $\mathrm{N} \lhd \mathrm{G}$ un sous-groupe distingué de G. Désignons par ρ_U la représentation régulière de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. Autrement dit U est un espace vectoriel de dimension égale à $|{}^{\mathrm{G}}\!/_{\mathrm{N}}| = \frac{|\mathrm{G}|}{|\mathrm{N}|}$ de base $(e_g)_{g\in{}^{\mathrm{G}}\!/_{\mathrm{N}}}$ et $\rho_U(h)(e_{\mathrm{G}}) = e_{hg}$. La représentation régulière est fidèle (c)) donc ρ_U est injective. Le b) permet d'étendre cette représentation en une représentation $\widetilde{\rho}_U\colon \mathrm{G} \to U$. Notons χ le caractère de la représentation $\widetilde{\rho}_U$. On a $\ker\widetilde{\rho}_U = \ker(\rho_U \circ \pi) = \mathrm{N}$ D'où $\mathrm{N} = K_\chi$. Ecrivons la décomposition de la représentation $\widetilde{\rho}_U$ en fonction des représentations irréductibles

$$\chi = a_1\chi_1 + a_2\chi_2 + \ldots + a_r\chi_r$$

D'après la troisième assertion de a) on a

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}}).$$

On a donc l'égalité $\chi(g) = \chi(e_{\mathrm{G}})$, *i.e.* $g \in K_\chi$, si et seulement si

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| = \sum_{i=1}^{r} a_i|\chi_i(g)| = \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}})$$

autrement dit si et seulement si

$$\forall\, i \qquad a_i\chi_i(g) = a_i\chi_i(e_{\mathrm{G}}).$$

Ceci est finalement équivalent à

$$\forall\, i \qquad a_i > 0 \Rightarrow g \in K_{\chi_i}.$$

On obtient donc le résultat voulu avec $I = \{i \,|\, a_i > 0\}$.

Réciproquement comme les K_{χ_i} sont distingués tout sous-groupe du type $\bigcap_{i\in I} K_{\chi_i}$ l'est aussi.

e) Supposons qu'il existe un élément de $\mathrm{G} \smallsetminus \{e_\mathrm{G}\}$ tel que $\chi_i(g) = \chi_i(e_\mathrm{G})$; alors $K_{\chi_i} \subset \mathrm{G}$ est un sous-groupe distingué non trivial et G n'est pas simple.

Réciproquement si G n'est pas simple, il existe $g \neq e_\mathrm{G}$ dans un certain sous-groupe distingué $\mathrm{N} \triangleleft \mathrm{G}$ non trivial. Le d) assure que $\mathrm{N} = \bigcap_{i\in I} K_{\chi_i}$ donc g appartient à K_{χ_i} pour $i \in I \subset \{2, 3, \ldots, r\}$. Ceci signifie bien que $\chi_i(g) = \chi_i(e_\mathrm{G})$.

Exercice 501

Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}(n, \mathbb{C})$ est le groupe des homothéties.

Une représentation ρ du groupe $\mathrm{GL}(n, \mathbb{C})$ est donnée par son action naturelle sur $\mathbb{C}^n$.

1. Montrer que la représentation ρ est irréductible.
2. Montrer que tout élément du centre de $\mathrm{GL}(n, \mathbb{C})$ est un morphisme de la représentation ρ, *i.e.* montrer que pour tout élément h du centre et pour tout élément M de $\mathrm{GL}(n, \mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M).$$
3. Conclure en utilisant le Lemme de Schur.

Éléments de réponse 501

Puisque ρ est l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}(n, \mathbb{C})$ dans $\mathrm{GL}(n, \mathbb{C})$.

1. Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}(n, \mathbb{C})$, alors $V = \{0\}$ ou $V = \mathbb{C}^n$, *i.e.* ρ est irréductible.
2. Soit h un élément du centre de $\mathrm{GL}(n, \mathbb{C})$. Pour tout M dans $\mathrm{GL}(n, \mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M)$$
ainsi h est bien un morphisme de la représentation ρ.
3. Comme ρ est irréductible, le Lemme de Schur assure que $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, *i.e.* h est une homothétie.

Exercice 502

Soit G un groupe fini. Soit E un ensemble fini sur lequel G agit et soit ρ la représentation de permutation correspondante. Notons χ le caractère de ρ. Montrer que $\chi(g)$ est le nombre d'éléments de E fixé par g.

Éléments de réponse 502

Dans la représentation de permutation la matrice $\rho(g)$ est une matrice de permutation avec

- ◇ un 1 à la position (i,i) si i est fixé par g,
- ◇ un 0 à la position (i,i) sinon.

Puisque $\chi(g) = \mathrm{tr}\rho(g)$, $\chi(g)$ coïncide avec le nombre d'éléments de E fixé par g.

Exercice 503

Soit G un groupe fini. Soit ρ une représentation linéaire de G. Notons χ le caractère de ρ. Montrons que le nombre de fois où ρ_{triv} apparaît dans ρ est égal à $\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)$.

Éléments de réponse 503

Décomposons ρ en somme de représentations irréductibles : $\rho = \bigoplus_{i=1}^{k}\rho_i^{n_i}$. Quitte à réindicer les ρ_i on peut supposer que $\rho_1 = \rho_{\mathrm{triv}}$.

De plus

$$\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)\cdot 1 = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)\cdot\chi_{\rho_{\mathrm{triv}}}(g^{-1}) = \langle\chi,\chi_{\rho_{\mathrm{triv}}}\rangle = n_1$$

Exercice 504

Soit G un groupe abélien.

1. Si $\rho\colon \mathrm{G}\to\mathrm{GL}(V)$ est une représentation de G, montrer que tout élément G de G définit un G-morphisme $V\to V$.
2. En déduire que toute représentation irréductible de G est de dimension 1.
3. Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 504

1. Pour tous g, h et x dans G on a
$$g\cdot(h\cdot x) = (gh)\cdot x = (hg)\cdot x = h\cdot(g\cdot x)$$
c'est-à-dire l'application $\rho(g)\colon x\mapsto g\cdot x$ est un G-morphisme pour tout $g\in\mathrm{G}$.
2. On suppose que V est une représentation irréductible de G. Si $g\in\mathrm{G}$, alors, d'après 1. et le Lemme de Schur, $\rho(g) = \lambda\mathrm{id}$. De plus comme $\rho(g)\in\mathrm{GL}(V)$, λ est non nul. Par conséquent tout sous-espace vectoriel de V est stable par G donc est une sous-représentation de G. Puisque V est irréductible, $\dim V = 1$.

3. D'après 1. une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes
$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*$$
Tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n ; par suite $\rho(k)$ est aussi d'ordre divisant n, *i.e.* $\rho(k)^n = 1$. Réciproquement pour tout racine $n$ième de l'unité ω l'application
$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$
est une représentation de $\mathbb{Z}/n\mathbb{Z}$. On les obtient donc toutes ainsi.

Notons aussi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 505

Soit G un groupe fini. Soit H un sous-groupe abélien de G.

Montrer que toute représentation irréductible de G est de dimension au plus [G : H].

Indication : si V est une représentation irréductible de G*, c'est aussi une représentation de* H*. On pourra considérer la représentation de* G *engendrée par une sous-représentation de* H*.*

Éléments de réponse 505

Soit V une représentation irréductible de G. C'est aussi par restriction une représentation irréductible de H. Puisque H est abélien, V vu comme représentation de H se décompose en somme directe de représentations de H de degré 1. Soit v un vecteur directeur d'une de ces représentations et soit V' le sous-espace vectoriel de V engendré par les vecteurs de la forme $g \cdot v$ où g parcourt G. Il est clair que $V' \neq \{0\}$ est une sous-représentation de V du groupe G ; ainsi $V' = V$. Or si $g' = gh$ avec h dans H, alors par définition de v, $g' \cdot v$ et $g \cdot v$ sont colinéaires. Par conséquent V' est engendré par [G : H] vecteurs, et est donc de dimension au plus [G : H].

Exercice 506

Montrer que tout groupe non abélien admet une représentation irréductible de dimension > 1.

Éléments de réponse 506

Soit G un groupe dont toutes les représentations irréductibles sont de degré 1. La somme des carrés des dimensions des représentations irréductibles de G est égale au cardinal de G ; par suite les classes de conjugaisons de G sont toutes réduites à un élément. Autrement dit G est abélien.

Exercice 507

Montrer que si V est une représentation d'un groupe fini vérifiant $\langle \chi_V, \chi_V \rangle = 2$, alors V est somme de deux représentations irréductibles.

Éléments de réponse 507

Si $V = \oplus V_i^{a_i}$, alors $\langle \chi_V, \chi_V \rangle = 2$ si et seulement si deux a_i distincts sont non nuls et égaux à 1.

Exercice 508

Soit $\mathfrak{S}_3$ le groupe des permutations de $\{1, 2, 3\}$.

Notons e, s et t les trois classes de conjugaison de $\mathfrak{S}_3$ où e est la classe de conjugaison de l'identité, s celle des transpositions et t celle des 3-cycles.

1. Montrer (sans les construire) que $\mathfrak{S}_3$ a deux représentations irréductibles de dimension 1 et une de dimension 2.
2. Notons χ_1 le caractère de la représentation triviale, χ_2 celui de la signature sgn qui est l'autre représentation de dimension 1 et θ celui de la représentation W de dimension 2. De quelle représentation $\psi = \chi_1 + \chi_2 + 2\theta$ est-il le caractère ? Compléter la table

	e	s	t
χ_1			
χ_2			
$\chi_1 + \chi_2 + 2\theta$			
θ			

3. Faisons agir $\mathfrak{S}_3$ sur lui-même par conjugaison intérieure ($g \cdot x = gxg^{-1}$). Notons V la représentation de permutation associée et χ son caractère. Calculer χ. En déduire les multiplicités de la représentation triviale, de la représentation sgn et de la représentation W dans la décomposition de V.

Éléments de réponse 508

1. Puisque le groupe $\mathfrak{S}_3$ a trois classes de conjugaison, il a trois représentations irréductibles ; nous les notons W_1, W_2 et W_3. Comme $(\dim W_1)^2 + (\dim W_2)^2 + (\dim W_3)^2 = 6$ la seule possibilité est que deux des dimensions valent 1 et la troisième 2.
2. La première colonne des première, deuxième et quatrième lignes correspond aux dimensions des W_i.

   Les seconde et troisième colonnes des deux premières lignes s'obtiennent directement.

   Les seconde et troisième colonnes de la troisième ligne s'obtient par orthogonalité des colonnes (si on note a (resp. b) le coefficient de la seconde (resp. troisième) colonne, on a $1 \times 1 + 1 \times (-1) + 2 \times a = 0$ soit $a = 0$ et $1 \times 1 + 1 \times 1 + 2 \times b = 0$ soit $b = -1$).

   La troisième ligne s'obtient à partir des première, seconde et quatrième lignes.

   Finalement on a

	e	s	t
χ_1	1	1	1
χ_2	1	-1	1
$\chi_1+\chi_2+2\theta$	6	0	0
θ	2	0	-1

Enfin $\chi_1+\chi_2+2\theta$ est le caractère de la représentation régulière [21].

3. Comme V est une représentation de permutation, $\chi(g)$ est le nombre de points fixes de g, *i.e.* le nombre d'éléments h de $\mathfrak{S}_3$ tels que $ghg^{-1}=h$, ou encore le nombre d'éléments de $\mathfrak{S}_3$ qui commutent avec g. Nous avons donc $\chi(g)=|Z_g|=|\mathfrak{S}_3|\cdot|C_g|^{-1}$ où Z_g désigne l'ensemble des éléments de $\mathfrak{S}_3$ qui commutent à g et C_g la classe de conjugaison de g. Nous en déduisons que $\chi(e)=6$, $\chi(s)=2$ et $\chi(t)=3$.

   Si W' est une représentation irréductible, alors la multiplicité de W' dans V est $\langle\chi_{W'},\chi\rangle$. Comme

$$\langle\chi_1,\chi\rangle=\frac{1}{6}\Big(6+3\times(1\times 2)+2\times(1\times 3)\Big)=3$$
$$\langle\chi_2,\chi\rangle=\frac{1}{6}\Big(6+2\times(-1\times 2)+2\times(1\times 3)\Big)=1$$
$$\langle\theta,\chi\rangle=\frac{1}{6}\Big(2\times 6+3\times(0\times 2)+2\times(-1\times 3)\Big)=1$$

   nous avons $V=3\rho_{\text{triv}}\oplus\text{sgn}\oplus W$.

Exercice 509

On se propose d'établir la table des caractères du groupe $\mathfrak{S}_4$ des permutations de $\{1, 2, 3, 4\}$. Les partitions de 4 sont

$$4 \qquad 3+1 \qquad 2+2 \qquad 2+1+1 \qquad 1+1+1+1;$$

il en résulte que le groupe $\mathfrak{S}_4$ a 5 classes de conjugaison : la classe C_1 de l'élément neutre (1 élément), celle C_2 des transpositions (6 éléments), celle $C_{2,2}$ des produits de deux transpositions de supports disjoints (3 éléments), celle C_3 des 3-cycles (8 éléments), celle C_4 des 4-cycles (6 éléments) ;

21. Rappelons que si G est fini, si $E=\text{G}$ et si l'action de G est donnée par la multiplication à gauche, alors la représentation régulière est donnée par : $\chi(1)=|\text{G}|$ et $\chi(g)=0$ si $g\in\text{G}\smallsetminus\{e\}$.

	1	6	3	8	6
	C_1	C_2	$C_{2,2}$	C_3	C_4
$\chi_{\rho_{\text{triv}}}$	1	1	1	1	1
sgn	1	-1	1	1	-1
θ	2	0	2	-1	0
χ_1	3	1	-1	0	-1
χ_2	3	-1	-1	0	1

1. Soit V la représentation de permutation associée à l'action de $\mathfrak{S}_4$ sur $\{1, 2, 3, 4\}$.
   a) Calculer χ_V et $\langle \chi_V, \chi_V \rangle$. En déduire que V est la somme directe $V_1 \oplus V_2$ de deux représentations irréductibles V_1, V_2 non isomorphes.
   b) Déterminer les sous-espaces V_1 et V_2 de V et montrer, en revenant à la définition, que ce sont des représentations irréductibles de $\mathfrak{S}_4$.
   c) Calculer les caractères de V_1 et V_2. Quelles lignes de la table cela permet-il de remplir ?
2. Quelle est la seconde représentation de dimension 1 ? Comment peut-on obtenir la seconde de dimension 3 (pourquoi est-elle irréductible et différente de celle déjà construite ?) ?
3. Comment peut-on compléter la table des caractères de $\mathfrak{S}_4$?

Éléments de réponse 509

1. a) Puisque V est une représentation de permutation, $\chi_V(\sigma)$ est le nombre de points fixes de σ agissant sur $\{1, 2, 3, 4\}$. Par conséquent nous avons

$$\chi_V(C_1) = 4, \qquad \chi_V(C_2) = 2, \qquad \chi_V(C_{2,2}) = 0, \qquad \chi_V(C_3) = 1, \qquad \chi_V(C_4) = 0.$$

   Par suite

$$\langle \chi_V, \chi_V \rangle = \frac{1}{24}\Big(4^2 + 6 \times 2^2 + 3 \times 0^2 + 8 \times 1^2 + 6 \times 0^2\Big) = 2.$$

   Si $V = \bigoplus_{W \in \mathrm{Irr}(\mathfrak{S}_4)} m_W W$, $\langle \chi_V, \chi_V \rangle$ est aussi égal à $\sum_{W \in \mathrm{Irr}(\mathfrak{S}_4)} m_W^2$ puisque les χ_W forment une famille orthonormale. Étant donné que la seule écriture de 2 comme somme de deux carrés est $1^2 + 1^2$ nous en déduisons que $m_W = 1$ pour exactement deux représentations irréductibles W de $\mathfrak{S}_4$ et $m_W = 0$ pour les autres ce qui permet de conclure.

   b) La droite V_1 engendrée par $e_1 + e_2 + e_3 + e_4$ et l'hyperplan V_2 d'équation $x_1 + x_2 + x_3 + x_4 = 0$ sont stables par $\mathfrak{S}_4$.

   Puisque V_1 est de dimension 1 elle est automatiquement irréductible.

Soit $x = (x_1, x_2, x_3, x_4) \in V_2$ non nul. Il s'agit de démontrer que le sous-espace vectoriel U_x de V_2 engendré par les $\sigma \cdot x$, pour $\sigma \in \mathfrak{S}_4$, est égal à V_2. Il existe $i \neq j$ tels que $x_i \neq x_j$. Soit τ la transposition $(i\ j)$. Alors $x - \tau \cdot x$ est un multiple non nul de $e_i - e_j$. Il en résulte que $e_i - e_j$ appartient à U_x et donc que $\sigma \cdot (e_i - e_j) = e_{\sigma(i)} - e_{\sigma(j)}$ appartient à U_x pour tout $\sigma \in \mathfrak{S}_4$. Mais $(\sigma(i), \sigma(j))$ décrit les couples d'éléments distincts de $\{1, 2, 3, 4\}$ quand σ décrit $\mathfrak{S}_4$; ainsi U_x contient $e_1 - e_2$, $e_1 - e_3$ et $e_1 - e_4$. Ces vecteurs engendrant V_2 cela permet de conclure.

c) La représentation V_1 est la représentation triviale ; par conséquent $\chi_{V_1}(C) = 1$ pour toute classe de conjugaison C de $\mathfrak{S}_4$. Nous pouvons donc remplir la première ligne de la table.

Par ailleurs $\chi_V = \chi_{V_1} + \chi_{V_2}$, cela permet donc de déterminer χ_{V_2}. Nous pouvons donc remplir la quatrième ligne de la table.

2. La seconde représentation de dimension 1 est la signature sgn. Ses valeurs sont bien celles reportées dans la seconde ligne. La seconde représentation de dimension 3 est $V_1 \otimes \mathrm{sgn}$. Si elle pouvait se décomposer sous la forme $V_1 \otimes \mathrm{sgn} = W_1 \oplus W_2$, alors $V_1 = (V_1 \otimes \mathrm{sgn}) \otimes \mathrm{sgn}$ pourrait se décompose sous la forme $(W_1 \otimes \mathrm{sgn}) \oplus (W_2 \otimes \mathrm{sgn})$ ce qui est absurde. Nous avons $\chi_{V_1 \otimes \mathrm{sgn}}(g) = \chi_{V_1}(g)\mathrm{sgn}(g)$; ainsi $\chi_{V_1 \otimes \mathrm{sgn}}(C_2) = -1$ est différent de $\chi_{V_1}(C_2) = 1$. Les représentations $V_1 \otimes \mathrm{sgn}$ et V_1 ne sont donc pas isomorphes (leurs caractères sont distincts).

3. Le groupe $\mathfrak{S}_4$ ayant cinq classes de conjugaison, il y a cinq représentations irréductibles. Soient d la dimension de la représentation manquante et θ son caractère. La formule de Burnside assure que
$$24 = 1^2 + 1^2 + 3^2 + 3^2 + d^2$$
d'où $d = 2$.

Pour remplier la dernière ligne on utilise le fait que $\chi_{\rho_{\mathrm{triv}}} + \mathrm{sgn} + 2\theta + 3\chi_1 + 3\chi_2$ est le caractère de la représentation régulière qui est connu [22].

Exercice 510

Soit $\Bbbk$ un corps. Soit $\mathrm{G} \subset \mathrm{GL}(2, \Bbbk)$ le sous-groupe des $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ avec $a \in \Bbbk^*$ et $b \in \Bbbk$. Faisons agir G sur $\Bbbk$ par
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot x = ax + b.$$

1. Calculer
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1}.$$

22. Rappelons que si G est fini, si $E = \mathrm{G}$ et si l'action de G est donnée par la multiplication à gauche, alors la représentation régulière est donnée par : $\chi(1) = |\mathrm{G}|$ et $\chi(g) = 0$ si $g \in \mathrm{G} \smallsetminus \{e\}$.

En déduire que les classes de conjugaison de G sont

$$C_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \qquad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \smallsetminus \{0\} \right\}$$

et les

$$D_a = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \right\}$$

pour $a \in \Bbbk^* \smallsetminus \{1\}$.

2. Supposons désormais que $\Bbbk$ est fini, de cardinal q et donc que $|\mathrm{G}| = q(q-1)$ et G compte q classes de conjugaison. Désignons par V la représentation de permutation de G associée à l'action de G sur $\Bbbk$ et W l'hyperplan de V défini par

$$W = \Big\{ \sum_{x \in \Bbbk} \lambda_x e_x, \sum_{x \in \Bbbk} \lambda_x = 0 \Big\}$$

Montrer que W est une sous-représentation de V.

3. Calculer χ_W ; en déduire que W est irréductible.
4. Quelles sont les dimensions des autres représentations irréductibles de G ?
5. Comment peut-on construire un caractère linéaire de G à partir d'un caractère linéaire de $\Bbbk^*$?

   En déduire que si $\Bbbk = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, alors la table des caractères de G est la suivante

	C_1	N	D_2	D_4	D_3
χ_{triv}	1	1	1	1	1
η	1	1	-1	1	-1
η^2	1	1	1	-1	-1
η^3	1	1	-1	-1	1
χ_W	2	-2	0	0	0

6. Supposons que $q = 4$. Établir la table des caracères de G. Cette table vous rappelle-t-elle quelque chose ? Pouvez-vous expliquer cette coïncidence ?

Éléments de réponse 510

1. Nous avons

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c & ad + (1-c)b \\ 0 & 1 \end{pmatrix}$$

Par suite un conjugué de $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ est de la forme $\begin{pmatrix} c & d' \\ 0 & 1 \end{pmatrix}$ et tout élément de cette forme est un conjugué de $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ si $c \neq 1$.

Les D_a, pour $a \in \Bbbk^* \smallsetminus \{1\}$ forment donc des classes de conjugaison.

Par ailleurs C_1 est la classe de conjugaison de l'élément neutre et N est la classe de conjugaison de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ car pour $a \neq 0$

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

2. Nous avons
$$g \cdot \Big(\sum_{x \in \Bbbk} \lambda_x e_x \Big) = \sum_{x \in \Bbbk} \lambda_x e_{g \cdot x} = \sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} e_x.$$
Or $x \mapsto g^{-1} \cdot x$ est une bijection de $\Bbbk$ donc $\sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} = \sum_{x \in \Bbbk} \lambda_x$ ce qui montre que $g \cdot v = \sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} e_x$ appartient à W si $v = \sum_{x \in \Bbbk} \lambda_x e_x \in W$.

3. V est une représentation de permutation ; par conséquent $\chi_V(g)$ est le nombre de points fixes de g agissant sur $\Bbbk$. Nous sommes donc ramenés à calculer le nombre de solutions de l'équation $ax + b = x$ dans $\Bbbk$ ce qui conduit à
$$\chi_V(C_1) = q, \qquad \chi_V(N) = 0, \qquad \chi_V(D_a) = 1 \text{ si } a \in \Bbbk^* \smallsetminus \{1\}.$$
Maintenant V est la somme directe de W et de la droite engendrée par $\sum_{x \in \Bbbk} e_x$ sur laquelle G agit trivialement. Nous en déduisons $\chi_V(g) = \chi_W(g) + 1$ ce qui conduit à
$$\chi_W(C_1) = q - 1, \qquad \chi_W(N) = -1, \qquad \chi_W(D_a) = 0 \text{ si } a \in \Bbbk^* \smallsetminus \{1\}.$$
Alors
$$\langle \chi_W, \chi_W \rangle = \frac{1}{q(q-1)} \Big((q-1)^2 + |N| \times 1^2 + \sum_{a \in \Bbbk^* \smallsetminus \{1\}} |D_a| \times 0^2 \Big) = \frac{1}{q(q-1)} \Big((q-1)^2 + (q-1) \Big) = 1$$
ce qui assure l'irréductibilité de W [23].

4. Puisque
   - ◇ le nombre de classes de conjugaison de G coïncide avec le nombre de représentations irréductibles de G
   - ◇ G compte q classes de conjugaison

23. Nous utilisons ici le critère d'irréductibilité suivant : une représentation V de G est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.

il y a $q-1$ autres représentaitons irréductibles. Notons d_1, d_2, …, d_{q-1} leurs dimensions. La formule de Burnside assure que

$$q(q-1) = |\mathrm{G}| = (\dim W)^2 + \sum_{i=1}^{q-1} d_i^2;$$

comme $\dim W = q-1$ nous obtenons

$$\sum_{i=1}^{q-1} d_i^2 = q(q-1) - (q-1)^2 = q-1.$$

Une somme de $q-1$ entiers ≥ 1 ne pouvant être égale à $q-1$ que si tous les entiers sont égaux à 1 nous obtenons que les $q-1$ autres représentations de G sont de dimension 1 (*i.e.* sont des caractères linéaires).

5. Si χ est un caractère linéaire de $\Bbbk^*$, alors $\chi \circ \det$ est un caractère linéaire de G. Le groupe $\mathbb{F}_5^*$ est cyclique d'ordre 4 engendré par 2 (en effet $2^2 = 4$, $2^3 = 8 = 3$ et $2^3 = 16 = 1$). Un caractère de $\mathbb{F}_5^*$ est donc déterminé par sa valeur en 2 qui doit être une racine 4-ième de l'unité, c'est-à-dire 1, -1, $\mathbf{i}$ ou $-\mathbf{i}$. On compte donc quatre tels caractères. Si on note η celui pour lequel $\eta(2) = \mathbf{i}$ les autres sont η^2, η^3 et η^4 qui n'est autre que le caractère trivial. Les quatre caractères de G recherchés sont donc exactement les $\eta^j \circ \det$, pour $0 \leq j \leq 3$, ce qui fournit bien la table annoncée.

6. Le groupe $\Bbbk^*$ est d'ordre 3 ; il est donc cyclique, engendré par n'importe quel $a \neq 1$ (en effet si K est un corps fini, alors K^* est toujours cyclique ; dans le cas présent si $a \in K^* \smallsetminus \{1\}$, alors l'ordre du sous-groupe engendré par a divise $|K^*| = 3$, et donc vaut 3 ce qui fait que ce sous-groupe est K^*). Un caractère linéaire de $\Bbbk^*$ est donc déterminé par sa valeur en a qui est une racine cubique de l'unité. Il y a trois tels caractères. Si on note η celui pour lequel $\eta(a) = \mathbf{j} = \exp\left(\frac{2\mathbf{i}\pi}{3}\right)$ les autres sont η^2 et η^3 qui n'est autre que le caractère trivial. Nous obtenons donc la table

	C_1	N	D_a	D_{a^2}
χ_{triv}	1	1	1	1
η	1	1	j	j^2
η^2	1	1	j^2	j
χ_W	3	-1	0	0

Nous reconnaissons la table des caractères de $\mathcal{A}_4$ ce qui n'est pas étonnant car G est isomorphe à $\mathcal{A}_4$. En effet le choix d'une bijection entre $\Bbbk$ et $\{1, 2, 3, 4\}$ transforme l'action de G sur $\Bbbk$ en une action de G sur $\{1, 2, 3, 4\}$ et fournit donc une injection de G dans $\mathfrak{S}_4$. L'image H de cette injection est donc un sous-groupe de $\mathfrak{S}_4$, isomorphe à G. Un tel groupe est distingué dans $\mathfrak{S}_4$; en effet si g n'appartient pas à H nous avons $g\mathrm{H} = \mathrm{H}g = \mathfrak{S}_4 \smallsetminus \mathrm{H}$ pour des raisons d'ordre ($|\mathrm{H}| = |\mathrm{G}| = 12 = |\mathcal{A}_4|$ et $|\mathfrak{S}_4| = 24 = 2|\mathrm{H}|$) et

donc $gHg^{-1} = Hgg^{-1} = H$. Le quotient G/H est de cardinal 2 et donc isomorphe à $\{\pm id\}$ ce qui fournit un caractère linéaire $\eta\colon \mathfrak{S}_4 \to \{\pm id\}$. La restriction de η à $\mathcal{A}_4$ est encore un caractère linéaire mais les caractères de $\mathcal{A}_4$ sont à valeurs dans $\mu_3 = \{z \in \mathbb{C}^* \mid z^3 = 1\}$ ce qui implique $\eta = 1$ sur $\mathcal{A}_4$. Autrement dit $\mathcal{A}_4$ est inclus dans le noyau H de η et lui est donc égal pour des raisons d'ordre. Ainsi $G \simeq \mathcal{A}_4$.

Exercice 511

Soit G un groupe non abélien d'ordre 6.

1. Quels sont les ordres des éléments de G ?
2. Montrer que G a deux caractères irréductibles de degré 1 (notés **1** et η) et un de degré 2 (noté χ).
3. Montrer que G a trois classes de conjugaison. Quelles sont-elles ?
4. Montrer que $\eta(g) = 1$ si g est d'ordre 2 et que $\eta(g) = -1$ si g est d'ordre 2 (on s'intéressera à $\eta(g^2)$). En déduire le cardinal de chaque classe de conjugaison.
5. Dresser la table des caractères de G.

Éléments de réponse 511

Exercice 512

Faisons agir $\mathfrak{S}_n$ sur $\mathbb{C}^n$ par permutation des éléments de la base canonique. Montrer que l'hyperplan $\sum_{i=1}^{n} x_i = 0$ est stable par $\mathfrak{S}_n$ et que la représentation ainsi obtenue est irréductible (considérer $v - \sigma \cdot v$ où σ est une transposition).

En déduire une décomposition de $\mathbb{C}^n$ en somme de représentations irréductibles de $\mathfrak{S}_n$.

Éléments de réponse 512

Exercice 513

Soit G un sous-groupe fini de $GL(n, \mathbb{C})$. Montrer que $\sum_{M \in G} \operatorname{tr} M$ est un entier. Comment cet entier s'interprète-t-il ?

Éléments de réponse 513

Exercice 514

Soit V une représentation de degré fini d'un groupe G (non nécessairement fini).

1. On suppose qu'il existe une forme hermitienne H sur V invariante par G, c'est-à-dire
$$H(u, v) = H(g \cdot u, g \cdot v) \qquad \forall\, u,\, v \in V \quad \forall\, g \in G.$$
Montrer que toute sous-représentation de V admet une sous-représentation supplémentaire.

2. Montrer que si G est fini, alors il existe toujours une telle forme hermitienne G-invariante.
3. On suppose V irréductible. Montrer que deux formes hermitiennes G-invariantes sont multiples l'une de l'autre (c'est-à-dire $H_1 = \mu H_2$).

Éléments de réponse 514

Cet exercice est une (re)démonstration du théorème de Maschke.

1. Soit W une sous-représentation de V. La forme hermitienne H nous donne un moyen canonique de trouver un supplémentaire de W : on prend son orthogonal. Comme H est invariante par G, on en déduit que $W^\perp$ est une sous-représentation de G par le calcul suivant
$$\forall\, g \in \mathrm{G} \quad \forall\, v \in W \quad \forall w \in W^\perp \quad H(v, g \cdot w) = H(g^{-1} \cdot v, w) = 0.$$
2. Soit H_0 une forme hermitienne sur V. Puisque G est fini, on peut définir une forme hermitienne H G-invariante en « moyennant » H_0 par G :
$$H(v, w) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} H_0(g \cdot v, g \cdot w)$$
Remarque : dans une base adéquate, une représentation d'un groupe fini sur un $\mathbb{C}$-espace vectoriel est donc unitaire. En particulier, tous les automorphismes linéaires sont diagonalisables.
3. Soient H et H' deux formes hermitiennes G-invariantes sur V. Alors H induit une bijection anti-linéaire
$$\varphi_H \colon V \to V^* \qquad\qquad v \mapsto (w \to H(w, v)).$$
De plus, comme H est G-invariante, $\varphi_H(g \cdot v) = g \cdot \varphi_H(v)$. L'application $\varphi_{H'}^{-1} \circ \varphi_H$ est donc un G-automorphisme linéaire de V, donc d'après le Lemme de Schur, $\varphi_{H'}^{-1} \circ \varphi_H = \mu \mathrm{id}$, c'est-à-dire $H = \mu H'$.

Exercice 515

Soient p un nombre premier et G un groupe d'ordre p^3 non abélien. On note $\mathbb{U}_p = \{z \in \mathbb{C} \mid z^p = 1\}$.

1. Montrer que les représentations irréductibles de G ont dimension 1 ou p. Que peut-on dire du nombre des représentations de G dans $\mathbb{C}$?
2. Montrer que le nombre de classes d'isomorphie de représentations irréductibles de dimension p de G est $p - 1$ et donner l'ordre de l'abélianisé de G.

   Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$.
3. Montrer que pour tout $\zeta \in \mathbb{U}_p$ il existe une représentation V de dimension 1 de G telle que $\chi_V(g) = \zeta$.

4. Déduire de ce qui précède et du fait que si G est un groupe fini le produit d'un caractère irréductible de G par un caractère de degré 1 est un caractère irréductible de G de même degré que si V est une représentation irréductible de dimension p de G, alors $\chi_V(g) = 0$.
5. Montrer que si V est une représentation de G de dimension n ($n \in \mathbb{N}^*$) alors l'un des nombres $\chi_V(g)$, $\chi_V(g^2)$, …, $\chi_V(g^n)$ est non nul (on pourra considérer la somme $\sum_\lambda C(\lambda)$, où C désigne le polynôme caractéristique de $v \cdot gv$, et λ parcourt ses n valeurs propres).
6. Déduire des questions 4. et 5. que l'abélianisé de G n'est pas cyclique. à quel groupe est-il isomorphe ?
7. Montrer à l'aide de la question 4. que si $g' \in D(\mathrm{G})$ et si (V, ρ) est une représentation irréductible de G alors $|\chi_V(g')| = \dim V$. Préciser les endomorphismes $\rho(g')$ pour g' parcourant $D(\mathrm{G})$.
8. Décrire le centre de G et donner le cardinal des différentes classes de conjugaison de G.
9. Donner explicitement la table des caractères de G lorsque $p = 3$.

Éléments de réponse 515

Soient p un nombre premier et G un groupe d'ordre p^3 non abélien. On note $\mathbb{U}_p = \{z \in \mathbb{C} \,|\, z^p = 1\}$.

1. La dimension des représentations irréductibles de G divise l'ordre de G, donc p^3 ; par la formule de Burnside, la somme des carrés de ces dimensions vaut l'ordre, p^3. Donc les seules valeurs possibles sont 1 et p. On sait que 1 est la dimension de la représentation triviale, irréductible. Et que G possède une représentation irréductible de dimension > 1, car il est non abélien (cours). Donc $\{1, p\}$ est l'ensemble des dimensions des représentations irréductibles de G. On sait qu'une représentation de G dans $\mathbb{C}$ est donnée précisément par un morphisme de G dans $\mathbb{C}^\times$ (*i.e.* un élément du dual G) et que leur nombre est l'ordre de l'abélianisé G_{ab}. En particulier ce nombre divise $|\mathrm{G}| = p^3$.
2. On écrit la formule de Burnside pour G : si r est le nombre de classes d'isomorphie de représentations irréductibles de dimension p de G, on obtient : $p^3 = |\mathrm{G}_{\mathrm{ab}}| + rp^2$. Par suite p^2 divise G_{ab}, qui divise lui-même p^3. Or G n'est pas abélien, donc l'ordre de G_{ab} n'est pas p^3, et c'est p^2. Il suit de la formule que $r = p - 1$.

   Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$.
3. Toute représentation (V, χ) de dimension 1 de G factorise par G_{ab}, d'ordre p^2. Puisque $g \notin D(\mathrm{G})$ on sait qu'il existe χ un caractère de degré 1 tel que $\chi(g) \neq 1$. On a $\chi(g)^{p^2} = 1$; si $\chi(g)$ est d'ordre p dans $\mathbb{C}^\times$, alors il engendre $\mathbb{U}_p$, donc tout $\zeta \in \mathbb{U}_p$ s'écrit $\zeta = \chi(g)^k = \chi^k(g)$ et la représentation $(\mathbb{C}, \chi^k)$ convient pour V. Sinon, $\chi^p(g)$ est d'ordre p, on remplace χ par le caractère χ^p dans l'argument.
4. Supposons $\chi_V(g) \neq 0$. Alors en multipliant χ_V par les p caractères de degré 1 obtenus en 3), on obtient par I 3. p caractères irréductibles de degré p distincts, car leur valeur en g diffère. Or par 2) G n'admet que $p - 1$ caractères irréductibles de degré p, contradiction.

5. Si on note λ_1, λ_2, …, λ_n les n valeurs propres de $\rho_V(g)$ (diagonalisable), alors celles de $\rho_V(g^k)$ sont λ_1^k, λ_2^k, …, λ_n^k. De plus $\rho_V(g)$ est inversible, donc de déterminant d_g non nul. La somme proposée par l'énoncé $\sum_\lambda C(\lambda)$, qui est nulle par définition, s'écrit donc aussi
$$\sum_{k=1}^{n} a_k \chi_V(g^k) + n a_0,$$
où on note $C(X) = \sum_{k=0}^{n} a_k X^k$ ($a_n = 1$, $a_0 = \pm d_g$). Le fait que na_0 soit non nul entraîne ainsi que l'un des $\chi_V(g^k)$, $1 \leq k \leq n$, l'est également.

6. Si l'abélianisé de G était cyclique, il serait engendré par la classe, d'ordre p^2, d'un certain élément g de $\mathrm{G} \smallsetminus D(\mathrm{G})$. On applique alors 5) à g et V une représentation irréductible de G de dimension p : avec 4) on en déduit que l'un des g^i, $1 \leq i \leq p$ est dans $D(\mathrm{G})$. Mais alors l'ordre de la classe de g dans l'abélianisé serait majorée par $i \leq p$, contradiction. Par suite G_{ab} est un groupe abélien d'ordre p^2, non cyclique. Par le théorème de structure des groupes abéliens finis, on a $\mathrm{G}_{\mathrm{ab}} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

7. Si $\dim V = 1$, alors $\chi_V(g') = 1$ pour tout $g' \in D(\mathrm{G})$ car χ_V est un morphisme dans $\mathbb{C}^\times$ abélien. Sinon, $\dim V = p$ et on écrit que le carré hermitien de χ_V vaut 1 : d'après 4), on trouve $\sum_{g' \in D(\mathrm{G})} |\chi_V(g')|^2 = p^3$. Or pour tout g' on sait que $|\chi_V(g')| \leq p = \dim V$. Puisque $|D(\mathrm{G})| = p$, ceci entraîne l'égalité $|\chi_V(g')| = p$ pour tout g'. Le cours montre que l'égalité $|\chi_V(g')| = \dim V$ a lieu si et seulement si $\rho_V(g')$ est une homothétie. Or si $g' \neq 1$, g' est d'ordre p donc l'ordre de $\rho_V(g')$ est 1 ou p. Si c'était 1, alors g' et donc $D(\mathrm{G})$ seraient dans le noyau de ρ_V ; ainsi ρ_V factoriserait en un morphisme de G_{ab} abélien dans $\mathrm{GL}(V)$, ce qui contredit le fait que V est irréductible de dimension > 1. Donc $\rho_V(g')$ est une homothétie d'ordre p, de rapport une racine primitive $p$ième ζ de 1. Alors on a $D(\mathrm{G}) = \{g'^{\ell} \mid 0 \leq \ell \leq p-1\}$, et chaque $\rho(g'^{\ell})$ est l'homothétie de V de rapport ζ^ℓ.

8. D'après 7., les p éléments de $D(\mathrm{G})$ ont pour carré hermitien de leur colonne associée dans la table de caractères de G la valeur $|\mathrm{G}| = p^3$ obtenue (Burnside) pour la colonne de 1, donc leur centralisateur est G, *i.e.* ils sont dans le centre de G. Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$. Par 4., g n'est pas dans le centre car il n'agit pas comme une homothétie sur V irréductible de dimension p (en effet, on sait que $\rho_V(g)$ est alors un G–morphisme, donc par Schur une homothétie). Or le centralisateur de g contient g et $D(\mathrm{G})$, donc ce sous-groupe a cardinal $> p$, et distinct de p^3, soit exactement p^2 par Lagrange. Le cardinal de la classe de conjugaison de g est donc $\frac{p^3}{p^2} = p$ (toute la classe a même image dans l'abélianisé, par cardinalité elle coïncide donc avec la classe à droite $gD(\mathrm{G})$). On obtient en particulier que le centre de G est égal à $D(\mathrm{G})$.

9. On note x un générateur de $D(\mathrm{G})$ (d'ordre 3), et g_{ij} un élément de $\mathrm{G} \smallsetminus D(\mathrm{G})$ qui s'envoie sur $(\bar{i}, \bar{j})$ dans le quotient G_{ab}, identifié au groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. On a $Z(\mathrm{G}) = D(\mathrm{G})$,

et la classe de conjugaison de g_{ij} dans G est $g_{ij}\langle x\rangle$ (cf. 8.). Ainsi la partie haute de la table privée des colonnes de x et x^2 est la table de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (groupe abélien, donc isomorphe à son groupe dual). Les deux représentations de degré 3, duales l'une de l'autre, correspondent sur $Z(\mathrm{G}) = D(\mathrm{G})$ à une action fidèle par homothéties, et on a $\rho(x^2) = \rho(x)^2$. Leurs caractères sont conjugués.

	1	x	x^2	g_{10}	g_{20}	g_{01}	g_{02}	g_{11}	g_{22}	g_{12}	g_{21}
χ_{00}	1	1	1	1	1	1	1	1	1	1	1
χ_{10}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$
χ_{20}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$
χ_{01}	1	1	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$
χ_{02}	1	1	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$
χ_{11}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$	1	1
χ_{22}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$	1	1
χ_{12}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$	1	1	$\mathbf{j}^2$	$\mathbf{j}$
χ_{21}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$	1	1	$\mathbf{j}$	$\mathbf{j}^2$
χ'	3	$3\mathbf{j}$	$3\mathbf{j}^2$	0	0	0	0	0	0	0	0
χ''	3	$3\mathbf{j}^2$	$3\mathbf{j}$	0	0	0	0	0	0	0	0

Exercice 516

1. Soit G un groupe abélien fini. Pour $g \in \mathrm{G}$ notons δ_g l'élément de $\mathbb{C}[\mathrm{G}]$ qui vaut 1 en g et 0 sur $\mathrm{G} \smallsetminus \{g\}$.
   a) Énoncer la formule d'inversion de Fourier et l'appliquer aux éléments δ_g de $\mathbb{C}[\mathrm{G}]$.
   b) En déduire que le morphisme naturel de G dans son bidual $\widehat{\widehat{\mathrm{G}}}$ est injectif.
2. Soit V une représentation d'un groupe fini G qui est somme directe de r représentations irréductibles deux à deux non isomorphes.
   a) Décrire l'algèbre $\mathrm{End}_{\mathrm{G}}(V)$ des G-endomorphismes de V.
   b) Déterminer toutes les sous–représentations de V.
3. Soit G un groupe fini. Montrer que le produit d'un caractère irréductible de G par un caractère de degré 1 est un caractère irréductible de G de même degré.

Éléments de réponse 516

1. Soit G un groupe abélien fini. Pour $g \in \mathrm{G}$ notons δ_g l'élément de $\mathbb{C}[\mathrm{G}]$ qui vaut 1 en g et 0 sur $\mathrm{G} \smallsetminus \{g\}$.

a) Pour toute f dans $\mathbb{C}[\mathrm{G}]$, nous avons

$$f = \frac{1}{|\mathrm{G}|} \sum_{\xi \in \widehat{\mathrm{G}}} \widehat{f}(\chi)\chi^{-1}$$

Et

$$\widehat{\delta_g}(\chi) = \sum_{g'} \delta_g(g')\chi(g') = \chi(g).$$

Ainsi

$$\delta_g = \frac{1}{|\mathrm{G}|} \sum_{\chi \in \widehat{\mathrm{G}}} \chi(g)\chi^{-1}.$$

b) Soit $g \in \mathrm{G}$. Par a), la transformée de Fourier de δ_g est l'application $\chi \mapsto \chi(g)$. Elle s'identifie donc à l'image naturelle de g dans son bidual. Un élément g est dans le noyau de ce morphisme naturel d'évaluation si et seulement si tous les caractères $\chi \in \widehat{\mathrm{G}}$ y valent 1, c'est-à-dire si et seulement si g a même transformée de Fourier que 1. Par la formule d'inversion ceci équivaut à $g = 1$.

2. Soit V une représentation d'un groupe fini G qui est somme directe de r représentations irréductibles deux à deux non isomorphes.

a) Si $V = \bigoplus_{i=1}^{r} V_i$, alors chaque élément de $\mathrm{End}_{\mathrm{G}}(V)$ se « décompose » en une somme directe de G-morphismes de V_i dans V_j, pour (i, j) variant dans $\{1, \ldots, r\} \times \{1, \ldots, r\}$. Par le lemme de Schur, les G-morphismes entre irréductibles non isomorphes sont nuls, et $\mathrm{End}_{\mathrm{G}}(V_i) = \mathbb{C}\mathrm{id}_{V_i}$. Nous en déduisons que l'algèbre $\mathrm{End}_{\mathrm{G}}(V)$ s'identifie au produit des algèbres $\mathbb{C}\mathrm{id}_{V_i}$ (blocs diagonaux d'une homothétie sur chaque V_i).

b) On utilise l'unicité de la décomposition canonique de V : par l'hypothèse, toutes les composantes isotypiques de V sont irréductibles, et les sous-représentations sont toutes les sommes (directes) de certaines de ces composantes. (Attention, si une représentation irréductible apparaissait dans V avec multiplicité > 1, la composante isotypique correspondante, et par suite V, possèderait une infinité de sous-représentations irréductibles, toutes isomorphes !)

3. Soit G un groupe fini.

Le produit des caractères de deux représentations V et (W, ρ) est le caractère de la représentation $\mathrm{Hom}(V^*, W)$, où V^* est la représentation duale de V. Ou encore : si $\dim V = 1$, ce produit est le caractère de la représention $\chi_V \cdot \rho$ de G sur W ($g \cdot w =: \chi_V(g) \cdot \rho(g)(w) \in W$). Le degré de ce caractère produit est sa valeur en 1, donc clairement le degré de χ_W. L'irréductibilité du produit (valable si $\dim V = 1$!) s'obtient facilement en calculant le carré hermitien de $\chi_V\chi_W$, égal à celui de χ_W (car χ_V, morphisme de G dans $\mathbb{C}^\times$, a pour valeurs des racines de l'unité donc de module 1), donc ce carré hermitien vaut 1 par l'irréductibilité de χ_W. On peut aussi remarquer qu'une sous–représentation de $(W, \chi_V \cdot \rho)$,

c'est-à-dire un sous-espace vectoriel stable pour l'action correspondante de G, est une sous–représentation de (W, ρ), donc $\{0\}$ ou W.

Exercice 517

Soit C le cube de l'espace euclidien $\mathbb{R}^3$ dont les huit sommets ont pour coordonnées $(\pm 1, \pm 1, \pm 1)$. Soit G le groupe des isométries de $\mathbb{R}^3$ qui laissent stable le cube, *i.e.* permutent ses huit sommets. Soit T le tétraèdre de sommets $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$.

a) Montrer que C est réunion de T et de τT, où $\tau = -\mathrm{id}$.

b) Soit $S(T)$ le groupe des isométries de T. Montrer que G est produit direct de $S(T) \simeq \mathfrak{S}_4$ et de $\{\mathrm{id}, \tau\}$.

c) Montrer que G a deux fois plus de caractères irréductibles que $\mathfrak{S}_4$.

d) Décrire les caractères irréductibles de G et écrire sa table de caractères.

Éléments de réponse 517

Exercice 518

Soit G un groupe abélien infini. Soit p un nombre premier ; supposons que tout élément x de G vérifie $x^p = 1$.

a) Soit n un entier positif. Montrer que si $\Bbbk$ est un corps de caractéristique différente de p, alors G ne peut pas être un sous-groupe de $\mathrm{GL}(n, \Bbbk)$.

b) Soit $\Bbbk$ un corps quelconque. Montrer que le groupe infini $\mathbb{Z}/2\mathbb{Z}^{\mathbb{N}} \times \mathbb{Z}/3\mathbb{Z}^{\mathbb{N}}$ n'admet pas de représentation linéaire fidèle de dimension finie sur $\Bbbk$.

Éléments de réponse 518

1.13. À classer

Exercice 519 Soit G un groupe fini dont tout sous-groupe propre est cyclique.

1. G est-il nécessairement cyclique, abélien ?
2. Si G est de plus supposé abélien, G est-il cyclique ?

Éléments de réponse 519

1. La réponse est négative. Par exemple le groupe $\mathrm{G} = \mathfrak{S}_3$ n'est pas abélien et ses sous-groupes propres, qui sont d'ordre 2 ou 3, sont cycliques. Autre exemple : le groupe des quaternions est non abélien et ses sous-groupes propres sont $\langle -1 \rangle$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$.
2. La réponse est négative. Ainsi le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ où p est premier a tous ses éléments non nuls d'ordre p et n'est donc pas cyclique. Cependant ses sous-groupes sont d'ordre 1 ou p et sont donc cycliques.

Exercice 520 Soit $n \in \mathbb{N}^*$ un entier. Soit G un groupe d'ordre n. Soit p un diviseur premier de n.

1. Montrer que G a au plus $\frac{n-1}{p-1}$ sous-groupes d'ordre p.
2. Donner un exemple où on a exactement $\frac{n-1}{p-1}$ sous-groupes d'ordre p.

Éléments de réponse 520

1. Soient H et K deux sous-groupes d'ordre p de G. Si $\mathrm{H} \cap \mathrm{K} \neq \{1\}$, alors il existe $x \in \mathrm{H} \cap \mathrm{K}$ tel que $x \neq 1$; en particulier x est d'ordre > 1. D'après le Théorème de Lagrange l'ordre de x divise $|\mathrm{H}| = |\mathrm{K}| = p$. Comme p est premier x est donc nécessairement d'ordre p et $\mathrm{H} = \mathrm{K} = \langle x \rangle$. Ainsi deux sous-groupes d'ordre p de G sont soit égaux, soit ont pour seul élément commun l'élément neutre 1. Notons k le nombre de sous-groupes d'ordre p de G et soient H_1, H_2, …, H_k les k sous-groupes d'ordre p (distincts) de G. Posons $A_i = \mathrm{H}_i \smallsetminus \{e\}$. Nous avons l'inclusion de l'union disjointe suivante dans G :
$$\{1\} \sqcup \bigsqcup_{i=1}^{k} A_i \subset \mathrm{G}$$
d'où
$$|\{1\}| + \sum_{i=1}^{k} |A_i| \leq |\mathrm{G}|.$$
Mais $|\mathrm{G}| = n$, $|A_i| = |\mathrm{H}| - 1 = p - 1$ donc $1 + \sum_{i=1}^{k}(p-1) \leq n$ soit $1 + k(p-1) \leq n$ ou encore $k \leq \frac{n-1}{p-1}$.
2. Considérons le groupe $\mathrm{G} = \mathbb{Z}/p\mathbb{Z}$; alors $n = p$ et $k = 1 = \frac{n-1}{p-1}$.

Exercice 521 Soit $n \in \mathbb{N}^*$.

1. Donner un élément d'ordre n de $\mathfrak{S}_n$.
2. Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$ un sous-groupe distingué de $\mathfrak{S}_n$ contenant une transposition. Montrer que $\mathrm{H} = \mathfrak{S}_n$.

Éléments de réponse 521

1. Soit σ l'élément défini par $\sigma(i) = i + 1$ pour tout $1 \leq i \leq n-1$ et $\sigma(n) = 1$. On vérifie par récurrence que $\sigma^k(1) = k + 1$ pour $1 \leq k \leq n-1$ et que $\sigma^n = \mathrm{id}$. Ainsi $\sigma^k \neq \mathrm{id}$ pour $1 \leq k \leq n-1$ et $\sigma^n = \mathrm{id}$; autrement dit σ est d'ordre n.
2. Si H contient une transposition τ_{ij} et si τ est une autre transposition, alors il existe un élément g dans $\mathfrak{S}_n$ tel que $\tau = g\tau_{ij}g^{-1}$ et H étant distingué dans G, $g\tau_{ij}g^{-1}$ appartient à H, *i.e.* τ appartient à H. Ainsi H contient toutes les transpositions.

   Il en résulte que H contient donc aussi le sous-groupe engendré par toutes les transpositions. Mais les transpositions engendrent $\mathfrak{S}_n$. Par suite $\mathrm{H} = \mathfrak{S}_n$.

Exercice 522 Pour tout entier $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple. Dans l'exercice qui suit nous montrons que parmi les groupes à 60 éléments la simplicité caractérise $\mathcal{A}_5$.

Soit G un groupe simple à 60 éléments. Nous allons montrer que G est isomorphe à $\mathcal{A}_5$.

1. Montrer que le groupe $\mathcal{A}_5$ est simple (Indication : penser à dénombrer).
2. Montrer que G possède exactement six sous-groupes d'ordre 5.
3. Désignons par X l'ensemble des 5-Sylow de G. Construire un morphisme injectif φ de G dans le groupe des permutations de X.
4. Montrer que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$ (où $\mathcal{A}_X$ désigne l'ensemble des permutations de X de signature 1).
5. Notons $E = {}^{\mathcal{A}_X}\!/_{\varphi(\mathrm{G})}$ l'ensemble des classes à gauche. On définit un morphisme ψ de $\mathcal{A}_X$ dans $\mathfrak{S}_E$ de la manière suivante

$$\begin{array}{rcl} \psi\colon \mathcal{A}_X & \to & \mathfrak{S}_E \\ x & \mapsto & \psi_x\colon E \to E \\ & & a\varphi(\mathrm{G}) \mapsto xa\varphi(\mathrm{G}) \end{array}$$

Montrer que ψ est injectif. Conclure que G est isomorphe à $\mathcal{A}_5$.

Éléments de réponse 522

1. Cette question se résout par dénombrement. Le groupe $\mathcal{A}_5$ possède
   - ◇ un élément d'ordre 1 (l'élément neutre),
   - ◇ quinze éléments d'ordre 2 (ce sont les produits de deux transpositions à supports disjoints),
   - ◇ vingt éléments d'ordre 3 (les 3-cycles),
   - ◇ vingt-quatre éléments d'ordre 5 (les autres).

   Si σ appartient à $\mathfrak{S}_5$ et si $(a_1\ a_2\ \ldots\ a_k)$ est un cycle, on a alors la formule suivante

$$\sigma(a_1\ a_2\ \ldots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)).$$

   On en déduit que tous éléments d'ordre 2 sont conjugués dans $\mathcal{A}_5$ et qu'il en est de même pour les 3-cycles. Ainsi si G est un sous-groupe distingué dans $\mathcal{A}_5$ et s'il contient un élément d'ordre 2, il les contient tous. Il en est de même pour les éléments d'ordre 3. Finalement s'il contient un élément d'ordre 5, alors il contient le 5-Sylow qu'il engendre. Comme tous les 5-Sylow sont conjugués, il contient tous les éléments d'ordre 5. Pour conclure il suffit maintenant de remarquer qu'aucune somme d'au moins deux entiers distincts pris parmi 1, 15, 20 ou 24 ne divise l'entier 60 (sauf 60). Le groupe $\mathcal{A}_5$ est donc simple.

2. On décompose 60 en facteurs premiers : $60 = 2^2 \times 3 \times 5$. Soit n_5 le nombre de 5-Sylow. D'une part $n_5 \equiv 1 \bmod 5$, d'autre part $n_5 | 60$ (car G agit transitivement sur les 5-Sylow par conjugaison). Comme G est simple, $n_5 \neq 1$ (en effet si n_5 alors G contient un unique 5-Sylow qui est distingué dans G). Il en résulte que $n_5 = 6$.

3. On peut faire agir G sur X par conjugaison ce qui induit un morphisme $\varphi\colon \mathrm{G} \to \mathfrak{S}_X$ défini de la manière suivante :

$$\begin{array}{rcl} \varphi\colon \mathrm{G} & \to & \mathfrak{S}_X \\ g & \mapsto & \varphi_g\colon X \to X \\ & & \qquad S \mapsto \varphi(g)(S) = gSg^{-1} \end{array}$$

   Ce morphisme n'est pas trivial car les 5-Sylow sont conjugués. L'action de G sur X est donc transitive. Comme G est simple, le noyau de φ doit être trivial. Par conséquent φ est bien injectif.

4. Soit H un groupe. Notons $D(\mathrm{H})$ son groupe dérivé. En passant au groupe dérivé l'inclusion $\varphi(\mathrm{G}) \subset \mathfrak{S}_X$ nous obtenons

$$D(\varphi(\mathrm{G})) \subset D(\mathfrak{S}_X) = \mathcal{A}_X.$$

   Comme G est simple il en est de même pour $\varphi(\mathrm{G})$. De plus $\varphi(\mathrm{G})$ possède aussi six 5-Sylow et donc n'est pas abélien. On en déduit alors $D(\varphi(\mathrm{G})) = \varphi(\mathrm{G})$ (le sous-groupe dérivé est toujours distingué). On a bien montré que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$.

5. Si x appartient à $\ker\psi$, alors $x\varphi(\mathrm{G}) = \varphi(\mathrm{G})$; ainsi x appartient à $\varphi(\mathrm{G})$ et $\ker\psi \subset \varphi(\mathrm{G})$. Le morphisme ψ ne peut donc pas être trivial pour des raisons de cardinalité (la partie $\varphi(\mathrm{G})$ est strictement contenue dans $\mathcal{A}_X$ de cardinal 360). Puisque $\mathcal{A}_X \simeq \mathcal{A}_6$ est simple on en déduit que ψ est injectif.

   Comme précédemment, en passant aux sous-groupes dérivés on sait également que $\psi(\varphi(\mathrm{G})) \subset \mathcal{A}_E$. Finalement on remarque que

$$\forall\, x \in \varphi(\mathrm{G}) \qquad \psi(x)(\varphi(\mathrm{G})) = x\varphi(\mathrm{G}) = \varphi(\mathrm{G}).$$

   Ainsi l'image de ψ est incluse dans le groupe des permutations de E qui fixent $\varphi(\mathrm{G}) \in E$. On note A le sous-groupe de $\mathcal{A}_E$ formé de telles permutations. Comme de plus E possède six éléments, $A \simeq \mathcal{A}_5$ et, pour des raisons de cardinalité, ψ est un bien isomorphisme de $\varphi(\mathrm{G})$ sur A. Nous avons donc montré que $\mathrm{G} \simeq \mathcal{A}_5$.

Exercice 523

1. Lemme de Cauchy. Soit G un groupe fini ; notons e son élément neutre. Soit p un nombre premier qui divise $|\mathrm{G}|$. Définissons l'ensemble

$$E = \{(x_1, x_2, \ldots, x_p) \in \mathrm{G}^p \mid x_1 x_2 \ldots x_p = e\}$$

   En faisant agit $\mathbb{Z}/p\mathbb{Z}$ sur E montrer que G possède un élément d'ordre p.

Supposons jusqu'à la fin de l'exercice que Aut(G) agit transitivement sur l'ensemble $\mathrm{G} \setminus \{e\}$.

2. Montrer que G est un p-groupe, c'est-à-dire qu'il existe un entier naturel n tel que $|\mathrm{G}| = p^n$.
3. Montrer que le centre de G est non trivial.
4. Conclure que $\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

Éléments de réponse 523

1. Soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$, *i.e.* $(x_2, x_3, \ldots, x_p, x_1)$ appartient à E. Notons c le cycle $(1\ 2\ \ldots\ p)$ de $\mathfrak{S}_p$. Il s'agit d'un élément d'ordre p qui engendre un sous-groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Nous définissons une opération de K sur l'ensemble G^p par

$$c \cdot (x_1, x_2, \ldots, x_p) = (x_{c(1)}, x_{c(2)}, \ldots, x_{c(p)}) = (x_2, x_3, \ldots, x_p, x_1).$$

La remarque ci-dessus montre que E est stable par cette opération.

Si x appartient à E, nous notons $\mathcal{O}(x)$ l'orbite de x sous l'action de G. Les éléments de E^{K} sont exactement les éléments x de E tels que $\mathcal{O}(x) = \{x\}$. Notons ω_1, ω_2, …, ω_r les orbites de E de cardinal strictement supérieur à 1. Si x_i est un élément de ω_i, alors $|\omega_i| = [\mathrm{G} : \mathrm{G}_{x_i}]$, c'est donc une puissance de p. Il résulte de l'équation aux classes que

$$|E| = |E^{\mathrm{K}}| + \sum_{i=1}^{r} |\omega_i| \equiv |E^{\mathrm{K}}| \mod p$$

Nous avons $|E| \equiv |E^{\mathrm{K}}| \mod p$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, …, x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n, $|E^{\mathrm{K}}|$ est nul modulo p. Or les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Notons que E^{K} contient le p-uplet $(e, e, \ldots, e)$; en particulier E^{K} est non vide et par suite le cardinal de E^{K} est supérieur à p. Il y a donc au moins $(p-1)$ éléments d'ordre p dans G.

2. Soit x un élément d'ordre p (l'existence d'un tel élément est assuré par le Lemme de Cauchy que nous venons de redémontrer). Soit $y \in \mathrm{G} \setminus \{e\}$. Par hypothèse il existe un automorphisme φ de G tel que $\varphi(x) = y$. On en déduit que

$$y^p = \varphi(x)^p = \varphi(x^p) = \varphi(e) = e$$

ce qui prouve que y est d'ordre p. On vient de montrer que p est le seul nombre premier qui divise $|\mathrm{G}|$. En effet si q en est un autre, il existe d'après la question précédente un élément d'ordre q et nécessairement $q = p$. Il existe donc un entier n tel que $|\mathrm{G}| = p^n$.

3. Faisons agir G sur lui-même par conjugaison, *i.e.* considérons l'action donnée par l'application $(g_1, g_2) \mapsto g_1 g_2 g_1^{-1}$. En reprenant les notations utilisées précédemment l'équation aux classes s'écrit
$$p^n = |\mathrm{G}| = |\mathrm{G}^{\mathrm{G}}| + \sum_{x \in A} |\mathcal{O}(x)|$$
où G^{G} est l'ensemble des éléments de G laissés fixes par l'action de G et A est un système de représentants de chaque orbite non trivial. Remarquons que $\mathrm{G}^{\mathrm{G}} = Z(\mathrm{G})$. Autrement dit
$$p^n = |\mathrm{G}| = |Z(\mathrm{G})| + \sum_{x \in A} \frac{|\mathrm{G}|}{|\mathrm{G}_x|} = |Z(\mathrm{G})| + \sum_{x \in A} \frac{|p^n|}{|\mathrm{G}_x|}$$
ou encore
$$|Z(\mathrm{G})| = p^n - \sum_{x \in A} \frac{|p^n|}{|\mathrm{G}_x|}.$$
Ceci entraîne que p divise $|Z(\mathrm{G})|$ et donc $|Z(\mathrm{G})| \neq 1$.

4. Soit g un élément de $Z(\mathrm{G}) \setminus \{e\}$ et soit g' un élément de $\mathrm{G} \setminus \{e\}$. Par hypothèse il existe un automorphisme φ de G tel que $\varphi(g) = g'$. Par suite
$$\forall\, h \in \mathrm{G} \qquad g'h = \varphi(g\varphi^{-1}h) = \varphi(\varphi^{-1}hg) = hg'$$
ce qui prouve que g' appartient au centre de G et donc que G est abélien. Si on note $+$ la loi de groupe de G on vérifie que l'action de $\mathbb{Z}/p\mathbb{Z}$ sur G (bien) définie par
$$\overline{k} \cdot g = \underbrace{g + g + \ldots + g}_{k \text{ termes}}$$
munit alors $(\mathrm{G}, +, \cdot)$ d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Sa dimension est donc nécessairement n et
$$\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n.$$

Exercice 524

Soit G un groupe fini dont tout sous-groupe propre est cyclique.

1. G est-il nécessairement cyclique, abélien ?
2. Si G est de plus supposé abélien, G est-il cyclique ?

Éléments de réponse 524

Exercice 525 Soit $n \in \mathbb{N}^*$ un entier. Soit G un groupe d'ordre n. Soit p un diviseur premier de n.

1. Montrer que G a au plus $\frac{n-1}{p-1}$ sous-groupes d'ordre p.
2. Donner un exemple où on a exactement $\frac{n-1}{p-1}$ sous-groupes d'ordre p.

Éléments de réponse 525

Exercice 526 Soit $n \in \mathbb{N}^*$.

1. Donner un élément d'ordre n de $\mathfrak{S}_n$.
2. Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$ un sous-groupe distingué de $\mathfrak{S}_n$ contenant une transposition. Montrer que $\mathrm{H} = \mathfrak{S}_n$.

Éléments de réponse 526

Exercice 527 Pour tout entier $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple. Dans l'exercice qui suit nous montrons que parmi les groupes à 60 éléments la simplicité caractérise $\mathcal{A}_5$.

Soit G un groupe simple à 60 éléments. Nous allons montrer que G est isomorphe à $\mathcal{A}_5$.

1. Montrer que le groupe $\mathcal{A}_5$ est simple (Indication : penser à dénombrer).
2. Montrer que G possède exactement six sous-groupes d'ordre 5.
3. Désignons par X l'ensemble des 5-Sylow de G. Construire un morphisme injectif φ de G dans le groupe des permutations de X.
4. Montrer que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$ (où $\mathcal{A}_X$ désigne l'ensemble des permutations de X de signature 1).
5. Notons $E = {}^{\mathcal{A}_X}\!/_{\varphi(\mathrm{G})}$ l'ensemble des classes à gauche. On définit un morphisme ψ de $\mathcal{A}_X$ dans $\mathfrak{S}_E$ de la manière suivante

$$\begin{array}{rcl} \psi\colon \mathcal{A}_X & \to & \mathfrak{S}_E \\ x & \mapsto & \psi_x\colon E \to E \\ & & a\varphi(\mathrm{G}) \mapsto xa\varphi(\mathrm{G}) \end{array}$$

Montrer que ψ est injectif. Conclure que G est isomorphe à $\mathcal{A}_5$.

Éléments de réponse 527

Exercice 528

1. Lemme de Cauchy. Soit G un groupe fini ; notons e son élément neutre. Soit p un nombre premier qui divise $|\mathrm{G}|$. Définissons l'ensemble

$$E = \{(x_1, x_2, \ldots, x_p) \in \mathrm{G}^p \mid x_1x_2\ldots x_p = e\}.$$

En faisant agit ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ sur E montrer que G possède un élément d'ordre p.

Supposons jusqu'à la fin de l'exercice que $\mathrm{Aut}(\mathrm{G})$ agit transitivement sur l'ensemble $\mathrm{G} \setminus \{e\}$.

2. Montrer que G est un p-groupe, c'est-à-dire qu'il existe un entier naturel n tel que $|\mathrm{G}| = p^n$.

3. Montrer que le centre de G est non trivial.
4. Conclure que $\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

Éléments de réponse 528

1.14. Groupe des permutations

Exercice 529

Dans le groupe symétrique $\mathfrak{S}_5$, combien y a-t-il de 5-cycles distincts ? de 4-cycles distincts ?

Éléments de réponse 529

L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire, c'est-à-dire :

$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$

de sorte que chaque classe est constituée de 5 éléments. On obtient alors $\binom{5}{5}(5-1)!$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le même raisonnement donne $\binom{4}{5}3!$.

Plus généralement le nombre de r-cycles dans $\mathfrak{S}_n$ est $\binom{n}{r}(r-1)!$.

Exercice 530

Soient $p \geq 5$ un nombre premier et $\mathrm{H} \subset \mathfrak{S}_p$ un sous-groupe tel que $1 < [\mathfrak{S}_p : \mathrm{H}] < p$.

1. Montrer que tout cycle d'ordre p est contenu dans H.
2. Montrer que tout cycle d'ordre 3 est produit de deux cycles d'ordre p.
3. Montrer que $\mathrm{H} = \mathcal{A}_p$.
4. Montrer que $\mathfrak{S}_5$ ne contient aucun sous-groupe d'ordre 30, 40.

Éléments de réponse 530

1. Soit c un p-cycle et soit $\overline{c}$ son image dans $\mathfrak{S}_p/\mathrm{H}$ qui n'est qu'un ensemble et n'est pas muni de structure de groupe car H n'est pas distingué dans $\mathfrak{S}_p$. L'ensemble $\mathfrak{S}_p/\mathrm{H}$ étant de cardinal strictement inférieur à p, on en déduit qu'il existe $0 \leq i < j < p$ tel que $\overline{c^i} = \overline{c^j}$ de sorte qu'il existe $h \in \mathrm{H}$ tel que $c^j = c^i h$ soit $c^{j-i} \in \mathrm{H}$. Or p étant premier, il existe u et v tel que $u(j-i) + vp = 1$ de sorte que $c^{(j-i)u} = c \in \mathrm{H}$ (car $c^p = \mathrm{id}$ puisque c est un p-cycle).
2. On remarque que

$$(1\ 3\ 2\ 4\ \ldots\ p)^{-1} \circ (1\ 2\ 3\ \ldots\ p) = (1\ 3\ 2)$$

de sorte que pour un 3-cycle quelconque $(a\ b\ c)$ nous avons

$$(a\ b\ c) = (a\ b\ c\ i_1\ \ldots\ i_{p-3})^{-1} \circ (a\ c\ b\ i_1\ \ldots\ i_{p-3})$$

où $\{i_1, \ldots, i_{p-3}\} = \{1, \ldots, n\} \setminus \{a, b, c\}$.

3. Le groupe $\mathcal{A}_p$ étant engendré par les 3-cycles qui d'après la question précédente appartiennent à H, nous obtenons que $\mathcal{A}_p \subset \mathrm{H} \subset \mathfrak{S}_p$ de sorte que $\frac{p!}{2}$ divise l'ordre de H qui est lui-même un diviseur de $p!$. Comme H est un sous-groupe strict de $\mathfrak{S}_p$, nous en déduisons que H est d'ordre $\frac{p!}{2}$ et donc que $\mathcal{A}_p = \mathrm{H}$.
4. Appliquons ce qui précède au cas $p = 5$. Si H était un sous-groupe de $\mathfrak{S}_5$ de cardinal 30 (resp. 40), il serait d'indice 4 (resp. 3) de sorte qu'il devrait contenir $\mathcal{A}_5$ ce qui n'est pas possible.

Exercice 531

Quel est l'ordre maximal d'un élément de $\mathfrak{S}_5$?

Éléments de réponse 531

Soit σ un élément de $\mathfrak{S}_5$. Soit $\sigma = c_1 \circ c_2 \circ \ldots \circ c_r$ la décomposition en cycles à supports disjoints de σ. Chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints de sorte que l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leq i \leq r$. En particulier dans $\mathfrak{S}_5$ on trouve que l'ordre maximal d'un élément est 6.

Exercice 532

Le groupe $\mathcal{A}_4$ est-il simple ? le groupe $\mathfrak{S}_4$ est-il simple ?

Éléments de réponse 532

Le groupe $\mathcal{A}_4$ n'est pas simple : le groupe

$$\mathcal{K} \simeq \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué non trivial et strict de $\mathcal{A}_4$.

Le groupe $\mathfrak{S}_4$ n'est pas simple : le groupe $\mathcal{A}_4$ est un sous-groupe distingué non trivial et strict de $\mathfrak{S}_4$.

Exercice 533

Décomposer la permutation $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2)$ en produit de cycles à support disjoint.

Éléments de réponse 533

On a $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2) = (2\ 1\ 4\ 5)$.

Exercice 534

Exprimer comme produit de cycles disjoints :

1. $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$;
2. $(1\ 2)(1\ 2\ 3)(1\ 2)$.

Quelle est la signature de ces permutations ?

Éléments de réponse 534

1. Posons $\sigma_1 = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$. Explicitons σ_1 :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 1\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 6\ 7\ 8\ 9\ 1 \\ 4\ 2\ 3\ 5\ 6\ 7\ 8\ 9\ 1 \\ 4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2 \end{array}$$

   Donc $\sigma_1 = (4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2)$.

   C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

2. Posons $\sigma_2 = (1\ 2)(1\ 2\ 3)(1\ 2)$. Explicitons σ_2 :

$$\begin{array}{c} 1\ 2\ 3 \\ 2\ 1\ 3 \\ 3\ 2\ 1 \\ 3\ 1\ 2 \end{array}$$

   Ainsi $\sigma_2 = (3\ 1\ 2)$.

   C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

Exercice 535

Calculer aba^{-1} pour

1. $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$;
2. $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$.

Éléments de réponse 535

1. Calcul de aba^{-1} pour $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$.

   Explicitons a :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 1\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 3\ 5\ 4\ 1\ 6\ 7\ 8\ 9 \end{array}$$

   autrement dit $a = (1\ 2\ 3\ 5)$. Il s'en suit que

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9 \end{array}$$

Finalement nous obtenons

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$
$$5\ 1\ 2\ 4\ 3\ 6\ 7\ 8\ 9$$
$$7\ 5\ 2\ 4\ 3\ 6\ 9\ 8\ 1$$
$$7\ 1\ 3\ 4\ 5\ 6\ 9\ 8\ 2$$

2. Calcul de aba^{-1} pour $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$. Les cycles a et b sont à supports disjoints donc commutent. Ainsi $aba^{-1} = aa^{-1}b = b$, autrement dit $aba^{-1} = b$.

Exercice 536 Considérons les éléments suivants de $\mathfrak{S}_5$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

1. Calculer les puissances successives et déterminer l'ordre de σ.
2. Calculer les puissances successives et déterminer l'ordre de ρ.
3. Calculer les puissances successives et déterminer l'ordre de $\sigma\rho$.
4. Calculer les puissances successives et déterminer l'ordre de $\rho\sigma$.
5. Calculer les puissances successives et déterminer l'ordre de $\sigma\rho^{-1}$.
6. Calculer les puissances successives et déterminer l'ordre de $\rho^{-1}\sigma$.

Éléments de réponse 536

Exercice 537

Déterminer la parité des permutations suivantes et les écrire comme produits de transpositions :

$$\sigma_1 = (1\ 3\ 5)(5\ 4\ 3\ 2)(5\ 6\ 7\ 8), \qquad \sigma_2 = (1\ 2)(2\ 4)(1\ 7)(7\ 6\ 8).$$

Éléments de réponse 537

L'application signature est un morphisme de $\mathfrak{S}_8$ dans le groupe multiplicatif $\{-1, 1\}$.

La permutation σ_1 est le produit d'un cycle pair avec deux cycles impairs, elle est donc paire.

La permutation σ_2 est le produit de 3 cycles impairs et d'un cycle pair, elle est donc impaire.

Autre méthode :

$$\sigma_1 = (3\ 5)(5\ 1)(2\ 3)(4\ 2)(2\ 5)(7\ 8)(6\ 8)(5\ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^8 = 1$ et

$$\sigma_2 = (1\ 2)(2\ 4)(1\ 7)(6\ 8)(7\ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^5 = -1$.

Exercice 538

Soit σ la permutation de $\{1, 2, \ldots, 12\}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

Calculer σ^{2000}.

Éléments de réponse 538

Posons $\sigma_1 = (1\ 10\ 5\ 7\ 2\ 9\ 12)$, $\sigma_2 = (3\ 8\ 6)$ et $\sigma_3 = (4\ 11)$.

Ces trois permutations sont à supports disjoints deux à deux donc commutent. Il en résulte que $\sigma^{2000} = \sigma_1^{2000}\sigma_2^{2000}\sigma_3^{2000}$.

Par ailleurs σ_1 est d'ordre 7 et $2000 = 285 \times 7 + 5$ d'où $\sigma_1^{2000} = \sigma_1^5$.

De plus σ_2 est d'ordre 3 et $2000 = 666 \times 3 + 2$ d'où $\sigma_2^{2000} = \sigma_2^2$.

Enfin σ_3 est d'ordre 2 et $2000 = 1000 \times 2$ d'où $\sigma_3^{2000} = \mathrm{id}$.

Par suite

$$\sigma^{2000} = \sigma_1^5\sigma_2^2 = (1\ 9\ 7\ 10\ 12\ 2\ 5)(3\ 8\ 6)$$

Exercice 539

Soit n un entier, soit σ une permutation de $\{1, 2, \ldots, n\}$ et soit $(x_1\ x_2\ \ldots\ x_k)$ un cycle de $\mathfrak{S}_n$.

Calculer $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}$.

Éléments de réponse 539

Pour $1 \leq i \leq j$ posons $\sigma(x_i) = y_i$. Alors $\sigma^{-1}(y_i) = x_i$ et $((x_1\ x_2\ \ldots\ x_k)\sigma^{-1})(y_i) = ((x_1\ x_2\ \ldots\ x_k))(x_i) = x_{i+1}$ donc $\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1}(y_i) = \sigma(x_{i+1}) = y_{i+1}$.

Par ailleurs si $y \notin \{y_1, y_2, \ldots, y_k\}$, alors $(\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1})(y) = y$.

Il en résulte que

$$\sigma(x_1\ x_2\ \ldots\ x_k)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \ldots\ \sigma(x_k))$$

Exercice 540

Dans le groupe $\mathfrak{S}_7$ calculer le produit

$$(4\ 5\ 6)(5\ 6\ 7)(6\ 7\ 1)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

Éléments de réponse 540

Nous avons

1 2 3 4 5 6 7

1 2 4 5 3 6 7

1 3 2 5 4 6 7

2 1 3 5 4 6 7

2 6 3 5 4 7 1

2 7 3 6 4 5 1

2 7 3 4 5 6 1

Exercice 541

Soit n un entier. Construire des morphismes injectifs de $\mathfrak{S}_n$ dans $\mathfrak{S}_{n+1}$.

Éléments de réponse 541

Soit x un élément de $\{1, 2, \ldots, n+1\}$. Posons $E_x = \{1, 2, \ldots, n+1\} \setminus \{x\}$. Il existe un isomorphisme φ entre $\mathfrak{S}_n$ et $\mathfrak{S}_{E_x}$. Le morphisme $f_x \colon \mathfrak{S}_n \to \mathfrak{S}_{n+1}$ défini par

$$\begin{cases} f_x(\sigma)(i) = \varphi(\sigma)(i) \text{ pour } i \in E_x \\ f_x(\sigma)(x) = x \end{cases}$$

est injectif.

Exercice 542

Montrer que si c et γ sont des n-cycles de $\mathfrak{S}_n$ qui commutent entre eux, il existe un entier r tel que $\gamma = c^r$.

Éléments de réponse 542

Soient $c = (1\ c(1)\ c^2(1)\ \ldots\ c^{n-1}(1))$ et $\gamma = (1\ \gamma(1)\ \gamma^2(1)\ \ldots\ \gamma^{n-1}(1))$ deux n-cycles de $\mathfrak{S}_n$ qui commutent entre eux, *i.e.* $c\gamma = \gamma c$.

L'ensemble $\{1, 2, \ldots, n\}$ coïncide avec $\{1, c(1), c^2(1), \ldots, c^{n-1}(1)\}$. Par conséquent il existe $0 \leq r \leq n-1$ tel que $\gamma(1) = c^r(1)$. De plus si $i \in \{1, \ldots, n\}$, alors il existe $0 \leq s \leq n-1$ tel que $i = c^s(1)$. Il en résulte que

$$\gamma(i) = \gamma(c^s(1)) = c^s(\gamma(1)) = c^s(c^r(1)) = c^r(c^s(1)) = c^s(i).$$

Par suite $\gamma = c^s$.

Autre méthode : faisons agir $\mathfrak{S}_n$ sur l'ensemble des n-cycles par conjugaison (c'est possible car les n-cycles sont dans la même orbite pour cette action). Cet ensemble est de cardinal $(n-1)!$ En effet un n-cycle σ s'écrit $(1\ \sigma(1)\ \sigma(2)\ \ldots\ \sigma(n-1))$ et nous avons $(n-1)$ choix pour $\sigma(1)$ puis $(n-2)$ choix pour $\sigma(2)$ etc. Le groupe $\mathfrak{S}_n$ agit transitivement sur cet ensemble. L'indice du stabilisateur de c pour cette action est $(n-1)!$ et son cardinal est n. Ce stabilisateur est le centralisateur de c qui contient au moins les n puissances de c et tout n-cycle qui commute avec c est donc égal à une puissance de c.

Exercice 543

Soit $n \geq 3$ un entier. Sachant que le groupe $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de $\{1, 2, \ldots, n\}$ montrer que $\mathfrak{S}_n$ est engendré par les ensembles suivants de permutations :

1. $(1\ 2)$, …, $(1\ n)$;
2. $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$;
3. $(1\ 2)$, $(2\ 3\ \ldots\ n)$.

Éléments de réponse 543

1. Notons que $(i\ j) = (i\ 1)(j\ 1)(i\ 1)$ lorsque $i \neq j$;
2. Soit $i < j$.

   Si $j > i+1$, alors

$$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j) \tag{1.14.1}$$

   Si $j - 1 = i + 1$, alors $(i\ j) \in \langle (1\ 2), (2\ 3), \ldots, (n-1\ n)\rangle$.

   Sinon nous appliquons (1.17.1) en remplaçant $(i\ j)$ par $(i\ j-1)$ et nous arrivons de proche en proche au résultat.
3. Nous avons

$$(2\ 3\ \ldots\ n)(1\ 2)(2\ 3\ \ldots\ n)^{-1} = (1\ 3).$$

   Par suite par récurrence pour $i > 2$ nous avons

$$(1\ i) = (2\ 3\ \ldots\ n)^{i-2}(1\ 2)(2\ 3\ \ldots\ n)^{-i+2}$$

   d'où le résultat (en utilisant la première question).

Exercice 544

Soit G un sous-groupe de $\mathfrak{S}_4$ opérant sur $\{1, 2, 3, 4\}$ par l'action induite par l'action naturelle de $\mathfrak{S}_4$.

Pour $i = 1, 2, 3, 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i.

Déterminer $\mathcal{O}_i$ et S_i pour $i = 1, 2, 3, 4$ dans chacun des cas suivants :

1. $\mathrm{G} = \langle (1\ 2\ 3)\rangle$;
2. $\mathrm{G} = \langle (1\ 2\ 3\ 4)\rangle$;
3. $\mathrm{G} = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$;
4. $\mathrm{G} = \{e, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$;
5. $\mathrm{G} = \mathcal{A}_4$.

Éléments de réponse 544

1. Supposons que $\mathrm{G} = \langle (1\ 2\ 3) \rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{4\}$ et $S_i = \mathrm{G}$.
2. Supposons que $\mathrm{G} = \langle (1\ 2\ 3\ 4) \rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
3. Supposons que $\mathrm{G} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
4. Supposons que $\mathrm{G} = \{\mathrm{id}, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
5. Supposons que $\mathrm{G} = \mathcal{A}_4$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (2\ 3\ 4) \rangle$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1\ 3\ 4) \rangle$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1\ 2\ 4) \rangle$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1\ 2\ 3) \rangle$.

Exercice 545

Établir la table de $\mathfrak{S}_3$ et de $\mathbb{Z}/6\mathbb{Z}$.
Quels sont les sous-groupes de $\mathfrak{S}_3$?
Quels sont les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$?

Éléments de réponse 545

La table de $\mathfrak{S}_3$ est

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

La table de $\mathbb{Z}/6\mathbb{Z}$ est

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[4]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Les sous-groupes de $\mathfrak{S}_3$ sont :

- un sous-groupe d'ordre 1 ;
- trois sous-groupes d'ordre 2 : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$;
- un sous-groupe d'ordre 3 : $\langle(1\ 2\ 3)\rangle$.

Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont :

- un sous-groupe d'ordre 1 ;
- un sous-groupes d'ordre 2 : $\langle[3]\rangle$;
- un sous-groupes d'ordre 3 : $\langle[2]\rangle$.

Exercice 546

a) Déterminer les classes de conjugaison dans $\mathfrak{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 546

a) Soit $c = (a_1\ \ldots\ a_k)$ un k-cycle de $\mathfrak{S}_n$. Pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1)\ \ldots\ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathfrak{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathfrak{S}_n$ la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \ldots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \ldots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \ldots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathfrak{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i\ j)\sigma(i\ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 547

Considérons les deux éléments suivants du groupe symétrique $\mathfrak{S}_9$

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad\qquad \sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathfrak{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathfrak{S}_9$?

Éléments de réponse 547

Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

nous trouvons parmi de nombreux choix possibles $\omega = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathfrak{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 548

Montrer que le groupe symétrique $\mathfrak{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathfrak{S}_3)$.

Éléments de réponse 548

L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathfrak{S}_3$ dans $\mathrm{Aut}(\mathfrak{S}_3)$, car le centre de $\mathfrak{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathfrak{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathfrak{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 549

Montrer que tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Éléments de réponse 549

Soit H un sous-groupe d'indice n dans $\mathfrak{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $\mathrm{H} \not\simeq \mathfrak{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q - 1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathfrak{S}_n$, et donc aussi H, opère par translation à gauche sur $E = \mathfrak{S}_n/\mathrm{H}$ d'où un morphisme

$$\varphi \colon \mathfrak{S}_n \to \mathfrak{S}_E \simeq \mathfrak{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathfrak{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathfrak{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$). Pour des raisons de cardinalité ($|\mathfrak{S}_n| = |\mathfrak{S}_E \simeq \mathfrak{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathfrak{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathfrak{S}_{n-1}$.

Exercice 550

a) Déterminer les classes de conjugaison dans $\mathfrak{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 550

a) Soit $c = (a_1 \ \dots \ a_k)$ un k-cycle de $\mathfrak{S}_n$. Pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathfrak{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathfrak{S}_n$ la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \ldots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathfrak{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 551

Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathfrak{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathfrak{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathfrak{S}_n$.

b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1\ 2\ 3)$, …, $(1\ 2\ n)$. En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathfrak{S}_n$ (autrement dit $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathfrak{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré

— si n est impair ≥ 5 par $(1\ 2\ 3)$ et $(3\ 4\ \ldots\ n)$;

— si n est pair ≥ 4 par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathfrak{S}_n$ de la forme $(a\ b)(c\ d)$ avec a, b, c, d deux à deux distincts.

Éléments de réponse 551

a) Soient $i < j < k < l$. Nous avons

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l)$$

Or $(i\ j)(j\ k) = (i\ j\ k)$ donc

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

b) i) Soient i, j et k des éléments de $\{1, \ldots, n\}$ tels que $i < j < k$. Nous avons

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

et

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle.$$

Soient ϕ un automorphisme de $\mathfrak{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathfrak{S}_n$.

ii) Pour $i \geq 4$ et $n \geq 4$ nous avons

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

Par ailleurs si $n \geq 5$ est impair, $(3\ 4\ \ldots\ n)$ est une permutation paire car c'est un cycle de longueur impaire $n-2$. Ainsi pour $n \geq 5$ impair on a

$$\mathcal{A}_n = \langle (1\ 2\ 3),\ (3\ 4\ \ldots\ n) \rangle$$

Nous avons

$$(1\ 2)^{\alpha}(1\ 2\ i)(1\ 2)^{\alpha} = \begin{cases} (1\ 2\ i) \text{ pour } \alpha \text{ pair} \\ (1\ 2\ i)^{-1} \text{ pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geq 4$ et $n \geq 4$

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

alors pour $i \geq 4$ impair et $n \geq 4$

$$(1\ 2\ i) = [(1\ 2)(3\ 4\ \ldots\ n)]^{i-3}(1\ 2\ 3)[(1\ 2)(3\ 4\ \ldots\ n)]^{-3+i}.$$

Et pour $i \geq 4$ pair et $n \geq 4$

$$(1\ 2\ i) = \big[\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{i-3}(1\ 2\ 3)\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{-3+i}\big]^{-1}.$$

Or si $n \geq 4$ est pair $(1\ 2)(3\ 4\ \ldots\ n)$ est une pemutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Il suffit de montrer que tout 3-cycle $(i\ j\ k)$ (avec $i < j < k$) est produit de permutations de la forme $(a\ b)(c\ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n \geq 5$ il existe ℓ et m dans $\{1, 2, \ldots, n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or nous avons

$$(i\ j\ k) = (m\ \ell)(j\ k)(m\ \ell)(i\ k)$$

d'où le résultat.

Exercice 552

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathfrak{S}_n$ dans $\mathcal{A}_{n+2}$.

Éléments de réponse 552

Considérons l'application $\psi\colon \mathfrak{S}_n \to \mathcal{A}_{n+2}$ définie par

$$\begin{cases} \psi(\sigma) = \sigma \text{ si } \sigma \text{ est une permutation paire} \\ \psi(\sigma) = \sigma \circ (n+1\ n+2) \text{ si } \sigma \text{ est une permutation impaire} \end{cases}$$

L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints.

On peut vérifier que ψ est un morphisme de groupes.

Exercice 553

Construire un morphisme surjectif de $\mathfrak{S}_4$ sur $\mathfrak{S}_3$.

Éléments de réponse 553

Faire agir $\mathfrak{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathfrak{S}_4$ qui ne sont pas des transpositions.

Exercice 554

On rappelle que le groupe symétrique $\mathfrak{S}_n$ agit par applications linéaires sur $\mathbb{R}^n$ muni de sa base canonique (e_i), en posant pour tout $\sigma \in \mathfrak{S}_n$ et tout vecteur e_i de la base canonique $\sigma \cdot e_i = e_{\sigma(i)}$. Pour $\sigma = (1\ 2\ 3) \in \mathfrak{S}_3$ expliciter la matrice associée et calculer $\sigma \cdot (x_1, x_2, x_3)$.

Éléments de réponse 554

L'action de $\mathfrak{S}_3$ par applications linéaires sur $\mathbb{R}^3$ correspond à un morphisme de $\mathfrak{S}_3$ vers le groupe $\mathrm{GL}(3, \mathbb{R})$ des bijections linéaires de $\mathbb{R}^3$. Il s'agit de trouver l'image de $\sigma = (1\ 2\ 3) \in \mathfrak{S}_3$. L'application linéaire est entièrement déterminée par l'image d'une base : puisque $e_1 \mapsto e_2$, $e_2 \mapsto e_3$, $e_3 \mapsto e_1$ nous obtenons la matrice

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

et finalement l'image de (x_1, x_2, x_3) est (x_3, x_1, x_2) car

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}.$$

Remarque : une erreur classique est de croire que l'action est donnée par

$$\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

Ce n'est pas le cas, cette définition donnerait une action à droite, pas à gauche ! En fait on peut vérifier que la formule correcte pour l'action exprimée en coordonnées est

$$\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

Exercice 555

Considérons le groupe alterné $\mathcal{A}_4$. Rappelons que $D(\mathcal{A}_4)$ désigne son groupe dérivé. Soit $\mathcal{K}$ le sous-groupe de $\mathcal{A}_4$ constitué de l'identité et des doubles transpositions.

1. Montrer que $\mathcal{K}$ est un sous-groupe distingué de $\mathcal{A}_4$.
2. Montrer que $D(\mathcal{A}_4)$ est contenu dans $\mathcal{K}$ (indication : $\mathcal{A}_4/\mathcal{K}$ est d'ordre 3).
3. Montrer que $D(\mathcal{A}_4)$ n'est pas trivial.
4. Montrer que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.
5. En déduire que $D(\mathcal{A}_4) = \mathcal{K}$.

Éléments de réponse 555

1. Montrons que $\mathcal{K} \triangleleft \mathcal{A}_4$.

   Si on conjugue la double transposition $(a\ b)(c\ d)$ par une permutation σ nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ ce qui montre que $\mathcal{K}$ est distingué dans $\mathfrak{S}_4$ donc a fortiori dans $\mathcal{A}_4$.

2. Montrons que $D(\mathcal{A}_4) \subset \mathcal{K}$.

   Comme $\mathcal{A}_4/\mathcal{K}$ est d'ordre $\frac{12}{4} = 3$, il est cyclique d'ordre 3 (car 3 est premier) et en particulier abélien ce qui montre que $D(\mathcal{A}_4) \subset \mathcal{K}$.

3. Montrons que $D(\mathcal{A}_4) \neq \{1\}$.

   Le groupe $\mathcal{A}_4$ n'est pas abélien donc $D(\mathcal{A}_4) \neq \{1\}$.

4. Montrons que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.

   Soit H un sous-groupe d'ordre 2 de $\mathcal{A}_4$. Il est composé de l'identité et d'une double transposition $\tau = (a\ b)(c\ d)$. Si on conjugue τ par $\sigma \in \mathcal{A}_4$, nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ qui n'appartient pas à H si on choisit par exemple $\sigma \in \mathcal{A}_4$ tel que $\sigma(a) = a$ et $\sigma(b) = c$ ce qui est toujours possible.

5. Montrons que $D(\mathcal{A}_4) = \mathcal{K}$.

   Nous avons vu que $D(\mathcal{A}_4) \subset \mathcal{K}$ donc l'ordre de $D(\mathcal{A}_4)$ divise 4. Mais nous avons aussi vu que $D(\mathcal{A}_4)$ n'est d'ordre ni 1, ni 2. Il en résulte que $D(\mathcal{A}_4)$ est d'ordre 4 et que $D(\mathcal{A}_4) = \mathcal{K}$.

1.15. Autour des théorèmes de Sylow

Exercice 556

Donner un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 556

Le sous-groupe des matrices triangulaires supérieures strictes de $\mathrm{GL}(n, \mathbb{F}_p)$ est un p-Sylowde $\mathrm{GL}(n, \mathbb{F}_p)$.

Exercice 557

Parmi les assertions suivantes, démontrer celles qui sont vraies et donner un contre-exemple pour celles qui sont fausses (on indiquera d'abord si l'assertion est vraie ou fausse).

a) Soit G un groupe quelconque. Soient x, y dans G. Si xy est d'ordre fini p dans G, alors yx est d'ordre fini p dans G.

b) Si G est un groupe fini abélien et p est un nombre premier divisant $|\mathrm{G}|$, alors G contient un unique p-Sylow.

c) Soit p un nombre premier. Soit G un groupe fini vérifiant : pour tout $x \in \mathrm{G}$, il existe $m \in \mathbb{N}^*$ tel que $x^{p^m} = e_{\mathrm{G}}$. Alors G est un p-groupe.

Éléments de réponse 557

a) C'est vrai. Remarquons que

$$(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n \text{ termes}} = x\,\underbrace{(yx)(yx)\dots(yx)}_{(n-1) \text{ termes}}\,y = x(yx)^{n-1}y.$$

Ainsi

$$(xy)^n = e \iff x(yx)^{n-1}y = e \iff yx(yx)^{n-1}y = y \iff (yx)^n = e$$

ce qui montre que les ordres de xy et yx sont identiques.

b) C'est vrai. En effet, on sait que G possède un p-Sylow S et que tout p-Sylow H est conjugué à S mais comme G est abélien ceci implique $\mathrm{H} = \mathrm{S}$.

c) C'est vrai. Sinon $|\mathrm{G}|$ aurait un diviseur premier $q \neq p$ et G contiendrait donc un q-Sylow non trivial H. Tout élément x dans $\mathrm{H} \setminus \{e_{\mathrm{G}}\}$ serait alors d'ordre q^s avec $s > 0$ ce qui n'est pas possible étant donné que par hypothèse l'ordre de x est de la forme p^r avec $r > 0$.

Exercice 558

Déterminer les p-Sylow de $\mathbb{Z}/n\mathbb{Z}$ pour tout diviseur p de n.

Éléments de réponse 558

Posons $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$. Le groupe G est abélien ; par suite tous les sous-groupes de G sont distingués. En particulier si H est un p-Sylow de G, alors H est un p-Sylow de G distingué dans G donc H est l'unique p-Sylow de G. Il en résulte que G possède un seul p-Sylow, et ce pour tout diviseur p de n.

Plus précisément, si on écrit n sous la forme $p^\alpha m$ avec $p \nmid m$, le groupe H est le sous-groupe $m\mathbb{Z}/n\mathbb{Z}$ de $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m modulo n.

Exercice 559

Montrer qu'un groupe d'ordre 30 n'est pas simple.

Éléments de réponse 559

Supposons qu'il existe un groupe simple G d'ordre 30. Considérons les p-Sylow de G. Désignons par n_p le nombre de p-Sylow de G.

Rappelons que $30 = 2 \times 3 \times 5$.

Les théorèmes de Sylow assurent que

$$\begin{aligned} &n_2 \equiv_2, && n_2 \mid 3 \times 5 = 15 \\ &n_3 \equiv_3 1, && n_3 \mid 2 \times 5 = 10 \\ &n_5 \equiv_5 1, && n_5 \mid 2 \times 3 = 6 \end{aligned}$$

i.e.

$$n_2 \in \{1, 3, 5, 15\}, \qquad n_3 \in \{1, 10\}, \qquad n_5 \in \{1, 6\}.$$

Mais G est simple donc $n_2 \neq 1$, $n_3 \neq 1$ et $n_5 \neq 1$; finalement

$$n_2 \in \{3, 5, 15\}, \qquad n_3 = 10, \qquad n_5 = 6.$$

On en déduit que le groupe G contient $6 \times 4 = 24$ éléments d'ordre 5 (les intersections des 5-Sylow sont restreintes à l'élément neutre [24]) et au moins 20 éléments d'ordre 3. En particulier d'une part $|\mathrm{G}| = 30$, d'autre part $|\mathrm{G}| \geq 44$: contradiction.

Exercice 560

Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Montrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Éléments de réponse 560

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv_3 1$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \{\mathrm{id}, g, h\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 5-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv_5 1$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a nécessairement huit éléments d'ordre 15. Ainsi G possède un élément g d'ordre son cardinal ; G est donc le groupe cyclique engendré par g, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 561

Montrer qu'un groupe d'ordre 200 n'est pas simple.

Éléments de réponse 561

Soit G un groupe d'ordre 200. Notons que $200 = 2^3 \times 5^2$. D'après les Théorèmes de Sylow le nombre de 5-Sylow de G est congru à 1 modulo 5 et divise $2^3 = 8$ donc vaut 1. L'unique 5-Sylow de G est donc nécessairement distingué dans G ; en particulier G n'est pas simple.

Exercice 562

24. En effet un 5-Sylow P est un groupe d'ordre 5 donc est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et tout élément de $\mathrm{P} \setminus \{e\}$ engendre P ; en particulier si P et S sont deux 5-Sylow distincts et si g appartient à $\mathrm{P} \cap \mathrm{S} \setminus \{e\}$, alors d'une part $\langle g \rangle = \mathrm{P}$ et d'autre part $\langle g \rangle = \mathrm{S}$ d'où $\mathrm{S} = \mathrm{P}$: contradiction. Il en résulte que $\mathrm{P} \cap \mathrm{S} = \{e\}$.

Soient p et q deux nombres premiers distincts. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Éléments de réponse 562

Soit G un groupe d'ordre p^2q. Soit n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G. Nous allons distinguer le cas $q < p$ du cas $p < q$.

- ◇ Si $p > q$, alors n_p divise q et $n_p \equiv 1 \bmod p$. Comme $q < p$ nécessairement $n_p = 1$; le groupe G possède alors un unique p-Sylow qui est distingué dans G et G n'est pas simple.
- ◇ Si $p < q$, alors n_q divise p^2 et $n_q \equiv 1 \bmod q$. Ainsi n_q appartient à $\{1, p, p^2\}$ et $n_q \equiv 1 \bmod q$. Puisque $q < p$, $n_q \neq p$, *i.e.* n_q appartient à $\{1, p^2\}$. Si $n_q = 1$, alors le groupe G n'est pas simple. Étudions la dernière possibilité : $n_q = p^2$. Si $n_q = p^2$, alors $p^2 \equiv 1 \bmod q$ et $p \equiv \pm 1 \bmod q$. Comme $p < q$ ceci entraîne que $p = q - 1$; étant donné que p et q sont premiers nous obtenons $p = 2$ et $q = 3$. Dans ce dernier cas, il y a quatre 3-Sylow d'ordre 3 qui contiennent huit éléments d'ordre 3 ; il ne reste de la place que pour un seul 2-Sylow qui devrait être distingué. Ce dernier cas est donc lui aussi impossible.

Exercice 563

Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Démontrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Éléments de réponse 563

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv 1 \bmod 3$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \{\mathrm{id}, g, h\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.
3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a huit éléments d'ordre 15. Ainsi G possède un élément d'ordre son cardinal ; G est donc le groupe cyclique engendré par cet élément, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 564

(1) Quel est le nombre de 2-Sylow dans le groupe symétrique $\mathfrak{S}_4$?

(2) Rappelons que $\mathfrak{S}_4$ est isomorphe au groupe des rotations de $\mathbb{R}^3$ préservant un cube. Interpréter géométriquement la réponse à la question précédente.

Éléments de réponse 564

(1) Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2 \times 3 \times 3$. Le nombre n de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $8 = 2^3$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n = 1$ ou $n = 3$. Montrons que $n = 1$ est impossible. Si $n = 1$, alors l'unique 2-Sylow serait un sous-groupe distingué de $\mathfrak{S}_4$. Mais les classes de conjugaison de $\mathfrak{S}_4$ sont de cardinaux 1, 3 et 8, et il est impossible d'obtenir 8 en sommant 1 et 3 ou 8 (rappelons qu'un sous-groupe contient le neutre, donc la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : $\mathfrak{S}_4$ contient 3 sous-groupes d'ordre 8.

(2) Cherchons géométriquement un sous-groupe d'ordre 8 dans $\mathfrak{S}_4$ vu comme le groupe des rotations préservant un cube. Il y a cinq groupes d'ordre 8 à isomorphisme près, dont le groupe diédral D_8. Comme il y a un air de famille entre le cube et le carré, cela incite à chercher un sous-groupe de $\mathfrak{S}_4$ isomorphe à D_8. Effectivement il y en a : on tranche le cube suivant un « carré équateur » et on considère le sous-groupe des rotations préservant à la fois le cube et ce carré : il y en a 8.

Exercice 565

Montrer que tout groupe d'ordre 217 est cyclique (Indication : commencer par calculer le nombre de p-Sylow pour chaque diviseur premier p de 217).

Éléments de réponse 565

Soit G un groupe d'ordre 217. Notons que $217 = 7 \times 31$ et que 7 et 31 sont premiers. Le nombre de 7-Sylow de G est congru à 1 modulo 7 et divise 31 : la seule possibilité est donc 1. D'autre part le nombre de 31-Sylow est congru à 1 modulo 31 et divise 7 ; de nouveau la seule possibilité est 1. Ainsi G contient un unique 7-Sylow S_7, qui est donc distingué, et de même contient un unique 31-Sylow S_{31}, lui-aussi distingué dans G.

L'intersection $S_7 \cap S_{31}$ est triviale par Lagrange (en effet l'ordre d'un élément de $S_7 \cap S_{31}$ divise 7 et 11 donc vaut 1).

Puisque S_7 est distingué dans G, $S_7 S_{31}$ est un sous-groupe de G [25]. Comme il contient strictement S_7 et S_{31}, son ordre est un multiple strict de 7 et de 31, la seule possibilité est donc 217 et on conclut que $\mathrm{G} = S_7 S_{31}$.

25. On utilise la propriété suivante : si K est un sous-groupe distingué de G et H est un sous-groupe de G, alors $\mathrm{KH} = \{kh \mid k \in \mathrm{K},\, h \in \mathrm{H}\}$ est un sous-groupe de G ; cela découle de :

$$\forall\, k_1,\, k_2 \in \mathrm{K},\, \forall\, h_1,\, h_2 \in \mathrm{H} \qquad (k_1h_1)(k_2h_2) = \underbrace{k_1 \underbrace{h_1k_2h_1^{-1}}_{\in \mathrm{K}} \underbrace{h_1h_2}_{\in \mathrm{H}}}_{\in \mathrm{K}} \in \mathrm{KH}$$

Puisque S_7 et S_{31} sont d'ordre premier ils sont cycliques et $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{7\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{31\mathbb{Z}}$; par le théorème chinois on conclut que $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{217\mathbb{Z}}$.

Exercice 566

Combien le groupe symétrique $\mathfrak{S}_4$ contient-il de 2-Sylow ?

Éléments de réponse 566

Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $8 = 2^3$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n = 1$ ou $n = 3$. Montrons que $n = 1$ est impossible. Si $n = 1$, alors l'unique 2-Sylow serait un sous-groupe distingué de $\mathfrak{S}_4$. Mais $\mathfrak{S}_4$ possède 24 éléments répartis en 5 classes de conjugaison. En effet, il y a :

- ◇ le neutre seul dans sa classe ;
- ◇ six transpositions ;
- ◇ huit 3-cycles ;
- ◇ six 4-cycles ;
- ◇ trois double transpositions.

Il est impossible d'écrire $8 = |\text{2-Sylow}|$ sous la forme

$$1 + 6\ell + 8k + 3p$$

avec $\ell \in \{0, 1, 2\}$, $k \in \{0, 1\}$, $p \in \{0, 1\}$ (rappelons que d'une part un sous-groupe distingué est une union de classes de conjugaison et que d'autre un groupe contient l'élément neutre ; en particulier la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : le groupe $\mathfrak{S}_4$ contient trois sous-groupes d'ordre 8.

Exercice 567

Soient p un nombre premier et n un entier naturel avec $p > n$. Considérons un groupe G d'ordre pn et H un sous-groupe de G d'ordre p. Montrer que H est un sous-groupe distingué de G.

Indication : compter les p-Sylow de G.

Éléments de réponse 567

D'après les hypothèses, $\mathrm{pgcd}(p, n) = 1$, donc H est un p-Sylow de G. Notons n_p le nombre de p-Sylow de G. Alors par les théorèmes de Sylow, $n_p \equiv 1 \bmod p$ et $n_p | n$. Si $n_p \neq 1$, alors $n_p \geq p + 1$, ce qui contredit que n_p divise n puisque $n < p$. Ainsi, $n_p = 1$ et H est l'unique p-Sylow de G donc est distingué dans G.

Exercice 568

Déterminer à isomorphisme près tous les groupes d'ordre 33.

Éléments de réponse 568

Soit G un groupe d'ordre 33.

Les éléments de G sont d'ordre 1, 3, 11 ou 33. Une application directe des théorèmes de Sylow montre que G contient un unique 3-Sylow S_3 et un unique 11-Sylow S_{11}. En effet soit n_p le nombre de p-Sylow de G ; d'une part $n_3 \equiv 1 \bmod 3$ et $n_3|11$, d'autre part $n_{11} \equiv 1 \bmod 11$ et $n_{11}|3$, *i.e.* $n_{11} = 1$. Les éléments d'ordre 3 sont contenus dans S_3, les éléments d'ordre 11 dans S_{11}. On a au plus

$$\underbrace{1}_{\text{élément neutre } e} + \underbrace{3-1}_{\text{éléments de } S_3 \smallsetminus \{e\}} + \underbrace{11-1}_{\text{éléments de } S_{11} \smallsetminus \{e\}} = 1+2+10 = 13$$

éléments d'ordre 1, 3 ou 11. Puisque $|\mathrm{G}| = 33$ le groupe G contient un élément d'ordre 33 et est donc cyclique isomorphe à $\mathbb{Z}/33\mathbb{Z}$.

Exercice 569

Considérons le groupe $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ des matrices inversibles de taille 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Déterminer l'ordre de G.
2. Déterminer les classes de conjugaison de G.
3. Déterminer les centralisateurs des éléments de G (on rappelle que le centralisateur d'un élément g de G est $Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}$).
4. Déterminer les sous-groupes de G.
5. Déterminer les sous-groupes de Sylow de G.
6. Déterminer les sous-groupes distingués de G.
7. Déterminer le centre de G.
8. Déterminer le groupe dérivé de G.
9. Déterminer les normalisateurs et les classes de conjugaison des sous-groupes de G.

Éléments de réponse 569

1. Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $n \in \mathbb{N}^*$. Le groupe $\mathrm{GL}(n, \mathbb{F}_p)$ est un fini de cardinal
$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$
en effet se donner une matrice de $\mathrm{GL}(n, \mathbb{F}_p)$ revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. Nous obtenons que $|\mathrm{GL}(2, \mathbb{F}_2)| = (2^2-1)(2^2-2) = 6$. Ses éléments sont

$$\mathrm{id}, \quad S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_3 = {}^{\mathrm{t}}S_2, \quad R = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad R^2 = R^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

2. Déterminons les classes de conjugaison de G.

> Rappel : soit G un groupe, la classe de conjugaison d'un élément g de G est
> $$\{hgh^{-1} \mid h \in \mathrm{G}\}$$
> Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n (cela découle de la formule $(hgh^{-1})^k = hg^kh^{-1}$).

On vérifie sans difficulté que S_1, S_2, S_3 sont d'ordre 2 et R, R^{-1} sont d'ordre 3.

Puisque

$$S_2RS_2^{-1} = S_2RS_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = R^{-1}$$

l'élément R^{-1} est dans la classe de conjugaison de R ; c'est le seul avec R (tout élément de la classe de conjugaison de R est nécessairement d'ordre 3).

Les éléments S_2 et S_3 appartiennent à la classe de conjugaison de S_1 : $RS_1R^{-1} = S_3$ et $R^{-1}S_1R = S_2$ et ce sont les seuls avec S_1 (tout élément de la classe de conjugaison de S_1 est nécessairement d'ordre 2) : la classe de conjugaison de S_1 est $\{S_1, S_2, S_3\}$.

De même on obtient que la classe de conjugaison de S_2 (resp. S_3) est $\{S_1, S_2, S_3\}$.

On remarque que la trace d'une matrice non scalaire caractérise sa classe de conjugaison.

3. Déterminons les centralisateurs des éléments de G.

> Rappel : si G est un groupe, alors le centralisateur de l'élément $g \in \mathrm{G}$ est $Z_g = \{h \in \mathrm{G} \mid hg = gh\}$.
> de

Le centralisateur de R ou R^{-1} est d'ordre $\frac{|\mathrm{G}|}{2} = 3$; puisqu'il contient $\langle R\rangle$ qui est d'ordre 3 le centralisateur de R et $\langle R\rangle$ coïncident.

Le centralisateur d'un élément S de la classe de conjugaison $\{S_1, S_2, S_3\}$ est d'ordre $\frac{|\mathrm{G}|}{3} = 2$, il s'agit donc de $\langle S\rangle$.

4. Déterminons les sous-groupes de G.

Les sous-groupes non triviaux de G sont $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$, et $\langle R\rangle = \langle R^{-1}\rangle$.

5. Déterminons les sous-groupes de Sylow de G.

Notons que $|\mathrm{G}| = 2 \times 3$; par suite nous nous intéressons aux 2-Sylow et aux 3-Sylow de G.

Les 2-Sylow de G sont $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$.

Le groupe G possède un unique 3-Sylow : $\langle R\rangle = \langle R^{-1}\rangle$.

6. Déterminons les sous-groupes distingués propres de G.

   Première méthode.

   Puisque la classe de conjugaison de S_i n'est pas contenue dans $\langle S_i\rangle$ le sous-groupe $\langle S_i\rangle$ n'est pas distingué dans G.

   Comme la classe de conjugaison de R est contenue dans $\langle R\rangle$ le sous-groupe $\langle R\rangle$ est distingué dans G.

   Seconde méthode.

   Puisque $\langle R\rangle$ est l'unique 3-Sylow de G, il est distingué dans G.

   Les 2-Sylow étant au nombre de 3, ils ne sont pas distingués dans G.

   Par suite G contient un unique sous-groupe distingué non trivial : $\langle R\rangle$.

7. Déterminons le centre de G.

   Rappelons que si G est un groupe ; alors $\bigcap_{g\in \mathrm{G}} Z_g = Z(\mathrm{G})$.

   Or d'après 3.

$$\bigcap_{g\in \mathrm{G}} Z_g = \mathrm{G}\cap\langle S_1\rangle\cap\langle S_2\rangle\cap\langle S_3\rangle\cap\langle R\rangle = \{\mathrm{id}\},$$

   le centre de G est donc réduit à $\{\mathrm{id}\}$.

8. Déterminons le groupe dérivé de G.

Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G. Le groupe $D(\mathrm{G})$ est un sous-groupe distingué de G. Le groupe ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

   Les sous-groupes distingués de G sont $\{\mathrm{id}\}$, $\langle R\rangle$ et G ; ainsi les quotients à considérer sont ${}^{\mathrm{G}}\!/_{\{\mathrm{id}\}} = \mathrm{G}$, ${}^{\mathrm{G}}\!/_{\langle R\rangle}$ et ${}^{\mathrm{G}}\!/_{\mathrm{G}} = \{\mathrm{id}\}$. Le groupe G n'étant pas abélien, le plus grand (au sens de l'inclusion) quotient abélien de G est ${}^{\mathrm{G}}\!/_{\langle R\rangle}$ ou $\{\mathrm{id}\}$. Nous sommes donc ramenés à considérer la question suivante : le groupe ${}^{\mathrm{G}}\!/_{\langle R\rangle}$ est-il abélien ? Notons que $\left|{}^{\mathrm{G}}\!/_{\langle R\rangle}\right| = \frac{|\mathrm{G}|}{|\langle R\rangle|} = \frac{6}{3} = 2$; or un sous-groupe d'ordre 2 est abélien donc ${}^{\mathrm{G}}\!/_{\langle R\rangle}$ est abélien et c'est le plus grand quotient abélien de G. Il en résulte que $D(\mathrm{G}) = \langle R\rangle$.

9.

Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est
$$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$
Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Puisque $\langle R\rangle$ est distingué dans G le normalisateur $N_{\mathrm{G}}(\langle R\rangle)$ est G. De plus le fait que $\langle R\rangle$ soit distingué dans G implique que la classe de conjugaison de $\langle R\rangle$ est
$$C_{\langle R\rangle} = \{g\langle R\rangle g^{-1} \,|\, g \in \mathrm{G}\} = \{\langle R\rangle\}.$$

Considérons désormais l'action de G sur l'ensemble X des sous-groupes de G :
$$\mathrm{G} \times X \to X, \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}.$$
De même que précédemment nous pouvons vérifier que $\mathrm{St}(\mathrm{H}) = N_{\mathrm{G}}(\mathrm{H})$, que $\mathcal{O}_{\mathrm{H}} = C_{\mathrm{H}}$ et que $|\mathrm{G}| = |N_{\mathrm{G}}(\mathrm{H})|\,|C_{\mathrm{H}}|$.

Les $\langle S_1\rangle$, $\langle S_2\rangle$, $\langle S_3\rangle$ forment une classe de conjugaison puisque les S_i sont conjugués, *i.e.* $C_{\langle S_i\rangle} = \{\langle S_1\rangle, \langle S_2\rangle, \langle S_3\rangle\}$ pour tout $i \in \{1, 2, 3\}$. Il en résulte que le normalisateur $N_{\langle S_i\rangle}(\mathrm{G})$ de $\langle S_i\rangle$ est d'ordre $\frac{|\mathrm{G}|}{|C_{\langle S_i\rangle}|} = \frac{6}{3} = 2$; de plus $N_{\langle S_i\rangle}(\mathrm{G})$ contient $\langle S_i\rangle$. Par suite $N_{\langle S_i\rangle}(\mathrm{G}) = \langle S_i\rangle$. Enfin G compte trois 2-Sylow qui sont les $\langle S_i\rangle$.

Remarque. Le groupe G est d'ordre 6 non abélien donc isomorphe à $\mathfrak{S}_3$.

Exercice 570

1. Quels sont les sous-groupes de Sylow de $\mathcal{A}_4$?
2. Déterminer l'ordre de tous les éléments de $\mathcal{A}_4$.

   Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.

   Montrer que H contient au moins trois éléments d'ordre 3.

   Peut-il être isomorphe à $\mathfrak{S}_3$?
4. Donner la liste des sous-groupes distingués du groupe alterné $\mathcal{A}_4$, en justifiant rapidement que votre liste est complète et non redondante.
5. En déduire qu'il n'y a pas de sous-groupe d'ordre 6 dans $\mathcal{A}_4$.
6. Donner la liste des sous-groupes de $\mathcal{A}_4$.

Éléments de réponse 570

1. Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$.

L'ordre de $\mathcal{A}_4$ est $12 = 2^2 \times 3$. Soient n_2 le nombre de sous-groupes de Sylow d'ordre $2^2 = 4$ et n_3 le nombre de sous-groupes de Sylow d'ordre 3. Les théorèmes de Sylow assurent que

$$n_2 \equiv 1 \bmod 2 \text{ et } n_2|3, \qquad n_3 \equiv 1 \bmod 3 \text{ et } n_3|2^2 = 4$$

autrement dit que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 (ils sont de signature -1) et ne contient pas de transpositions (elles sont de signature -1) donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois donc $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4 isomorphe au groupe de Klein, *i.e.* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet d'après le théorème de Lagrange un sous-groupe K de $\mathcal{A}_4$ d'ordre 4 contient des éléments d'ordre 1, 2 ou 4 ; mais $\mathcal{A}_4$ ne contient pas d'élément d'ordre 2 donc K contient des éléments d'ordre 1 ou 4. Comme $\mathcal{A}_4$ contient un seul élément d'ordre 1 et trois éléments d'ordre 4 il contient un seul sous-groupe d'ordre 4).

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

2. Déterminons l'ordre de tous les éléments de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?

   Le groupe $\mathcal{A}_4$ contient trois éléments d'ordre 2, huit éléments d'ordre 3 et un élément d'ordre 1. Le groupe $\mathcal{A}_4$ ne contient donc aucun élément d'ordre 6 ; par suite il ne contient pas de sous-groupe cyclique d'ordre 6.

3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3 ; désignons par $(a\ b)(c\ d)$ l'élément d'ordre 2 et par $(a\ b\ c)$ celui d'ordre 3.

   Notons que

   $$(a\ b)(c\ d)(a\ b\ c) = (b\ d\ c) \qquad (a\ b\ c)(a\ b)(c\ d) = (a\ c\ d).$$

   Le groupe H contient les 3-cycles : $(a\ b\ c)$, $(a\ c\ d)$ et $(b\ d\ c)$ donc les trois sous-groupes d'ordre 3

   $$\langle (a\ b\ c)\rangle, \qquad \langle (a\ c\ d)\rangle, \qquad \langle (b\ d\ c)\rangle.$$

   Un groupe d'ordre 6 ne contient qu'un sous-groupe d'ordre 3 (en effet soit K un sous-groupe d'ordre $6 = 2 \times 3$. Désignons par n_3' le nombre de 3-Sylow de K ; d'une part $n_3' \equiv 1 \bmod 3$ d'autre part $n_3'|2$ donc $n_3' = 1$). Par conséquent le groupe H n'est pas d'ordre 6. En particulier, H ne peut pas être isomorphe à $\mathfrak{S}_3$ qui est d'ordre 6.

4. Il y a quatre classes de conjugaison dans $\mathcal{A}_4$, qui sont l'identité, les trois double-transpositions, et deux classes de 3-cycles (chacune de cardinal 4 : en effet le stabilisateur d'un 3-cycle est d'ordre exactement 3, puisque c'était déjà le cas dans $\mathfrak{S}_4$). Comme tous sous-groupe distingué est une union de classes de conjugaison, et est d'ordre un diviseur de 12, on obtient exactement trois sous-groupes distingués dans $\mathcal{A}_4$: $\{\mathrm{id}\}$, $\mathcal{A}_4$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le sous-groupe d'ordre 4 contenant les double-transpositions.

5. Un sous-groupe d'ordre 6 de $\mathcal{A}_4$ serait d'indice 2, donc distingué car tout sous-groupe d'indice 2 est distingué. On conclut par la question précédente que $\mathcal{A}_4$ n'admet aucun sous-groupe d'ordre 6.
6. Le groupe $\mathcal{A}_4$ contient :
   — un sous-groupe d'ordre 1 : $\{\mathrm{id}\}$;
   — trois sous-groupes d'ordre 2 :
   $$\langle(1\ 2)(3\ 4)\rangle \qquad \langle(1\ 3)(2\ 4)\rangle \qquad \langle(1\ 4)(2\ 3)\rangle;$$
   — quatre sous-groupes d'ordre 3 :
   $$\langle(1\ 2\ 3)\rangle \qquad \langle(1\ 2\ 4)\rangle \qquad \langle(1\ 3\ 4)\rangle \qquad \langle(2\ 3\ 4)\rangle;$$
   — un sous-groupe d'ordre 4 :
   $$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 571 [Simplicité de $\mathcal{A}_n$, $n \geq 5$]

I) Commençons par démontrer que le groupe $\mathcal{A}_5$ est simple.

Soit G un groupe. Un sous-groupe H de G est caractéristique si pour tout automorphisme φ de G on $\varphi(\mathrm{H}) \subset \mathrm{H}$.

I) a) Montrer que tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

I) b) Montrer que tout groupe d'ordre 15 est cyclique.

I) c) Montrer que tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

I) d) Montrer que tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

I) e) Montrer que tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

I) f) Montrer que tout groupe d'ordre 12 contient un sous-groupe caractéristique.

I) g) Montrer que tout groupe d'ordre 6 contient un sous-groupe caractéristique.

I) h) Montrer que tout groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow est simple.

I) i) Montrer que le groupe $\mathcal{A}_5$ est simple.

II) Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué de $\mathcal{A}_n$ non trivial.

II) a) Montrer qu'il existe $\tau \in \mathrm{H}$ distinct de l'identité qui a au moins un point fixe.

II) b) Montrer que pour tout $1 \leq j \leq n$ le sous-groupe $\mathrm{G}_j = \mathrm{St}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

II) c) Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$. Montrer que $\mathcal{A}_n = \mathrm{H}$.

II) d) En déduire que $\mathcal{A}_n$ est simple pour $n \geq 5$.

Éléments de réponse 571

I) a) Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué dans G. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué dans G. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$.

I) b) Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{15\mathbb{Z}}$ et est donc cyclique.

I) c) Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.

Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.

— Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant id fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 de G.

— Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $\mathrm{K} \cap \mathrm{H} = \{\mathrm{id}\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

I) d) Au I) c) on a vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caractéristiques (voir I)a)) dans le groupe KH qui est cyclique et distingué dans G (car d'indice 2 dans G). Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow.

I) e) Soit G un groupe d'ordre $20 = 2^2 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$.

I) f) Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué dans G ; ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (cf I) a)).

— Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \,|\, 3$$

Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué dans G et donc caractéristique dans G (cf I) a)).

I) g) Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ses 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et I) b) permet de conclure.

I) h) Soit G un groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 12$$

d'où $n_5 \in \{1, 6\}$. Par hypothèse $n_5 \neq 1$ donc $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G. Notons que

$$|\mathrm{H}| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

◇ Si $|\mathrm{H}|$ est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en déduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs $|\mathrm{H}|$ divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$). Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 (voir I)d)) : contradiction avec le fait qu'il en contient 6. Par suite $|\mathrm{H}|$ n'est pas divisible par 5.

◇ Si $|\mathrm{H}|$ appartient à $\{6, 12\}$, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4 (d'après I)f) et I)g)). Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G.

◇ Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4. Dans ce cas G/H est d'ordre 30, 20 ou 15 (on renvoie à I)d) si G/H est d'ordre 30, à I)e) si G/H est d'ordre 20 ; enfin si G/H est d'ordre $15 = 3 \times 5$ et si n_5 est le nombre de 5-Sylow de G/H, les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et n_5 divise 3 donc

$n_5 = 1$). Donc G/H contient un sous-groupe K distingué d'ordre 5. Considérons la surjection canonique $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $\mathrm{K} = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction (voir le premier $\diamond$ du I)h)).

I) i) Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles (1 2 3 4 5) et (1 3 2 4 5). D'après I) h) le groupe $\mathcal{A}_5$ est simple.

II) a) **Remarque**. Supposons que pour tout $\tau \in \mathrm{H} \setminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Raisonnons par l'absurde : supposons qu'aucun élément non trivial de H n'a de point fixe, *i.e.* supposons que pour tout $\tau \in \mathrm{H} \setminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$.

- $\diamond$ Montrons dans un premier temps qu'aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Raisonnons par l'absurde : supposons qu'il existe τ dans H tel que la décomposition de τ en produit de cycles disjoints contient un cycle d'ordre ≥ 3 alors on peut écrire
$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$
Puisque $n \geq 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors
$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$
Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La remarque qui précède assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Les éléments de H sont donc des produits de transpositions disjointes.
- $\diamond$ Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ est une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit
$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$
Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a
$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$
D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (cf Remarque). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction.

Le groupe H contient donc au moins un élément non trivial qui possède un point fixe.

II) b) Soit τ un élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ pour lequel il existe $1 \leq i \leq n$ tel que $\tau(i) = i$ (l'existence d'un tel τ est assurée par II) a)). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple donc ou bien $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$ ou bien $\mathrm{G}_i \cap \mathrm{H} = \{\mathrm{id}\}$. Or τ est un élément non trivial de $\mathrm{G}_i \cap \mathrm{H}$ donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathfrak{S}_n$ on a $\sigma \mathrm{G}_i \sigma^{-1} = \mathrm{G}_{\sigma(i)}$ d'où $\mathrm{G}_i \subset \mathrm{H}$ donc $\mathrm{G}_{\sigma(i)} = \sigma \mathrm{G}_i \sigma^{-1} \subset \sigma \mathrm{H} \sigma^{-1} = \mathrm{H}$. Autrement dit pour tout $1 \leq j \leq n$ on a l'inclusion $\mathrm{G}_j \subset \mathrm{H}$.

II) c) Bien sûr $\mathrm{H} \subset \mathcal{A}_n$ donc pour montrer que $\mathcal{A}_n = \mathrm{H}$ il suffit de montrer que $\mathcal{A}_n \subset \mathrm{H}$. Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \dots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1 \mathrm{G}_2 \dots \mathrm{G}_n$. Mais $\mathrm{G}_1 \mathrm{G}_2 \dots \mathrm{G}_n \subset \mathrm{H}$ (cf II) b)). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$.

II) d) Le groupe $\mathcal{A}_5$ est simple (I)i)). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (cf II) c)).

Exercice 572

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.

   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}.$$

   Montrer par un calcul direct que cette action est transitive.

   Quel est le stabilisateur de

   $$S_0 = \left\{ \mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} ?$$

3. On note $\mathfrak{S}_X$ le groupe des bijections de X dans lui-même.

   Montrer que

   $$\phi \colon \mathrm{G} \to \mathfrak{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

Éléments de réponse 572

1. Déterminons l'ordre de G. Se donner un élément de G c'est se donner une première colonne non nulle ($2^2-1=3$ choix) et une seconde colonne non colinéaire à la première ($2^2-2=2$ choix). Nous en déduisons que $|\mathrm{G}|=6$.

   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?

   Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \text{ et } n_2|3, \qquad\qquad n_3 \equiv 1 \bmod 3 \text{ et } n_3|2$$

   Par conséquent $n_3=1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D=\begin{pmatrix}1&1\\1&0\end{pmatrix}$ et $D^{-1}=\begin{pmatrix}0&1\\1&1\end{pmatrix}$.

   Les éléments d'ordre 2 sont

   $$A=\begin{pmatrix}0&1\\1&0\end{pmatrix} \qquad B=\begin{pmatrix}1&1\\0&1\end{pmatrix} \qquad C=\begin{pmatrix}1&0\\1&1\end{pmatrix};$$

   chacun engendre un 2-Sylow de G.

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\{\langle A\rangle, \langle B\rangle, \langle C\rangle\}$.

   On fait agir G sur X par conjugaison :

   $$\mathrm{G}\times X\to X, \qquad\qquad (g,\mathrm{H})\mapsto g\cdot \mathrm{H}=g\mathrm{H}g^{-1}=\{ghg^{-1}\,|\,h\in \mathrm{H}\}.$$

   Montrons que cette action est transitive ; cela revient à montrer qu'il y a une seule orbite. Par exemple montrons que $\mathcal{O}_{\langle A\rangle}=X$; un calcul direct conduit à :

   $$A\cdot\langle A\rangle=\langle A\rangle \qquad B\cdot\langle A\rangle=\langle C\rangle \qquad C\cdot\langle A\rangle=\langle B\rangle$$

   dont on déduit l'inclusion $X\subset\mathcal{O}_{\langle A\rangle}$; comme par définition $\mathcal{O}_{\langle A\rangle}\subset X$ nous obtenons finalement que $\mathcal{O}_{\langle A\rangle}=X$.

   Déterminons le stabilisateur $\mathrm{St}(\langle A\rangle)=\{g\in \mathrm{G}\,|\,g\cdot\langle A\rangle=\langle A\rangle\}$ de $\langle A\rangle$. La bijection entre ${}^{\mathrm{G}}\!/_{\mathrm{St}(\langle A\rangle)}$ et $\mathcal{O}_{\langle A\rangle}$ assure que $\#{}^{\mathrm{G}}\!/_{\mathrm{St}(\langle A\rangle)}=\#\mathcal{O}_{\langle A\rangle}$; ceci entraîne :

   $$|\mathrm{St}(\langle A\rangle)|=\frac{|\mathrm{G}|}{\#\mathcal{O}_{\langle A\rangle}}=\frac{|\mathrm{G}|}{\#X}=\frac{6}{3}=2.$$

   Un calcul direct montre que Id et A appartiennent à $\mathrm{St}(\langle A\rangle)$. Finalement $\mathrm{St}(\langle A\rangle)=\{\mathrm{Id}, A\}$

3. On note $\mathfrak{S}_X$ le groupe des bijections de X dans lui-même. Soit ϕ le morphisme de groupes associé à l'action de G sur X :

   $$\phi\colon \mathrm{G}\to\mathfrak{S}_X, \qquad\qquad g\mapsto(\mathrm{S}\mapsto g\cdot\mathrm{S}=g\mathrm{S}g^{-1})$$

Il est injectif car

$$\begin{aligned}\ker\phi &= \{g\in \mathrm{G}\,|\,\phi(g)=\mathrm{id}_{\mathfrak{S}_X}\}\\ &= \{g\in \mathrm{G}\,|\,g\cdot \mathrm{S}=\mathrm{S}\quad \forall \mathrm{S}\in X\}\\ &= \bigcap_{\mathrm{S}\in X}\mathrm{St}(\mathrm{S})\\ &= \langle A\rangle\cap\langle B\rangle\cap\langle C\rangle\cap\\ &= \{e\}.\end{aligned}$$

De plus $|\mathfrak{S}_X|=|\mathrm{G}|=6$ nous obtenons que ϕ est un isomorphisme de groupes.

Exercice 573

Considérons le sous-groupe H de $\mathrm{GL}(2,\mathbb{R})$ engendré par $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$.

1. Donner tous les éléments de H.
2. À quel groupe classique H est-il isomorphe ?

   Considérons l'ensemble : $E:=\left\{\begin{pmatrix}x\\y\end{pmatrix},\ (x,y)\in\{-1;0;1\}^2\right\}$.
3. Représenter l'ensemble E sur un graphique.
4. Montrer que

$$\varphi\colon \mathrm{H}\times E\to E,\qquad (M,X)\mapsto MX$$

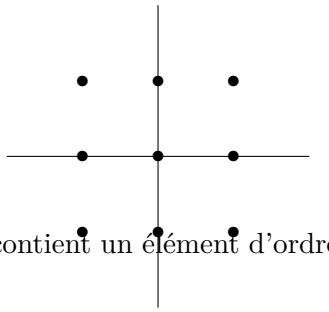
   définit bien une action de groupe de H sur E.
5. Cette action est-elle fidèle ?
6. Cette action est-elle transitive ? En donner les orbites.
7. Déterminer le stabilisateur de l'ensemble $\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}-1\\0\end{pmatrix}\right\}$.
8. Décrire les sous-ensembles de E admettant un stabilisateur non-trivial.

Éléments de réponse 573

1. Notons P la matrice $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$; alors

$$P^2=-\mathrm{Id},\qquad P^3=-P,\qquad P^4=\mathrm{Id}.$$

   Les éléments de H sont donc : Id, P, $-\mathrm{Id}$ et $-P$.



2. Le groupe H est d'ordre 4 et contient un élément d'ordre 4 (la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$) donc H est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

   Considérons l'ensemble : $E := \left\{ \begin{pmatrix} x \\ y \end{pmatrix},\ (x,y) \in \{-1;0;1\}^2 \right\}$.

3. L'ensemble E est constitué des neuf points de coordonnées

$$(-1,-1),\quad (-1,0),\quad (-1,1),\quad (0,-1),\quad (0,0),\quad (0,1),\quad (1,-1),\quad (1,0),\quad (1,1).$$

4. Montrons que

$$\mathrm{H} \times E \to E, \qquad (M,X) \mapsto M \cdot X = MX$$

   définit bien une action de H sur E :

   ◇ pour tout $X \in E$ nous avons $\mathrm{Id} \cdot X = \mathrm{Id}X = X$;

   ◇ pour tous M, N dans H, pour tout $X \in E$ nous avons

$$(MN) \cdot X = (MN)X = MNX \qquad M \cdot (N \cdot X) = M \cdot (NX) = M(NX) = MNX$$

   d'où $(MN) \cdot X = M \cdot (N \cdot X)$.

5. Soit $M \in \mathrm{H}$ tel que $M \cdot X = X$ pour tout $X \in E$, *i.e.* tel que $MX = X$ pour tout $X \in E$. Écrivons M sous la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

   D'une part $M \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ implique $M \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ou encore

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

D'autre part $M \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ implique $M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ou encore

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Autrement dit $M = \mathrm{Id}$ est l'unique élément de H à vérifier $M \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $M \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. L'action est donc fidèle.

6. Pour tout $M \in \mathrm{H}$ nous avons $M \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, l'action n'est donc pas transitive.

   Par définition

$$\begin{aligned} \mathcal{O}_X &= \mathcal{O}_{\begin{pmatrix} x \\ y \end{pmatrix}} \\ &= \{M \cdot X \,|M \in \mathrm{H}\} \\ &= \{MX \,|M \in \mathrm{H}\} \\ &= \{\mathrm{Id}X,\, PX,\, -\mathrm{Id}X,\, -PX\} \\ &= \{\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} -y \\ x \end{pmatrix}, \begin{pmatrix} -x \\ -y \end{pmatrix}, \begin{pmatrix} y \\ -x \end{pmatrix}\} \end{aligned}$$

   D'où

$$\mathcal{O}_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\mathcal{O}_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} -1 \\ 0 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} 0 \\ -1 \end{pmatrix}} = \left\{\begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$$

$$\mathcal{O}_{\begin{pmatrix} -1 \\ -1 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} 1 \\ -1 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} 1 \\ 1 \end{pmatrix}} = \mathcal{O}_{\begin{pmatrix} -1 \\ 1 \end{pmatrix}} = \left\{\begin{pmatrix} -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}\right\}$$

   Dans le second cas nous

7. Déterminons le stabilisateur de l'ensemble $\Upsilon = \left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}\right\}$.

   On cherche les $M \in \mathrm{H}$ tels que

   ◇ ou bien $M \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $M \cdot \begin{pmatrix} -1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ ce qui conduit à $M = \mathrm{Id}$;

$\diamond$ ou bien $M \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ et $M \cdot \begin{pmatrix} -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ce qui conduit à $M = -\mathrm{Id}$.

Par conséquent le stabilisateur de Υ est $\{\mathrm{Id}, -\mathrm{Id}\}$.

8. Posons $\Omega_0 = \{(0,0)\}$, $\Omega_1 = \{(1,0), (-1,0)\}$, $\Omega_2 = \{(0,1), (0,-1)\}$, $\Omega_3 = \{(1,1), (-1,-1)\}$ et $\Omega_4 = \{(1,-1), (-1,1)\}$.

   Le seul sous-groupe non-trivial de H est $\{\mathrm{Id}, -\mathrm{Id}\}$. Ainsi, si F est un sous-ensemble de stabilisateur non-trivial celui-ci est $\{\mathrm{Id}, -\mathrm{Id}\}$. Un tel ensemble F doit satisfaire la propriété suivante : si x appartient à F, alors $-x$ appartient à F, *i.e.* il est nécessairement réunion de certains des sous-ensembles suivants : Ω_0, Ω_1, Ω_2, Ω_3 et Ω_4.

   Par conséquent il y a $2^5 = 32$ sous-ensembles éventuellement possibles. Nous excluons ceux dont le stabilisateur est H qui sont les sous-ensembles que l'on obtient à partir des 3 orbites :

$\emptyset$,	$\Omega_1 \cup \Omega_2$,	$\Omega_3 \cup \Omega_4$,	$\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$,
Ω_0,	$\Omega_0 \cup \Omega_1 \cup \Omega_2$,	$\Omega_0 \cup \Omega_3 \cup \Omega_4$,	$\Omega_0 \cup \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$.

   Ainsi les sous-ensembles de E admettant un stabilisateur non-trivial sont les 24 ensembles suivants :

Ω_1,	Ω_2,	Ω_3,	Ω_4,
$\Omega_1 \cup \Omega_3$,	$\Omega_1 \cup \Omega_4$,	$\Omega_2 \cup \Omega_3$,	$\Omega_2 \cup \Omega_4$,
$\Omega_1 \cup \Omega_2 \cup \Omega_3$,	$\Omega_1 \cup \Omega_2 \cup \Omega_4$,	$\Omega_1 \cup \Omega_3 \cup \Omega_4$,	$\Omega_2 \cup \Omega_3 \cup \Omega_4$,
$\Omega_0 \cup \Omega_1$,	$\Omega_0 \cup \Omega_2$,	$\Omega_0 \cup \Omega_3$,	$\Omega_0 \cup \Omega_4$,
$\Omega_0 \cup \Omega_1 \cup \Omega_3$,	$\Omega_0 \cup \Omega_1 \cup \Omega_4$,	$\Omega_0 \cup \Omega_2 \cup \Omega_3$,	$\Omega_0 \cup \Omega_2 \cup \Omega_4$,
$\Omega_0 \cup \Omega_1 \cup \Omega_2 \cup \Omega_3$,	$\Omega_0 \cup \Omega_1 \cup \Omega_2 \cup \Omega_4$,	$\Omega_0 \cup \Omega_1 \cup \Omega_3 \cup \Omega_4$,	$\Omega_0 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$.

Exercice 574

Déterminer les p-Sylow de $\mathbb{Z}/n\mathbb{Z}$ pour tout diviseur p de n.

Éléments de réponse 574

Posons $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$. Le groupe G est abélien ; par suite tous les sous-groupes de G sont distingués. En particulier si H est un p-Sylow de G, alors H est un p-Sylow de G distingué dans G donc H est l'unique p-Sylow de G. Il en résulte que G possède un seul p-Sylow, et ce pour tout diviseur p de n.

Plus précisément, si on écrit n sous la forme $p^\alpha m$ avec $p \nmid m$, le groupe H est le sous-groupe $m\mathbb{Z}/n\mathbb{Z}$ de $\mathrm{G} = \mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m modulo n.

Exercice 575

Montrer que $\mathfrak{S}_4$ possède trois 2-sous-groupes de Sylow isomorphes à D_8.

Éléments de réponse 575

Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $D_8 \subset \mathfrak{S}_4$.

Soit n_2 le nombre de 2-Sylow de $\mathfrak{S}_4$. Le groupe D_8 est l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathfrak{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathfrak{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathfrak{S}_4$.

Exercice 576

Soit G un groupe. Soit p un nombre premier divisant $|G|$.

Montrer que si H est un p-sous-groupe de G distingué dans G, alors H est contenu dans tout p-sous-groupe de Sylow de G.

Éléments de réponse 576

Si H est un p-sous-groupe de G, il existe un p-Sylow de G qui contient H. Puisque H est distingué dans G et que les p-Sylow sont conjugués entre eux, H se trouve dans tous les p-Sylow de G.

Exercice 577

Montrer qu'un groupe d'ordre 56 n'est pas simple.

Éléments de réponse 577

Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-Sylow et n_7 le nombre de 7-Sylow.

D'après les théorèmes de Sylow

$$n_2 \equiv 1 \pmod 2 \qquad n_2 | 7$$

$$n_7 \equiv 1 \pmod 7 \qquad n_7 | 8$$

Par conséquent $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7-1$ = nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc « listé » 49 éléments du groupe G. Nous allons les noter $g_1 = e$, g_2, …, g_{49}. Supposons que $n_2 = 7$. Soit S un 2-Sylow de G ; il est d'ordre 8. Notons e, h_2, …, h_8 ses éléments. Pour des raisons d'ordre les h_i n'appartiennent pas $\{g_1, g_2, \ldots, g_{49}\}$. Donc G contient les éléments distincts g_1, g_2, …, g_{49}, h_2, h_3, …, h_8 ; en particulier $|G| \geq 49 + 7 = 56$. Par hypothèse $n_2 = 7$ donc G contient un 2-Sylow T distinct de S. Soit k dans $T \setminus S$. Pour des raisons d'ordre k n'appartient pas

$\{g_1, g_2, \ldots, g_{49}\}$. Par suite G contient les éléments distincts $g_1, g_2, \ldots, g_{49}, h_2, h_3, \ldots, h_8, k$. En particulier $|\mathrm{G}| \geq 49 + 7 + 1 = 57$: contradiction. Par conséquent $n_2 \neq 7$ et $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 578

1. Montrer qu'il n'y a pas de groupe simple d'ordre 42.
2. Montrer qu'il n'y a pas de groupe simple d'ordre 105.

Éléments de réponse 578

1. Montrons qu'il n'y a pas de groupe simple d'ordre 42.

   Soit G un groupe d'ordre 42. La décomposition de 42 en nombres premiers est $42 = 2 \times 3 \times 7$. Désignons par s_7 le nombre de 7-Sylow de G. Les théorèmes de Sylow assurent que d'une part $s_7 \equiv 1 \pmod 7$ et que d'autre part $s_7 \mid 6$. Il s'en suit que $s_7 = 1$, autrement dit G contient un seul 7-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.

2. Montrons qu'il n'y a pas de groupe simple d'ordre 105.

   Soit G un groupe d'ordre 105. La décomposition de 105 en nombres premiers est $105 = 3 \times 5 \times 7$. Désignons par s_7 (resp. s_5) le nombre de 7-Sylow (resp. 5-Sylow) de G. Les théorèmes de Sylow assurent que d'une part $s_7 \equiv 1 \pmod 7$ et que d'autre part $s_7 \mid 15$. Il s'en suit que $s_7 \in \{1, 15\}$. Étudions chacune de ces éventualités :

   - ◇ Si $s_7 = 1$, G contient un seul 7-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.
   - ◇ Si $s_7 = 15$, alors il y a six éléments d'ordre 7 dans chaque 7-Sylow ; comme ces 7-Sylow ne peuvent s'intersecter qu'en l'élément neutre (Lagrange), un total de $6 \times 15 = 90$ éléments. Les théorèmes de Sylow assurent que d'une part $s_5 \equiv 1 \pmod 5$ et que d'autre part $s_5 \mid 21$. Par conséquent $s_5 \in \{1, 21\}$.
     - — Si $s_5 = 1$, G contient un seul 5-Sylow qui est donc distingué dans G : le groupe G n'est donc pas simple.
     - — Si $s_5 = 21$, alors chaque 5-Sylow contient quatre éléments d'ordre 5 et

     $$\underbrace{\text{nb d'éléments d'ordre } 7}_{90} + \underbrace{\text{nb d'éléments d'ordre } 5}_{84} + \underbrace{\text{neutre}}_{1} > 105 = |\mathrm{G}|$$

     contradiction.

Exercice 579

1. Quel est l'ordre du groupe $\mathfrak{S}_4$?
2. Quels sont les ordres des éléments de $\mathfrak{S}_4$? Préciser le nombre d'éléments pour chaque ordre. Vérifier que leur somme est bien égale au cardinal de $\mathfrak{S}_4$.

3. Déterminer le nombre de 3-Sylow dans $\mathfrak{S}_4$.
4. Déterminer le nombre de 2-Sylow dans $\mathfrak{S}_4$.
5. Donner la liste des sous-groupes distingués de $\mathfrak{S}_4$.

Éléments de réponse 579

1. Le groupe $\mathfrak{S}_4$ est d'ordre 24.
2. Le groupe $\mathfrak{S}_4$ possède 24 éléments repartis en cinq classes de conjugaison. En effet, il y a :
   - ◇ le neutre, seul dans sa classe ;
   - ◇ $\binom{4}{2} = 6$ transpositions ;
   - ◇ $2 \times \binom{4}{3} = 8$ 3-cycles ;
   - ◇ $3 \times 2 = 6$ 4-cycles ;
   - ◇ $\frac{1}{2} \times \binom{4}{2} = 3$ double transpositions.

   On vérifie : $1 + 6 + 8 + 6 + 3 = 24$.
3. Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n_3 de 3-Sylow est congru à 1 modulo 3 et divise 8. Nous avons donc les deux possibilités $n_3 = 1$ ou $n_3 = 4$. Les 3-Sylow de $\mathfrak{S}_4$ sont d'ordre 3. Or un sous-groupe S_3 d'ordre 3 de $\mathfrak{S}_4$ est engendré par un élément d'ordre 3 et chacun contenant deux éléments d'ordre 3 il y en a $\frac{8}{2} = 4$, du type $\langle (a\ b\ c) \rangle$. Puisque les 3-cycles sont conjiugués, les quatre sous-groupes d'ordre 3 sont conjugués ; ce sont les 3-Sylow de $\mathfrak{S}_4$.
4. Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Le nombre n_2 de 2-Sylow (qui sont donc ici les sous-groupes d'ordre $2^3 = 8$) est congru à 1 modulo 2 et divise 3. Nous avons donc les deux possibilités $n_2 = 1$ ou $n_2 = 3$. Montrons que $n_2 = 1$ est impossible. Si $n_2 = 1$, alors l'unique 2-Sylow est un sous-groupe distingué de $\mathfrak{S}_4$. Mais les classes de conjugaison de $\mathfrak{S}_4$ sont de cardinaux 1, 3 et 8, et il est impossible d'obtenir 8 en sommant 1 et 3 ou 8 (rappelons qu'un sous-groupe contient le neutre, donc la classe de cardinal 1 est obligatoire pour tenter de construire un sous-groupe distingué). Conclusion : $\mathfrak{S}_4$ contient trois sous-groupes d'ordre 8.

   Autre rédaction possible

   Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$. Soit D_8 le groupe des isométries du plan qui préservent un carré ; D_8 est un sous-groupe d'ordre 8 de $\mathfrak{S}_4$. Soit n_2 le nombre de 2-Sylow de $\mathfrak{S}_4$. Les 2-Sylow de $\mathfrak{S}_4$ sont d'ordre 8 ; le groupe D_8 est donc l'un de ces 2-Sylow. Les théorèmes de Sylow assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathfrak{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons

que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathfrak{S}_4$. Il y a donc trois sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-Sylow de $\mathfrak{S}_4$.

5. Les sous-groupes distingués de $\mathfrak{S}_4$ sont : $\{\mathrm{id}\}$, $\mathcal{A}_4$ et $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$, $\mathfrak{S}_4$.

Exercice 580

Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Éléments de réponse 580

Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G.

Les théorèmes de Sylow assurent que $n_p \equiv 1 \pmod{p}$ et n_p divise q, autrement dit que $n_p \equiv 1 \pmod{p}$ et $n_p \in \{1, q\}$. Mais comme $p > q$, $q \not\equiv 1 \pmod{p}$. Par suite $n_p = 1$, *i.e.* il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué et propre. Il s'en suit que G n'est pas simple.

Exercice 581

Soient p et q deux nombres premiers.

Montrer qu'il existe au plus deux structures de groupes d'ordre pq.

Éléments de réponse 581

Exercice 582

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_3)$ le groupe des matrices 2×2 de déterminant égal à 1 et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que G est d'ordre 24.
2. Quel est l'ordre des éléments $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de G ?
3. Combien G a-t-il de 3-sous-groupes de Sylow ?
4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
5. Montrer que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
6. Montrer que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.

Éléments de réponse 582

1. Montrons que G est d'ordre 24.

   Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $n \in \mathbb{N}^*$. Le groupe $\mathrm{GL}(n, \mathbb{F}_p)$ est un fini de cardinal

   $$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$

   en effet se donner une matrice de $\mathrm{GL}(n, \mathbb{F}_p)$ revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. Nous obtenons que $|\mathrm{GL}(2, \mathbb{F}_3)| = 48$.

   Considérons le morphisme $\det\colon \mathrm{GL}(2, \mathbb{F}_3) \to \mathbb{F}_3^*$. C'est un morphisme surjectif et dont le noyau est $\mathrm{SL}(n, \mathbb{F}_3)$. Par conséquent $\mathrm{GL}(2, \mathbb{F}_3)/\mathrm{SL}(2, \mathbb{F}_3) \simeq \mathbb{F}_3^*$ d'où $|\mathrm{SL}(2, \mathbb{F}_3)| = \frac{\mathrm{GL}(2,\mathbb{F}_3)}{|\mathbb{F}_3^*|} = \frac{48}{2} = 24$.

2. Les ordres cherchés sont des diviseurs de 24 bien sûr. La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6. Les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sont d'ordre 3.

3. Soit n_3 le nombre de 3-Sylow de G qui est d'ordre $24 = 2^3 \times 3$. Notons que les 3-Sylow sont donc d'ordre 3. Les théorèmes de Sylow assurent que $n_3 \equiv 1 \pmod 3$ et que n_3 divise $2^3 = 8$. Il s'en suit que $n_3 \in \{1, 4\}$. D'après 2. il y a au moins deux sous-groupes de G d'ordre 3. Par conséquent $n_3 = 4$.

4. Montrons que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.

   Vérifions dans un premier temps que H est d'ordre 8. En effet, $A^2 = B^2 = -\mathrm{id}$ donc A et B sont d'ordre 4. Posons $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. On vérifie que

   $$\mathrm{H} = \{\mathrm{id}, -\mathrm{id}, A, -A, B, -B, C, -C\}$$

   (le groupe H est le groupe des quaternions).

   Soit $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $N^{-1} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$.

   Posons $M = NAN^{-1}$ et $L = NBN^{-1}$. Remarquons que si x appartient à $\mathbb{Z}/3\mathbb{Z}$ et $x \neq \overline{0}$, alors $x^2 = \overline{1}$.

   Un calcul montre que

   $$M = \begin{pmatrix} bd + ac & -(a^2 + b^2) \\ (c^2 + d^2) & -(bd + ac) \end{pmatrix}$$

   Comme N appartient à G, nous avons $ad - bc = \overline{1}$.

Si $a = \overline{0}$, alors $-bc = \overline{1}$ et $b = -c$. Si $d = \overline{0}$, alors $M = A$ appartient à H. Si $d \neq \overline{0}$, alors $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$ ou $M = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -M$; dans les deux cas M appartient à H.

Si maintenant $abcd \neq \overline{0}$, alors $a = -d$ et $b = c$ donc $M = -A$ appartient à H.

On démontre de manière analogue que L appartient à H. Ainsi H est distingué dans G. En effet, soit $P \in \mathrm{G}$, soit $Q \in \mathrm{H}$; remarquons que Q s'écrit $A^{m_1}B^{p_1}A^{m_2}B^{p_2}\dots A^{m_\ell}B^{p_\ell}$ et

$$\begin{aligned} PQP^{-1} &= P(A^{m_1}B^{p_1}A^{m_2}B^{p_2}\dots A^{m_\ell}B^{p_\ell})P^{-1} \\ &= PA^{m_1}P^{-1}PB^{p_1}P^{-1}PA^{m_2}P^{-1}PB^{p_2}P^{-1}P\dots P^{-1}PA^{m_\ell}P^{-1}PB^{p_\ell}P^{-1} \\ &= (PA^{m_1}P^{-1})(PB^{p_1}P^{-1})(PA^{m_2}P^{-1})(PB^{p_2}P^{-1})P\dots P^{-1}(PA^{m_\ell}P^{-1})(PB^{p_\ell}P^{-1}) \\ &= (PAP^{-1})^{m_1}(PBP^{-1})^{p_1}(PAP^{-1})^{m_2}(PBP^{-1})^{p_2}P\dots P^{-1}(PAP^{-1})^{m_\ell}(PBP^{-1})^{p_\ell} \end{aligned}$$

Or comme on vient de le voir pour tout $P \in \mathrm{G}$ PAP^{-1} et PBP^{-1} appartiennent à H ; puisque H est un groupe, nous obtenons que $(PAP^{-1})^{m_i}$ et $(PBP^{-1})^{p_i}$ appartiennent à H pour tous m_i et p_i et finalement que PQP^{-1} appartient à H.

Or H est un 2-Sylow de G, il y a donc un unique sous-groupe d'ordre 8 dans G qui est H.

5. Montrons que G est produit semi-direct de H par un sous-groupe K d'ordre 3.

   Soit K l'un des sous-groupes d'ordre 3 de G. Nous avons les propriétés suivantes : $\mathrm{H} \cap \mathrm{K} = \{e\}$, H est distingué dans G et $3 \times 8 = 24$. Il s'en suit que G est un produit semi-direct de H par K.

   Nous avons $\mathrm{G} = \mathrm{H} \rtimes_\rho \mathrm{K}$ où $\rho\colon \mathrm{K} \to \mathrm{Aut(H)}$ est tel que $\rho(k)$ est l'automorphisme intérieur associé à l'élément $k \in \mathrm{K}$.

6. Montrons que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.

   Un élément M de G appartient à $Z(\mathrm{G})$ si en particulier $MA = AM$ et $MB = BM$.

   Or $AM = MA$ si et seulement si

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

   et $BM = MB$ si et seulement si

$$\begin{pmatrix} a+b & b+d \\ a+c & b-d \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix}.$$

   Ces deux égalités conduisent à $a = d$, $b = -c$, $b + d = a - b$, $a = d$ et $b = c$, soit à $a = d$ et $b = c = 0$, *i.e.* à $M = \pm\mathrm{id}$. Par suite $Z(\mathrm{G}) = \{\mathrm{id}, \mathrm{id}\}$.

Exercice 583

Soit $\mathrm{G} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ où $n \geq 1$.

1. Déterminer l'ordre de G et de ses éléments.

2. Déterminer les sous-groupes de G.
3. Déterminer les quotients de G.

Éléments de réponse 583 Première méthode :

1. et 2. Établissons un résultat dont nous aurons besoin par la suite.

Lemme.

Soit G un groupe. Soit H un sous-groupe distingué de G. Soit $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ le morphisme quotient. Nous avons les deux assertions suivantes :

- ◇ Soit Γ un sous-groupe de G. Alors $\mathrm{H} \cap \Gamma$ est un sous-groupe distingué de Γ et $\pi(\Gamma)$ est isomorphe à ${}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.
- ◇ Les formules $\Gamma \mapsto \pi(\Gamma)$ et $\Delta \mapsto \pi^{-1}(\Delta)$ établissent une bijection croissante (pour l'inclusion) entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Démonstration du Lemme.

Puisque $\mathrm{H} = \ker \pi$, le noyau de $\pi_{|\Gamma}$ est égal à $\mathrm{H} \cap \Gamma$. Ce dernier est donc distingué dans Γ et $\pi(\Gamma) \simeq {}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.

Montrons maintenant la seconde assertion. Soit Γ un sous-groupe de G contenant H. Montrons que $\pi^{-1}(\pi(\Gamma)) = \Gamma$. Nous avons l'inclusion $\Gamma \subset \pi^{-1}(\pi(\Gamma))$. Réciproquement soit $g \in \mathrm{G}$ tel que $\pi(g) \in \pi(\Gamma)$. Il existe alors $\gamma \in \Gamma$ tel que $\pi(g) = \pi(\gamma)$, c'est-à-dire tel que $\pi(g\gamma^{-1}) = e$. Ainsi $g\gamma^{-1}$ appartient à $\ker \pi = \mathrm{H} \subset \Gamma$. Puisque $g = (g\gamma^{-1})\gamma$ nous avons $g \in \Gamma$.

La surjectivité de π implique par ailleurs que $\pi(\pi^{-1}(\Delta)) = \Delta$ pour toute partie Δ de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$; c'est en particulier le cas lorsque Δ est un sous-groupe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Ainsi les formules données établissent bien une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Par ailleurs elles définissent des applications croissantes. □

Soit G un sous-groupe de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ et soit Γ son image réciproque dans $\mathbb{Z}$. On peut écrire $\Gamma = a\mathbb{Z}$ pour un unique $a \in \mathbb{N}$. Le groupe G étant égal à l'image de Γ, il vient $\mathrm{G} = \langle \overline{a} \rangle$ (Lemme).

Soit $a \in \mathbb{Z}$. Soit $r \in \mathbb{N}$ le pgcd de a et n. L'image réciproque de $\langle \overline{a} \rangle$ dans $\mathbb{Z}$ est égale à $a\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$. Le Lemme assure que le groupe $\langle \overline{a} \rangle$ coïncide avec l'image de $r\mathbb{Z}$ dans ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, c'est-à-dire $\langle \overline{r} \rangle$. Le quotient ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\!/_{\langle \overline{a} \rangle}$ s'identifie canoniquement à ${}^{\mathbb{Z}}\!/_{r\mathbb{Z}}$.

L'intérêt de cette remarque est le suivant. Comme r divise n, l'ordre de $\overline{r}$ dans ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ est très facile à calculer. En effet si m est un entier, nous avons les équivalences suivantes

$$m\overline{r} = \overline{0} \iff n \text{ divise } mr \iff \frac{n}{r} \text{ divise } m.$$

L'ordre de $\overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$ est donc égal à $\frac{n}{r}$.

Description des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: il résulte de ce qui précède que pour tout diviseur d de n il existe un et un seul sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Il est cyclique, engendré par $\overline{\frac{n}{d}}$. Le quotient correspondant de $\mathbb{Z}/n\mathbb{Z}$ s'identifie canoniquement à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$.

3. Déterminons les quotients de G. Le quotient du groupe cyclique G par son sous-groupe d'ordre d où d est un diviseur donné de n est cyclique et donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$ où $q = \frac{n}{d}$.

Deuxième méthode :

1. Déterminons l'ordre de G et de ses éléments.

   Le groupe G est d'ordre n : ses éléments sont $\overline{1}$, $\overline{2}$, …, $\overline{n} = \overline{0}$.

   Si $1 \leq k \leq n$, alors $\overline{k}$ est d'ordre $\frac{n}{d}$ où $d = \text{pgcd}(n, k)$. En effet si $m \in \mathbb{Z}$ vérifie $m\overline{k} = \overline{0}$, alors n divise mk et donc $\frac{n}{d}$ divise $m\frac{k}{d}$ et comme les entiers $\frac{n}{d}$ et $\frac{k}{d}$ sont premiers entre eux c'est que, par Gauss, $\frac{n}{d}$ divise m de sorte que m appartient à $\frac{n}{d}\mathbb{Z}$ ce qui permet de conclure puisque $\frac{n}{d}k = n\frac{k}{d} \in n\mathbb{Z}$.

2. Déterminons les sous-groupes de G. Soit $\overline{\mathrm{H}}$ un sous-groupe de G. Alors $\mathrm{H} = \left\{k \in \mathbb{Z} \,|\, \overline{k} \in \overline{\mathrm{H}}\right\}$ est un sous-groupe de $\mathbb{Z}$ (c'est l'image réciproque de $\overline{\mathrm{H}}$ par la projection canonique $\pi : \mathbb{Z} \to \mathrm{G}$, $x \mapsto \overline{x}$). Par suite il existe $d \in \mathbb{N}$ tel que $\mathrm{H} = d\mathbb{Z}$ et comme H contient $n\mathbb{Z}$, d divise n. Par définition $\overline{\mathrm{H}} = \left\{\overline{k} \,|\, k \in \mathrm{H}\right\}$ donc $\overline{\mathrm{G}} = d\mathbb{Z}/n\mathbb{Z}$ et $\overline{\mathrm{H}}$ est le sous-groupe cyclique engendré par $\overline{d}$. De plus, puisque $\text{pgcd}(n, d) = d$, l'ordre de $\overline{\mathrm{H}}$ est $\frac{n}{d}$. Ce qui précède montre qu'il existe un unique sous-groupe d'ordre un diviseur donné δ de n : il s'agit du groupe cyclique engendré par $\overline{q}$ où $q = \frac{n}{\delta}$.

3. Déterminons les quotients de G. Le quotient du groupe cyclique G par son sous-groupe d'ordre d où d est un diviseur donné de n est cyclique et donc isomorphe à $\mathbb{Z}/q\mathbb{Z}$ où $q = \frac{n}{d}$.

Exercice 584

Déterminer l'ordre des éléments de $\mathfrak{S}_3$, les classes de conjugaison et les centralisateurs des éléments de $\mathfrak{S}_3$. Déterminer les sous-groupes de $\mathfrak{S}_3$, les sous-groupes distingués et les groupes-quotients correspondants, les classes de conjugaison et les normalisateurs des sous-groupes de $\mathfrak{S}_3$. Déterminer le centre de $\mathfrak{S}_3$ et le groupe dérivé de $\mathfrak{S}_3$.

Éléments de réponse 584

Commençons par :

Rappel : si G est un groupe, la classe de conjugaison de l'élément $g \in \mathrm{G}$ est

$$\{hgh^{-1} \,|\, h \in \mathrm{G}\}$$

et le centralisateur de l'élément $g \in \mathrm{G}$ est

$$Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}.$$

Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n. De plus nous avons $|\text{classe de conjugaison de } g| = \frac{|\mathrm{G}|}{|\text{centralisateur de } g|}$.

Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est

$$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$

Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Clairement id est d'ordre 1, la classe de conjugaison de id est

$$\{g\mathrm{id}g^{-1} \,|\, g \in \mathfrak{S}_3\} = \mathrm{id}$$

et le centralisateur de id est

$$\{g \in \mathfrak{S}_3 \,|\, g\mathrm{id} = \mathrm{id}g\} = \{g \in \mathfrak{S}_3 \,|\, g = g\} = \mathfrak{S}_3.$$

Traitons un autre exemple : (1 2 3) est d'ordre 3 :

$$(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2), \qquad (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)(1\ 2\ 3) = \mathrm{id}$$

La classe de conjugaison de (1 2 3) est $\{(1\ 2\ 3), (1\ 3\ 2)\}$; en effet d'une part tout élément de la classe de conjugaison de (1 2 3) est d'ordre 3 et d'autre part $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$. Le centralisateur de (1 2 3) est d'ordre

$$\frac{|\mathfrak{S}_3|}{|\text{classe de conjugaison de } (1\ 2\ 3)|} = \frac{6}{2} = 3$$

et contient $\langle(1\ 2\ 3)\rangle$; par suite le centralisateur de (1 2 3) est $\langle(1\ 2\ 3)\rangle$.

Nous avons les tableaux suivants :

élément	ordre	classe de conjugaison	centralisateur
id	1	$\{\mathrm{id}\}$	$\mathfrak{S}_3$
(1 2)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(1\ 2)\rangle$
(1 3)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(1\ 3)\rangle$
(2 3)	2	$\{(1\ 2), (1\ 3), (2\ 3)\}$	$\langle(2\ 3)\rangle$
(1 2 3)	3	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\langle(1\ 2\ 3)\rangle$
(1 3 2)	3	$\{(1\ 2\ 3), (1\ 3\ 2)\}$	$\langle(1\ 3\ 2)\rangle$

sous-groupe	ordre	quotient	classe de conjugaison	normalisateur
$\langle\mathrm{id}\rangle$	1	$\mathfrak{S}_3$	$\langle\mathrm{id}\rangle$	$\mathfrak{S}_3$
$\langle(1\ 2)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(1\ 2)\rangle$
$\langle(1\ 3)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(1\ 3)\rangle$
$\langle(2\ 3)\rangle$	2		$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$	$\langle(2\ 3)\rangle$
$\mathcal{A}_3 = \langle(1\ 2\ 3)\rangle$	3	$\mathbb{Z}/2\mathbb{Z}$	$\mathcal{A}_3$	$\mathfrak{S}_3$
$\mathfrak{S}_3$	6	$\{1\}$	$\mathfrak{S}_3$	$\mathfrak{S}_3$

dont on déduit : $Z(\mathfrak{S}_3) = \{\mathrm{id}\}$; en effet

$$Z(\mathfrak{S}_3) = \bigcap_{\sigma\in\mathfrak{S}_3} Z_\sigma = \mathfrak{S}_3 \cap \langle(1\ 2)\rangle \cap \langle(1\ 3)\rangle \cap \langle(2\ 3)\rangle \cap \langle(1\ 2\ 3)\rangle \cap \langle(1\ 3\ 2)\rangle$$

Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
Remarque : $D(\mathrm{G})$ est un sous-groupe distingué de G.
Remarque : $\mathrm{G}/D(\mathrm{G})$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que $\mathrm{G}/D(\mathrm{G})$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

D'après le second tableau, les quotients de $\mathfrak{S}_3$ sont $\{\mathrm{id}\}$, $\mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3$. Le groupe $\mathfrak{S}_3$ n'étant pas abélien le plus grand quotient abélien de $\mathfrak{S}_3$ est $\mathbb{Z}/2\mathbb{Z}$ et $D(\mathfrak{S}_3) = \mathcal{A}_3$.

Exercice 585

Soit $\mathbb{H}_8$ le groupe des quaternions, *i.e.* $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ la multiplication étant définie par la règle des signes et les formules

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

1. Déterminer l'ordre des éléments de $\mathbb{H}_8$.
2. Déterminer les classes de conjugaison des éléments de $\mathbb{H}_8$.
3. Déterminer les centralisateurs des éléments de $\mathbb{H}_8$.
4. Déterminer les sous-groupes de $\mathbb{H}_8$.
5. Déterminer les sous-groupes distingués et les groupes-quotients correspondants, les classes de conjugaisons et les normalisateurs des sous-groupes de $\mathbb{H}_8$ en reconnaissant d'éventuels isomorphismes avec des groupes connus.
6. Déterminer le groupe dérivé de $\mathbb{H}_8$.
7. Déterminer le centre $Z(\mathbb{H}_8)$.

Éléments de réponse 585

1. Nous avons :
   - $\diamond$ -1 est d'ordre 2.
   - $\diamond$ si $x \in \{\pm i, \pm j, \pm k\}$, alors x est d'ordre 4.
2. Déterminons les classes de conjugaison des éléments de $\mathbb{H}_8$.

Rappel : si G est un groupe, la classe de conjugaison de l'élément $g \in \mathrm{G}$ est $$\{hgh^{-1} \,|\, h \in \mathrm{G}\}$$ Remarque : si g est d'ordre n, alors tout élément de la classe de conjugaison de g est d'ordre n.

   Comme 1 est l'unique élément d'ordre 1 de $\mathbb{H}_8$, la classe de conjugaison de 1 est $\{1\}$.

   Comme -1 est l'unique élément d'ordre 2 de $\mathbb{H}_8$, la classe de conjugaison de -1 est $\{-1\}$.

   Si $x \in \{\pm i, \pm j, \pm k\}$ et $y \in \{\pm i, \pm j, \pm k\}$ tel que $y \notin \{x, -x\}$, alors $xy = -yx$, *i.e.* $yxy^{-1} = -x$. De plus, si x appartient à $\{\pm i, \pm j, \pm k\}$ et $y = \pm 1$, alors $yxy^{-1} = x$. Nous en déduisons que les conjugués de x dans $\mathbb{H}_8$ sont x et $-x$.
3. Déterminons les centralisateurs des éléments de $\mathbb{H}_8$.

Rappel : si G est un groupe, le centralisateur de l'élément $g \in \mathrm{G}$ est $$Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}.$$ De plus nous avons $\lvert\text{classe de conjugaison de } g\rvert = \frac{\lvert\mathrm{G}\rvert}{\lvert\text{centralisateur de } g\rvert}$.

   Nous avons :
   - $\diamond$ $Z_1 = \mathbb{H}_8$.
   - $\diamond$ $Z_{-1} = \mathbb{H}_8$.

◇ soit $x \in \{\pm i, \pm j, \pm k\}$. D'une part la classe de conjugaison de x dans $\mathbb{H}_8$ est de cardinal 2 d'où $|Z_x| = \frac{|\mathbb{H}_8|}{2} = 4$; d'autre part $\langle x\rangle \subset Z_x$ et $|\langle x\rangle| = 4$. Ainsi $Z_x = \langle x\rangle$.

4. Le groupe $\mathbb{H}_8$ n'admettant qu'un seul élément d'ordre 2 aucun sous-groupe d'ordre 4 n'est isomorphe au groupe de Klein. Par suite les sous-groupes propres de $\mathbb{H}_8$ sont cycliques.

5. Commençons par :

> Rappel : si G est un groupe, si H est un sous-groupe de G, alors le normalisateur de H dans G est
> $$N_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \,|\, g\mathrm{H}g^{-1} = \mathrm{H}\}.$$
> Notons que H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$ et que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand (au sens de l'inclusion) sous-groupe de G ayant cette propriété.

Chaque sous-groupe propre de $\mathbb{H}_8$ étant réunion de classes de conjugaison ces sous-groupes sont tous distingués ; on en déduit que si H est un sous-groupe de $\mathbb{H}_8$, alors

◇ sa classe de conjugaison est $\{\mathrm{H}\}$;

◇ son normalisateur est $\mathbb{H}_8$.

Intéressons-nous maintenant aux groupes quotients de $\mathbb{H}_8$.

◇ Si $\mathrm{H} = \{\mathrm{id}\}$, alors $\mathbb{H}_8/\mathrm{H} = \mathbb{H}_8$.

◇ Si $\mathrm{H} = \mathbb{H}_8$, alors $\mathbb{H}_8/\mathrm{H} = \{\mathrm{id}\}$.

◇ Si $\mathrm{H} = \langle x\rangle$ avec $x \in \{\pm i, \pm j, \pm k\}$, alors $\mathbb{H}_8/\mathrm{H}$ est d'ordre $\left|\mathbb{H}_8/\mathrm{H}\right| = \frac{|\mathbb{H}_8|}{|\mathrm{H}|} = \frac{8}{4} = 2$; par suite $\mathbb{H}_8/\mathrm{H}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

◇ Si $\mathrm{H} = \{-1, 1\}$, alors $\mathbb{H}_8/\mathrm{H}$ est d'ordre $\left|\mathbb{H}_8/\mathrm{H}\right| = \frac{|\mathbb{H}_8|}{|\mathrm{H}|} = \frac{8}{2} = 4$. Par suite ou bien $\mathbb{H}_8/\mathrm{H}$ est isomorphe à $\mathbb{Z}/4\mathrm{Z}$, ou bien $\mathbb{H}_8/\mathrm{H}$ est isomorphe au groupe de Klein $\mathbb{Z}/2\mathrm{Z} \times \mathbb{Z}/2\mathbb{Z}$. Remarquons que si g appartient à $\mathbb{H}_8$, alors g^2 appartient à H. Soit $g\mathrm{H}$ un élément de $\mathbb{H}_8/\mathrm{H}$, alors $g\mathrm{H} \cdot g\mathrm{H} = g^2\mathrm{H}$; mais g^2 appartenant à H nous avons $g^2\mathrm{H} = \mathrm{H}$ et $g\mathrm{H} \cdot g\mathrm{H} = \underbrace{\mathrm{H}}_{\text{neutre de } \left(\mathbb{H}_8/\mathrm{H}, \cdot\right)}$. En particulier, $g\mathrm{H}$ est d'ordre ≤ 2. Il s'en suit que $\mathbb{H}_8/\{-1, 1\}$ est isomorphe au groupe de Klein.

6. Déterminons le groupe dérivé de $\mathbb{H}_8$.

Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
Remarque : $D(\mathrm{G})$ est un sous-groupe distingué de G.
Remarque : ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

Puisque ${}^{\mathbb{H}_8}\!/_{\{-1,\,1\}}$ est isomorphe au groupe de Klein, $D(\mathbb{H}_8) \subseteq \{-1, 1\}$. Comme de plus $\mathbb{H}_8$ n'est pas abélien, $D(\mathbb{H}_8) \neq \{1\}$ et $D(\mathbb{H}_8) = \{-1, 1\}$.

7. Le centre de $\mathbb{H}_8$ est

$$\bigcap_{g\in\mathbb{H}_8} Z_g = \mathbb{H}_8 \cap \mathbb{H}_8 \cap \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle \cap \langle -i\rangle \cap \langle -j\rangle \cap \langle -k\rangle = \mathbb{H}_8 \cap \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle = \{1, -1\}.$$

Exercice 586

Soit G' un sous-groupe d'ordre $p(p-1)$ de $\mathfrak{S}_p$.
Montrer que G' est le normalisateur d'un p-Sylow de $\mathfrak{S}_p$.
En déduire que K est conjugué de tous les sous-groupes d'ordre $p(p-1)$ de $\mathfrak{S}_p$.

Éléments de réponse 586 Rappelons que dans un groupe G le normalisateur d'une partie X est l'ensemble, noté $N_{\mathrm{G}}(X)$, des éléments g de G qui normalisent X, *i.e.* qui vérifient $gXg^{-1} = X$:

$$N_{\mathrm{G}}(X) = \{g \in \mathrm{G} \,|\, gXg^{-1} = X\} = \{g \in \mathrm{G} \,|\, gX = Xg\}$$

$N_{\mathrm{G}}(\mathrm{H})$ est le plus grand sous-groupe de G dans lequel H est distingué ; en particulier $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{G}$ si et seulement si $\mathrm{H} \lhd \mathrm{G}$.

Exercice 587

Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.

(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{e\}$.
(ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ soit cyclique. Montrer qu'alors G est abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Éléments de réponse 587

Faisons agir G par conjugaison sur lui-même :

$$\begin{aligned} \mathrm{G}\times\mathrm{G} &\to \mathrm{G}\\ (g,h) &\mapsto g\cdot h = ghg^{-1}\end{aligned}$$

(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

Le centre de G est par définition l'ensemble

$$\begin{aligned} Z(\mathrm{G}) &= \{x\in\mathrm{G}\,|\,gx=xg \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,gxg^{-1}=x \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,g\cdot x=x \text{ pour tout } g\in\mathrm{G}\}\\ &= \{x\in\mathrm{G}\,|\,\mathcal{O}_x=\{x\}\}\end{aligned}$$

(rappelons que $\mathcal{O}_x=\{g\cdot x\,|\,g\in\mathrm{G}\}=\{gxg^{-1}\,|\,g\in\mathrm{G}\}$).

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{e\}$. Notons Ω_i, $i\in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|\mathrm{G}|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv_p |Z(\mathrm{G})|.$$

Puisque $|Z(\mathrm{G})|\geq 1$ (en effet $Z(\mathrm{G})$ contient 1) l'égalité $0\equiv_p |Z(\mathrm{G})|$ entraîne $|Z(\mathrm{G})|\geq p$. En particulier $Z(\mathrm{G})\neq\{1\}$.

(ii) Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons qu'alors G est abélien.

Par hypothèse il existe un élément a de G dont la classe $\overline{a}\in \mathrm{G}/Z(\mathrm{G})$ engendre $\mathrm{G}/Z(\mathrm{G})$. Tout élément de G peut alors s'écrire a^kh avec $k\in\mathbb{Z}$ et $h\in Z(\mathrm{G})$.

Soient g et g' dans G ; alors $g=a^kh$ et $g'=a^{k'}h'$ avec k, k' dans $\mathbb{Z}$ et h, h' dans $Z(\mathrm{G})$; ainsi

$$gg' = a^kha^{k'}h' \overset{h\in Z(\mathrm{G})}{=} a^ka^{k'}hh' = a^{k+k'}hh' \overset{h'\in Z(\mathrm{G})}{=} a^{k+k'}h'h = a^{k'+k}h'h = a^{k'}a^kh'h \overset{h\in Z(\mathrm{G})}{=} a^{k'}h'a^kh = g'g$$

Le groupe G est donc abélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G}=\left\{\begin{pmatrix}1 & a_1 & a_2\\ 0 & 1 & a_3\\ 0 & 0 & 1\end{pmatrix}\,\middle|\, a_i\in \mathrm{GL}(3,\mathbb{F}_p)\right\}$$

est un groupe non-abélien d'ordre p^3.

Chacun des coefficients a_i est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 588

Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset \mathrm{G}$ un p-Sylow de G et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $gSg^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Éléments de réponse 588

Nous avons $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. Faisons agir G (et donc également H) par translation sur l'ensemble ${}^{\mathrm{G}}\!/_{S}$ des classes à gauche de G modulo S

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{S} \to {}^{\mathrm{G}}\!/_{S}, \qquad (g, aS) \mapsto g \cdot (aS) = (ga)S$$

Notons que $g' \in \mathrm{St}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble ${}^{\mathrm{G}}\!/_{S}$ est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de ${}^{\mathrm{G}}\!/_{S}$ sous l'action de H est donc de cardinal p^c pour un certain $c \leq b$. Mais comme de plus $|\mathrm{St}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{St}(x)| = p^b$ comme attendu.

Exercice 589

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}(n, \Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 589

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathfrak{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathfrak{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathfrak{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 590

Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-Sylow.

b) Montrer que G contient dix 3-Sylow. Montrer que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-Sylow).

c) Conclure.

Éléments de réponse 590

a) Montrons que G contient trente six 5-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-Sylow serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $\mathrm{G} \to \mathfrak{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Le morphisme $\mathrm{G} \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ donné par la signature a nécessairement un noyau trivial donc G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathfrak{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|\mathrm{G}| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-Sylow. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-Sylow serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathfrak{S}_4$ ce qui est impossible car $180 = |\mathrm{G}| > |\mathfrak{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e$.

Soient S et T deux 3-Sylow de G distincts. Soit $g \in S \cap T$. Notons $Z = \{x \in \mathrm{G} \mid xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|Z| \in \{18, 36, 45, 90\}$. L'action transitive de G sur ${}^{\mathrm{G}}\!/_{Z}$ induit un morphisme injectif de G vers $\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}$. Or $|\mathrm{G}| = 180$ et $\left|\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}\right| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $\left|\mathfrak{S}_{{}^{\mathrm{G}}/_{Z}}\right| = 10!$ et $|Z| = 18$. Ainsi S et T sont des 3-Sylow de Z et un groupe d'ordre 18 admet un unique 3-Sylow d'où $S = T$: contradiction. Finalement $S \cap T = \{e\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.

D'après b) le groupe G contient dix 3-Sylow dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_{G} d'ordre divisant 9.

Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.

Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 591

Expliciter les sous-groupes de Sylow des groupes alternés $\mathcal{A}_4$.

Éléments de réponse 591

Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

Les théorèmes de Sylow assurent que

— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;

— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Exercice 592

Expliciter les sous-groupes de Sylow du groupe alterné $\mathcal{A}_5$.

Éléments de réponse 592

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. S'il y en a quatre l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathfrak{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathfrak{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient pas d'élément d'ordre 4. En effet, les éléments d'ordre 4 du groupe symétrique $\mathfrak{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1, 2, 3, 4, 5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

Exercice 593

Expliciter les sous-groupes de Sylow des groupes diédraux D_8 et D_{10}.

Éléments de réponse 593

i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $\frac{2\pi}{5}$ dont le centre est le centre du pentagone.

Exercice 594

a) Quel est l'ordre d'un p-Sylow de $\mathfrak{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathfrak{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Éléments de réponse 594

a) L'ordre de $\mathfrak{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathfrak{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathfrak{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathfrak{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathfrak{S}_p$ car $\mathfrak{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathfrak{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathfrak{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 595

On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p. Notons n_p le nombre de p-Sylow de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Éléments de réponse 595

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.

Les 60 éléments de $\mathcal{A}_5$ sont les suivants :

- l'identité d'ordre 1 qui forme une classe de conjugaison ;

- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;
- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de (1 2 3 4 5) et (2 1 3 4 5).

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $\mathrm{H} \neq \{e\}$ un sous-groupe distingué de $\mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans $\mathcal{A}_5$. Comme aucun des entiers $1 + 15 = 16$, $1 + 12 = 13$, $1 + 24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 20 + 15 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison de $\mathcal{A}_5$, donc $\mathrm{H} = \mathcal{A}_5$.

c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-Sylow. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $\mathrm{G} \to \mathfrak{S}_{\mathrm{Syl}_p} \simeq \mathfrak{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|\mathrm{G}|$ divise $|\mathfrak{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-Sylow de G est égal à 5 ou à 15.

Soit n_2 le nombre de 2-Sylow. Les théorèmes de Sylow assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|\mathrm{G}|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

e) Montrons que G contient un sous-groupe d'ordre 12.

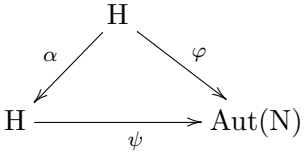
Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.

Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et T tels que $|\mathrm{S} \cap \mathrm{T}| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de Sylow assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46 + 24 = 70$ éléments et d'autre par $|\mathrm{G}| = 60$: contradiction. On dispose donc de deux 2-Sylow distincts S et T tels que $\mathrm{S} \cap \mathrm{T} = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6. Ainsi $|\mathrm{H}|$ appartient à $\{12, 20, 60\}$. Si $|\mathrm{H}| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $\mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathfrak{S}_3$: contradiction. Si $|\mathrm{H}| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(\mathrm{G})$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|\mathrm{H}| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathfrak{S}_5$. Ainsi G est isomorphe à un sous-groupe d'ordre 60 de $\mathfrak{S}_5$ qui est nécessairement $\mathcal{A}_5$.

Exercice 596

Rappelons l'énoncé suivant dont nous aurons besoin : Soient H et N deux groupes. Soient φ et ψ deux opérations de H sur N et α un automorphisme de H tels que le diagramme suivant commute



i.e. $\varphi = \psi \circ \alpha$.

L'application $(n, h) \mapsto (n, \alpha(h))$ est un isomorphisme de $\mathrm{N} \rtimes_\psi \mathrm{H}$ sur $\mathrm{N} \rtimes_\varphi \mathrm{H}$.

Soient p et q des nombres premiers avec $p < q$. Montrer que

1. Si p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.
2. Si p divise $q-1$, alors il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.

Indication : $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ ([Perrin, Cours d'algèbre, p. 24])

Éléments de réponse 596

Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Calculons ces produits. On a $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

On a l'alternative suivante :

- p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique.

- p divise $q-1$, $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. L'énoncé rappelé assure que les produits correspondants sont isomorphes.

Exercice 597

Soit $n \geq 1$. On note $\mathrm{Int}(\mathfrak{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathfrak{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition.

Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathfrak{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\}$$

de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}^n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$ montrer qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Soit q une puissance D'un nombre premier et $n \geq 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}(n, \mathbb{F}_q) \to \mathfrak{S}_N$ avec $N = \frac{q^n-1}{q-1}$.

g) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

h) En déduire que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Éléments de réponse 597

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition.

Montrons que ϕ est intérieur.

Puisque tout automorphisme de $\mathfrak{S}_i$ est intérieur dès que $i \leq 3$ (à vérifier) on peut supposer que $n \geq 4$.

Le groupe symétrique est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geq 2$. Comme τ_i et τ_j ne commutent pas si $i \neq j$ les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun noté α_1. Puisque $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ils ont nécessairement tous α_1 en commun. Écrivons $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. L'application φ étant injective $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, 2 \ldots, n\}$. Définissons la permutation $\alpha \in \mathfrak{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $1 \leq i \leq n$. Ainsi φ est la conjugaison par α et φ appartient à $\mathrm{Int}(\mathfrak{S}_n)$.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminons le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathfrak{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\}$$

de σ. Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, …, k_n cycles de longueur n, avec $n = \sum_i ik_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles pour tout k. Ainsi le commutant d'un n-cycle de $\mathfrak{S}_n$ est composé des puissances de ce dernier. Finalement on obtient

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Montrons que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Soit φ un automorphisme de $\mathfrak{S}_n$. Si τ est une transposition de $\mathfrak{S}_n$, alors $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. On a $|Z(\tau)| = |Z(\varphi(\tau))|$ ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Puisque $n \neq 6$ on a $k = 1$. D'après a) φ est donc intérieur.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}^n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrons que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués. Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$. L'action transitive de $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ induit un morphisme de groupes

$$\phi\colon \mathfrak{S}_n \to \mathfrak{S}_{{}^{\mathfrak{S}_n}\!/_{\mathrm{H}}} \simeq \mathfrak{S}_n.$$

Puisque $\ker\phi$ est un sous-groupe distingué de $\mathfrak{S}_n$, $\ker\phi \in \{\{\mathrm{id}\}, \mathcal{A}_n, \mathfrak{S}_n\}$. Le groupe $\ker\phi$ agit trivialement sur la classe de H dans ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$, d'où $\ker\phi \subset \mathrm{H}$. Il en résulte que $\ker\phi = \{\mathrm{id}\}$, *i.e.* que ϕ est injective. Ainsi φ appartient à $\mathrm{Aut}(\mathfrak{S}_n)$. Par hypothèse il existe une permutation σ telle que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathfrak{S}_{{}^{\mathfrak{S}_n}\!/_{\mathrm{H}}} \simeq \mathfrak{S}_n$. Enfin dans $\mathfrak{S}_n$ les stabilisateurs d'un point de $\{1, 2, \ldots, n\}$ sont tous conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$ montrons qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Les théorèmes de Sylow assurent que $\mathfrak{S}_5$ admet un ou six 5-Sylow. Comme $\mathcal{A}_5$ est simple $\mathfrak{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5 et $\mathfrak{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathfrak{S}_5$. L'action de $\mathfrak{S}_5$ sur X par conjugaison est transitive et induit un morphisme de groupes

$$\mu\colon \mathfrak{S}_5 \to \mathfrak{S}_X \simeq \mathfrak{S}_6$$

dont le noyau est trivial (les sous-groupes distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathfrak{S}_5$). Le groupe $\mathrm{H} = \mu(\mathfrak{S}_5) \subset \mathfrak{S}_6$ est un sous-groupe d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Preuve géométrique, par récurrence sur n : l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $\Bbbk$ (disons $\Bbbk^n$) et d'un hyperplan projectif de

dimension $n-2$, *i.e.* isomorphe à un $\mathbb{P}^{n-2}(\Bbbk)$, appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(\Bbbk) = \Bbbk^{-1} \sqcup \mathbb{P}^{n-2}(\Bbbk)$. On en déduit par récurrence la formule suivante

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \ldots + q + 1.$$

Autre preuve : le groupe $\mathrm{PGL}(\mathbb{F}_q^n)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_q^n)$ d'où le morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = \mathbb{F}_q^n \smallsetminus \{0\}\big/\mathbb{F}_q^*$ donc $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1}$. Par conséquent il existe un morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

g) Construisons géométriquement un sous-groupe H' d'indice 6 dans $\mathfrak{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

Le groupe $\mathrm{H}' = \mathrm{PGL}(2, \mathbb{F}_5)$ vu comme sous-groupe de $\mathfrak{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ n'est pas conjugué à $\mathfrak{S}_5 = \mathrm{St}(6) \subset \mathfrak{S}_6$ puisqu'il ne fixe aucun point.

h) Montrons que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Les d), e) et g) assurent que le groupe $\mathfrak{S}_6$ possède au moins un automorphisme extérieur.

Exercice 598 [Simplicité de $\mathcal{A}_n$, $g \geq 5$, version 2]

a) Montrer que le groupe $\mathcal{A}_5$ est simple.

b) Soit $n \geq 3$. Montrer que les 3-cycles engendrent $\mathcal{A}_n$.

c) Montrer que $\mathcal{A}_n$ est simple dès que $n \geq 5$.

d) Montrer que $\mathcal{A}_4$ n'est pas simple.

e) Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

f) Soit $n \geq 3$. Montrer que le centre de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$.

g) Soit $n \geq 5$. Montrer que les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

Éléments de réponse 598

a) Le groupe $\mathcal{A}_5$ a 60 éléments :

— le neutre ;

— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;

— 20 éléments d'ordre 3 (3-cycles) ;

— 24 éléments d'ordre 5 (5-cycles).

Les 3-cycles sont conjugués dans $\mathcal{A}_5$ [26]. Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.

Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.

Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geq 15 + 20 + 1 + 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$.

b) Puisque le groupe $\mathfrak{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

c) Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geq 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

---

26. Le groupe $\mathcal{A}_5$ est 3 fois transitif sur $\{1, 2, \ldots, 5\}$, *i.e.* si a_1, a_2, a_3 sont distincts et b_1, b_2, b_3 sont distincts il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, 5\} = \{a_1, a_2, \ldots, a_5\} = \{b_1, b_2, \ldots, b_5\}$$

et considérons $\sigma \in \mathfrak{S}_5$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, 5$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_4\ a_5)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_5$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;

— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E\smallsetminus F} = \mathrm{id}_{|E\smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors

— $\mathrm{H}_0 \lhd \mathcal{A}(F)$;

— $\rho_{|F} \in \mathrm{H}_0$;

— $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ [27] ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (cf b)) on a $\mathrm{H} = \mathcal{A}_n$.

d) Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

e) Calcul direct.

f) Soit σ un élément du centre de $\mathfrak{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite d'après e)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

---

27. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$, *i.e.* si $a_1, a_2, \ldots, a_{n-2}$ sont distincts et b_1, b_2, b_{n-2} sont distincts il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, n$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_{n-1}\ a_n)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ \ldots\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_n$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

g) Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \triangleleft \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \{\mathrm{id}, \mathcal{A}_n\}$.

Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathfrak{S}_n$.

Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leq 2$. Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathfrak{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathfrak{S}_n$ d'où $\sigma = \mathrm{id}$ (f)) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$.

Exercice 599

Soit G un groupe d'ordre 2009.

1. Montrer que $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$ où P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.
2. Classifier à isomorphisme près tous les groupes d'ordre 2009.
3. Soient P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. Montrer que $\mathrm{Aut}(\mathrm{G}) \simeq \mathrm{Aut}(\mathrm{P}) \times \mathrm{Aut}(\mathrm{Q})$.
4. Montrer que
   a) si Q est cyclique, alors Aut(Q) est cyclique aussi. Quel est l'ordre de Aut(Q) quand Q est cyclique ?
   b) si Q n'est pas cyclique, alors Aut(Q) est isomorphe à $\mathrm{GL}(2, \mathbb{F}_7)$ où $\mathbb{F}_7$ est le corps à 7 éléments. Quel est l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$?

Éléments de réponse 599

1. Notons que $|\mathrm{G}| = 2009 = 7^2 \times 41$. D'après le premier théorème de Sylow le groupe G possède un 41-Sylow P d'ordre 41 et un 7-Sylow Q d'ordre 49. Notons n_p le nombre de p-Sylow de G. D'après le troisième théorème de Sylow
   - $\diamond$ n_{41} est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
   - $\diamond$ n_7 est congru à 1 modulo 7 et divise 41 donc est égal à 1.

   Nous en déduisons que $\mathrm{P} \triangleleft \mathrm{G}$ et $\mathrm{Q} \triangleleft \mathrm{G}$.

   Nous constatons aussi que $\mathrm{P} \cap \mathrm{Q} = \{e\}$, que $\mathrm{G} = \mathrm{PQ}$ et que les deux sous-groupes dans le produit sont distingués dans G. Tout ceci revient à dire $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$.

   Reste à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs les éléments de P commutent avec ceux de Q. Ainsi G est abélien.
2. D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

soit encore

$$\mathbb{Z}/2009\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$

3. **Remarque**. Si φ est un automorphisme de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$ et $\varphi(\mathrm{Q}) = \mathrm{Q}$. En effet comme dans tout groupe et pour tout p premier l'image par un morphisme d'un p-élément est un p-élément et que P et Q sont les seuls 41-Sylow et 7-Sylow de G respectivement, $\varphi(\mathrm{P}) \subset \mathrm{P}$ et $\varphi(\mathrm{Q}) \subset \mathrm{Q}$. Comme φ est une bijection ces deux inclusions sont en fait des égalités.

   Il découle de la Remarque précédente que la restriction de tout automorphisme $\varphi \in \mathrm{Aut(G)}$ au sous-groupe P (respectivement Q) est un automorphisme qu'on appellera φ_P (respectivement φ_Q) de P (respectivement Q). Les automorphismes de φ_P et φ_Q ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

   Considérons l'application

$$\Phi\colon \mathrm{Aut(G)} \to \mathrm{Aut(P)} \times \mathrm{Aut(Q)}, \qquad \varphi \mapsto (\varphi_\mathrm{P}, \varphi_\mathrm{Q})$$

   Remarquons que $\Phi(\mathrm{id}) = (\mathrm{id}, \mathrm{id})$. Soient φ et ϕ deux éléments de Aut(G). Alors d'une part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{P}(\mathrm{P}) &= (\varphi \circ \phi)(\mathrm{P}) \\ &= \varphi(\phi(\mathrm{P})) \\ &= \varphi_\mathrm{P}(\phi_\mathrm{P}(\mathrm{P})) \\ &= (\varphi_\mathrm{P} \circ \phi_\mathrm{P})(\mathrm{P})\end{aligned}$$

   et d'autre part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{Q}(\mathrm{Q}) &= (\varphi \circ \phi)(\mathrm{Q}) \\ &= \varphi(\phi(\mathrm{Q})) \\ &= \varphi_\mathrm{Q}(\phi_\mathrm{Q}(\mathrm{Q})) \\ &= (\varphi_\mathrm{Q} \circ \phi_\mathrm{Q})(\mathrm{Q})\end{aligned}$$

   Autrement dit Φ est un morphisme de groupes.

   Montrons maintenant que Φ est un isomorphisme.

   Commençons par montrer que Φ est injective. Un automorphisme φ de Aut(G) appartient à $\ker\Phi$ si et seulement si $\varphi_\mathrm{P} = \mathrm{id}_\mathrm{P}$ et $\varphi_\mathrm{Q} = \mathrm{id}_\mathrm{Q}$. Or tout élément de G s'écrit sous la forme xy avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_\mathrm{P}(x)\varphi_\mathrm{Q}(y) = \mathrm{id}_\mathrm{P}(x)\mathrm{id}_\mathrm{Q}(y) = xy.$$

   Montrons que Φ est surjective. Soient φ_1 dans Aut(P) et φ_2 dans Aut(Q). Considérons l'application

$$\varphi\colon \mathrm{G} \to \mathrm{G}, \qquad xy \mapsto \varphi_1(x)\varphi_2(y)$$

avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. L'application φ est définie sans ambiguïté puisque G étant la somme directe de P et de Q chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q Montrons que φ est un automorphisme de G dont l'image sous l'action de Φ est (φ_1, φ_2).

Le fait que φ_1 et φ_2 soient des morphismes de groupes entraîne que φ est un morphisme de groupes. Il en est de même pour la surjectivité de φ. Supposons que $\varphi(xy) = 1$ pour $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. La définition de φ implique que $\varphi_1(x)\varphi_2(x) = 1$. Or $\varphi_1(x)$ appartient à P, $\varphi_2(y)$ appartient à Q et $\mathrm{P} \cap \mathrm{Q} = \{e\}$ donc $\varphi_1(x) = \varphi_2(y) = 1$. Puisque φ_1 est un automorphisme de P et φ_2 un automorphisme de Q nous obtenons $x = y = 1$. Comme $\mathrm{G} = \mathrm{PQ}$ tout élément de $\ker\varphi$ s'écrit comme produit d'un $x \in \mathrm{P}$ et d'un $y \in \mathrm{Q}$. Ainsi $\ker\varphi = \{e\}$.

Finalement φ est un automorphisme de G. Il s'ensuit de la définition de φ que $\varphi_{\mathrm{P}} = \varphi_1$ et $\varphi_{\mathrm{Q}} = \varphi_2$. Par conséquent $\Phi(\varphi) = (\varphi_1, \varphi_2)$. Ainsi Φ est surjective.

4. a) Si Q est cyclique, il est isomorphe à $\left(\mathbb{Z}/49\mathbb{Z}, +\right)$. Alors $|\mathrm{Aut}(\mathrm{Q})| = \varphi(49) = 7 \times 6 = 42$ où φ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$ le théorème chinois assure que $\mathrm{Aut}(\mathrm{Q})$ est cyclique d'ordre 42.

   b) Supposons maintenant que Q soit non cyclique. Alors $\mathrm{Q} \simeq \left(\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +\right)$. Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1,0)$ et $e_2 = (0,1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \qquad \lambda e_2 = \underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}$$

   avec $\lambda \in \mathbb{F}_7$, identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.

   Soit $\varphi \in \mathrm{Aut}(\mathrm{Q})$, alors

$$\begin{aligned}
\varphi(\lambda e_1) &= \varphi(\underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(1,0) + \varphi(1,0) + \ldots + \varphi(1,0)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((1,0)) \\
&= \lambda\varphi(e_1)
\end{aligned}$$

et

$$\begin{aligned}\varphi(\lambda e_2) &= \varphi(\underbrace{(0,1)+(0,1)+\ldots+(0,1)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(0,1)+\varphi(0,1)+\ldots+\varphi(0,1)}_{\lambda \text{ fois}} \\ &= \lambda\varphi((0,1)) \\ &= \lambda\varphi(e_2)\end{aligned}$$

Ainsi φ est une application linéaire. Étant bijectif $\varphi \in \mathrm{GL}(2,\mathbb{F}_7)$. Par suite $\mathrm{Aut}(\mathrm{Q}) \subset \mathrm{GL}(2,\mathbb{F}_7)$. L'autre inclusion est claire car chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Finalement $|\mathrm{GL}(2,\mathbb{F}_7)| = (7^2-1)(7^2-7)$.

Exercice 600

1. Soit H un sous-groupe distingué de $\mathfrak{S}_4$ qui contient un 4-cycle. Montrer que $\mathrm{H} = \mathfrak{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathfrak{S}_4$. Supposons que $\mathrm{P}_1 \cap \mathrm{P}_2$ contienne un 4-cycle. Montrer que $\mathrm{P}_1 = \mathrm{P}_2$ (indication : on montre que le normalisateur de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathfrak{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$, on considère le sous-groupe engendré par $\mathrm{P}_1 \cup \mathrm{P}_2$ et on utilise 1.)
3. D'après ce qui précède un 4-cycle est dans un unique sous-groupe d'ordre 8 de $\mathfrak{S}_4$. En déduire le nombre de sous-groupes d'ordre 8 de $\mathfrak{S}_4$ en comptant le nombre de 4-cycles.

Éléments de réponse 600

1. Les sous-groupes distingués de $\mathfrak{S}_4$ sont id, $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\mathcal{A}_4$ et $\mathfrak{S}_4$. Le seul de ces sous-groupes qui contient un 4-cycle est $\mathfrak{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathfrak{S}_4$. Si $\mathrm{P}_1 \neq \mathrm{P}_2$, alors $\mathrm{P}_1 \cap \mathrm{P}_2$ contient un 4-cycle et est donc d'ordre 4. Par conséquent $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_1 donc distingué dans P_1. De même $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_2 donc distingué dans P_2. Par suite le normalisateur N de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathfrak{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$. Ainsi N est un sous-groupe de $\mathrm{P}_1 \cap \mathrm{P}_2$ d'ordre un diviseur de 24 qui est un multiple de 8 et > 8. Il en résulte que $|\mathrm{N}| = 24$ et donc que $\mathrm{N} = \mathfrak{S}_4$. Ainsi $\mathrm{P}_1 \cap \mathrm{P}_2 \triangleleft \mathfrak{S}_4$ et $\mathrm{P}_1 \cap \mathrm{P}_2 = \mathfrak{S}_4$: absurde.
3. Déterminons le nombre de 4-cycles de $\mathfrak{S}_4$. Un 4-cycle s'écrit de manière unique $(1\ i\ j\ k)$ où i, j et k sont trois entiers distincts parmi $\{2, 3, 4\}$. Il y a donc $3 \times 2 \times 1 =$ six 4-cycles dans $\mathfrak{S}_4$. Soit n_2 le nombre de sous-groupes d'ordre 8. Ils sont tous isomorphes car ce sont les 2-Sylow qui sont tous conjugués. Soit k le nombre de 4-cycles dans un 2-Sylow. Nous avons donc $n_2 k = 6$ car un 4-cycle engendre un 2-groupe forcément contenu dans un 2-Sylow. De plus $k \geq 2$ car si c est un 4-cycle dans un sous-groupe P d'ordre 8, alors c^{-1} appartient à P. Si n_2 vaut 1 l'unique 2-Sylow contient un 4-cycle et est distingué dans $\mathfrak{S}_4$ donc est $\mathfrak{S}_4$: contradiction. Par suite $n_2 = 3$ et $k = 2$.

Exercice 601

Soit $n \geq 5$.

a) Montrer qu'un sous-groupe H d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

b) En utilisant les théorèmes de Sylow sur les 5-Sylow de $\mathfrak{S}_5$ construire un sous-groupe de $\mathfrak{S}_6$ d'indice 6 qui n'est pas de la forme

$$\mathfrak{S}_6(i) = \{\sigma \in \mathfrak{S}_6 \,|\, \sigma(i) = i\}$$

avec $1 \leq i \leq 6$.

Éléments de réponse 601

a) Faire agir $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ par translation. Comme nous connaissons les sous-groupes distingués de $\mathfrak{S}_n$ nous obtenons que le morphisme

$$\varphi\colon \mathrm{H} \to \mathrm{Bij}\Big({}^{\mathfrak{S}_n}\!/_{\mathrm{H}}\Big)$$

est injectif. De plus les éléments de $\varphi(\mathrm{H})$ fixent la classe H d'où le résultat.

b) Le troisième théorème de Sylow assure que $\mathfrak{S}_5$ compte six 5-Sylow. Faisons agir $\mathfrak{S}_5$ par conjugaison sur l'ensemble X des 5-Sylow. On obtient un morphisme de groupes

$$\varphi\colon \mathfrak{S}_5 \to \mathrm{Bij}(X).$$

Le premier théorème de Sylow assure que cette action est transitive. Puisque nous connaissons les sous-groupes distingués de $\mathfrak{S}_n$ nous obtenons que φ est injective. Finalement l'image de φ répond à la question.

Exercice 602

1. Soit G un groupe fini. Notons $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-sous-groupes de Sylow de G. Supposons que $|\mathrm{Syl}_p(\mathrm{G})| = m$. Montrons qu'il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathfrak{S}_m$.
2. Soit G un groupe de cardinal 36. Montrer qu'il n'est pas simple.

Éléments de réponse 602

1. D'après les théorèmes de Sylow l'action par conjugaison

$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}) \qquad\qquad (g, P) \mapsto gPg^{-1}$$

est transitive et détermine donc un morphisme non trivial $\rho\colon \mathrm{G} \to \mathrm{Bij}(\mathrm{Syl}_p(\mathrm{G})) \simeq \mathfrak{S}_m$.

2. Remarquons que $|\mathrm{G}| = 2^2 \times 3^2$. Soit n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise $2^2 = 4$ et que $n_3 \equiv 1 \bmod 3$, autrement dit que n_3 appartient à $\{1, 4\}$.

Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est forcément distingué dans G ; en particulier G n'est pas simple.

Si $n_3 = 4$, alors d'après 1. il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathfrak{S}_4$. Puisque $|\mathrm{G}| = 36$ ne divise pas $|\mathfrak{S}_4| = 24$ ce morphisme n'est pas injectif et $\ker\rho$ est un sous-groupe distingué non trivial et propre de G.

Exercice 603

Soit G un groupe d'ordre 231.

1. Montrer que G admet un seul 7-Sylowet un seul 11-Sylow.
2. Montrer que si P est le 11-Sylow de G, alors P est contenu dans le centre de G (indication : on considère l'action d'un 3-Sylowet l'action d'un 7-Sylow de G sur P par conjugaison).
3. Montrer que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G. Est-ce que ce sous-groupe d'ordre 77 est cyclique ? Justifier.
4. Montrer que G admet un sous-groupe cyclique d'ordre 33.

Éléments de réponse 603

1. Montrons que G admet un seul 7-Sylowet un seul 11-Sylow.

   Soit n_p le nombre de p-Sylowde G.

   Le troisième théorème de Sylow assure que $n_7 \equiv 1 \bmod 7$ et que n_7 divise 33, soit que $n_7 = 1$.

   Le troisième théorème de Sylow assure que $n_{11} \equiv 1 \bmod 11$ et que n_{11} divise 21, soit que $n_{11} = 1$.

2. Montrons que si P est le 11-Sylow de G, alors P est contenu dans le centre de G.

   Comme $n_{11} = 1$ nous avons $\mathrm{P} \lhd \mathrm{G}$. Soit Q un 3-Sylow ; il agit sur P par conjugaison.

   L'équation aux classes s'écrit $|\mathrm{P}| = \sum_i \mathcal{O}_i$. Chaque orbite est de cardinal $\frac{|\mathrm{Q}|}{|\mathrm{St}\mathcal{O}_i|}$ et $\frac{|\mathrm{Q}|}{|\mathrm{St}\mathcal{O}_i|} \in \{1, 3\}$. C'est 1 si l'orbite est réduite à un point x_i tel que pour tout $g \in \mathrm{Q}$ $gx_ig^{-1} = x_i$. Par suite

   $$|\mathrm{P}| = |\mathrm{P}^{\mathrm{Q}}| \bmod 3$$

   où

   $$\begin{aligned} \mathrm{P}^{\mathrm{Q}} &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, q \cdot p = p\} \\ &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, qpq^{-1} = p\} \\ &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, qp = pq\}. \end{aligned}$$

   Comme $|\mathrm{P}^{\mathrm{Q}}|$ divise 11 et $11 \neq 1 \bmod 3$, $\mathrm{P}^{\mathrm{Q}} = \mathrm{P}$, *i.e.* le sous-groupe des éléments qui commutent à tous les éléments de P contient Q. De même les éléments qui commutent à tous les éléments de P contient un 7-Sylow et bien entendu P car P est cyclique. Le sous-groupe des éléments qui commutent à tous les éléments de P est d'ordre un multiple de 3, 7 et 11, c'est donc G.

3. Montrons que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G.

   Commençons par montrer l'existence d'un tel sous-groupe. Soit Q un 7-Sylow. Puisque $P \triangleleft G$ et $P \cap Q = \{id\}$, PQ est un sous-groupe de G d'ordre 77. Comme $Q \triangleleft G$, $PQ \triangleleft G$.

   Montrons maintenant l'unicité. Soit H un sous-groupe de G d'ordre 77. Alors H contient un 11-Sylow et un 7-Sylow. Donc H = PQ. Soit p dans P d'ordre 11 et soit q dans Q d'ordre 7. Puisque $pq = qp$ (rappelons que p appartient à P et que $P \subset Z(G)$) pq est d'ordre 77 donc PQ est cyclique.

4. Montrons que G admet un sous-groupe cyclique d'ordre 33.

   Soit R un 3-Sylow. Alors PR est un sous-groupe distingué de G d'ordre 33. En effet soient p d'ordre 11 dans P et r d'ordre 3 dans R. Puisque P est contenu dans le centre de G nous avons $pr = rp$ et pr est d'ordre 33.

Exercice 604

Rappelons que D_{2n} désigne le groupe à $2n$ éléments des isométries d'un polygone régulier à n côtés. On se propose de montrer que si G est un groupe de cardinal 70, alors G est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Partie I

Soit G un groupe. Notons n_p le nombre de p-sous-groupes de Sylow de G et $o(n)$ le nombre d'éléments d'ordre n.

1. Soit p un premier impair. Montrer pourquoi un groupe de cardinal $2p$ est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou D_{2p}.
2. Que valent n_2 et n_p lorsque $G = D_{2p}$?

   Si S et T sont deux sous-groupes de G tels que $S \cap T = \{e\}$, alors on considère $ST = \{st \mid s \in S, t \in T\}$.
3. Montrer que si S est distingué dans G, alors ST = TS est un sous-groupe de cardinal $|S||T|$.
4. Montrer que si S et T sont distingués dans G, alors ST est un sous-groupe isomorphe à $S \times T$. En déduire qu'un groupe de cardinal 35 est cyclique.

Partie II

Soit G un groupe de cardinal 70.

1. Exprimer $o(p)$ en terme de n_p et énumérer les valeurs possibles a priori pour n_2, n_5 et n_7.
2. Déduire de ce qui précède que G possède un sous-groupe K d'ordre 35. Montrer que K est distingué dans G.
3. En déduire que G contient un sous-groupe distingué $H \simeq \mathbb{Z}/35\mathbb{Z}$.

4. Calculer n_2 dans le cas des quatre groupes

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

En déduire qu'ils ne sont pas isomorphes.

5. Inversement montrer en considérant les valeurs possibles de n_2 que G est isomorphe à l'un des quatre groupes

$$\mathbb{Z}/70\mathbb{Z} \qquad D_{70} \qquad D_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad D_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Éléments de réponse 604

Partie I

1. Si $|G| = 2p$, les théorèmes de Sylow assurent l'existence d'un sous-groupe distingué H de cardinal p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et un sous-groupe d'ordre 2 disons $K = \{e, s\}$. Soit r un générateur de H. Alors srs^{-1} appartient à H donc est égal à r^a pour un certain a. Alors d'une part $sr^as^{-1} = r^{a^2}$ et d'autre part $r = s^{-1}r^as$ qui se réécrit $r = sr^as^{-1}$ puisque $s^2 = e$. On en déduit que $r^{a^2} = r$ et donc $a^2 \equiv 1 \bmod p$ et donc $a \equiv \pm 1 \bmod p$. Si $a = 1$, l'élément s commute avec r donc rs est d'ordre $2p$ et $G \simeq \mathbb{Z}/2p\mathbb{Z}$. Si $a = -1$, alors $srs^{-1} = r^{-1}$ ce qui caractérise le groupe diédral.

2. Nous avons $n_p = 1$ (il n'y a qu'un seul p Sylow qui est distingué dans G) et $n_2 = p$ (en effet il y a p éléments d'ordre 2, les symétries).

3. Si S est distingué dans G, alors pour tout $t \in G$ nous avons $St = tS$ d'où l'égalité $ST = TS$. Si $g = st$ et $g' = s't'$, alors $gg' = sts't' = s(ts't^{-1})tt'$ appartient à ST. Si $g = st$, alors $g^{-1} = t^{-1}s^{-1}$ appartient à $TS = ST$. Par suite ST est bien un sous-groupe de G.

   Montrons que l'application

$$\phi\colon S \times T \to G \qquad\qquad (s,t) \mapsto st$$

est injective. Soient (s,t) et (s',t') dans $S \times T$ tels que $\phi(s,t) = \phi(s',t')$. L'égalité $\phi(s,t) = \phi(s',t')$ se réécrit $st = s't'$ dont on déduit $(s')^{-1}s = t't^{-1}$. En particulier $(s')^{-1}s = t't^{-1}$ est un élément de $S \cap T$; comme $S \cap T = \{e\}$, on obtient que $(s')^{-1}s = t't^{-1} = e$, soit que $s = s'$ et $t = t'$. Ainsi l'application ϕ est injective ; de plus son image est par définition ST. Par conséquent $|S \times T| = |ST|$. Mais $|S \times T| = |S| \cdot |T|$ d'où $|S| \cdot |T| = |ST|$.

4. D'une part $sts^{-1}t^{-1} = s(ts^{-1}t^{-1})$ donc $sts^{-1}t^{-1}$ appartient à S (par hypothèse $S \lhd G$), d'autre part $sts^{-1}t^{-1} = (sts^{-1})t^{-1}$ donc $sts^{-1}t^{-1}$ appartient à T (par hypothèse $T \lhd G$). Ainsi $sts^{-1}t^{-1}$ appartient à $S \cap T = \{e\}$, donc $sts^{-1}t^{-1} = e$ autrement dit s et t commutent. Ceci entraîne que ϕ est un morphisme ; en effet

$$\phi((s,t)\cdot(s',t')) = \phi(ss',tt') = ss'tt' = sts't' = \phi(s,t)\phi(s',t').$$

D'après ce qui précède $\phi\colon S \times T \to ST$ est donc un isomorphisme.

Si $|\mathrm{G}| = 35$ le groupe contient un unique 5-Sylow $\mathrm{S} \simeq \mathbb{Z}/5\mathbb{Z}$ et un unique 7-Sylow $\mathrm{T} \simeq \mathbb{Z}/7\mathbb{Z}$. Comme ils sont tous les deux distingués dans G d'intersection triviale nous obtenons d'après les questions précédentes que

$$\mathrm{ST} = \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Enfin $|\mathrm{ST}| = 35 = |\mathrm{G}|$ conduit à $\mathrm{ST} = \mathrm{G}$.

Partie II

Soit G un groupe de cardinal 70.

1. Comme les p-Sylow sont de cardinal p (pour $p = 2$, 5 ou 7) ils sont deux à deux disjoints hormis l'élément e bien sûr qui est présent dans chacun d'entre eux. Ainsi si H_1, H_2, …, H_{n_p} désignent les p-Sylow de G nous avons

$$\Big|\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}\Big| = n_p(p-1)$$

Par ailleurs d'après les théorèmes de Sylow $\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}$ est l'ensemble des éléments d'ordre p. Ainsi $o(p) = n_p(p-1)$.

D'après les théorèmes de Sylow n_7 divise 10 et $n_7 \equiv 1 \bmod 7$ donc $n_7 = 1$.

D'après les théorèmes de Sylow n_5 divise 14 et $n_5 \equiv 1 \bmod 5$ donc $n_5 = 1$.

D'après les théorèmes de Sylow n_2 divise 35 et $n_2 \equiv 1 \bmod 2$ donc $n_2 \in \{1, 5, 7, 35\}$.

2. Soient S l'unique 5-Sylow de G et T l'unique 7-Sylow de G. Ils sont tous les deux distingués dans G donc $\mathrm{K} = \mathrm{ST}$ est un sous-groupe de cardinal 35 qui est automatiquement distingué dans G (on peut aussi remarquer que $[\mathrm{G} : \mathrm{K}] = 2$ donc K est distingué dans G).

3. D'après les questions qui précèdent nous avons

$$\mathrm{K} = \mathrm{ST} \simeq \mathrm{S} \times \mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}.$$

4. Désignons par $n_2(\mathrm{G})$ le nombre de 2-Sylow du groupe G.

Le groupe $\mathbb{Z}/70\mathbb{Z}$ étant abélien nous avons $n_2\big(\mathbb{Z}/70\mathbb{Z}\big) = 1$.

Le groupe D_{2n} contient n symétries d'ordre 2. Par conséquent $n_2(\mathrm{D}_{70}) = 35$. De plus si B est de cardinal impair, un 2-Sylow de $\mathrm{A} \times \mathrm{B}$ est contenu dans $\mathrm{A} \times \{e\}$ donc $n_2(\mathrm{A} \times \{e\}) = n_2(\mathrm{A})$; par suite

$$n_2\Big(\mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}\Big) = n_2(\mathrm{D}_{14}) = 7 \qquad n_2\Big(\mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z}\Big) = n_2(\mathrm{D}_{10}) = 5.$$

5. Choisissons un générateur r de $\mathrm{ST} = \mathrm{K} \simeq \mathbb{Z}/35\mathbb{Z}$ et s un élément d'ordre 2. Posons $\mathrm{R} = \{e, s\}$. Observons que $srs^{-1} = r^a$ avec $a \in \mathbb{Z}/35\mathbb{Z}$ et $a^2 = 1$. Comme $a^2 \equiv 1 \bmod 35$ équivaut par le Lemme chinois à $a^2 \equiv 1 \bmod 5$ et $a^2 \equiv 1 \bmod 7$ on a quatre solutions :

— $a \equiv 1 \bmod 35$,

— $a \equiv -1 \bmod 35$,

— $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$,

— $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$.

Intéressons-nous à chacune de ces éventualités :

— si $a \equiv 1 \bmod 35$, alors R commute avec K et $\mathrm{G} \simeq \mathrm{K} \times \mathrm{R} \simeq \mathbb{Z}/35\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/70\mathbb{Z}$.

— si $a \equiv -1 \bmod 35$, alors s commute avec S mais pas avec T ainsi S commute avec T et R donc avec le sous-groupe RT qui est d'ordre 14. Puisqu'il est non abélien RT doit être isomorphe à D_{14}. Par conséquent $\mathrm{G} \simeq \mathrm{S} \times \mathrm{RT} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathrm{D}_{14}$.

— le cas $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$ se traite de la même façon que le cas précédent et on obtient $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathrm{D}_{10}$.

— si $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$ alors $\mathrm{G} \simeq \mathrm{D}_{70}$.

Exercice 605

1. Soit G un groupe fini d'ordre n. Soit p un facteur premier de n. Soit n_p le nombre de p-Sylowde G. Montrer que si n ne divise pas $n_p!$, alors le groupe G n'est pas simple.
2. Soit G un groupe fini d'ordre n. Montrer que si n est de la forme $p^\alpha q^\beta$ et si n ne divise pas $p^\alpha!$ ou $q^\beta!$, alors G n'est pas simple.
3. Montrer qu'il n'existe pas de groupe simple d'ordre 72.

Éléments de réponse 605

1. Si $n_p = 1$, alors l'unique p-Sylowde G est distingué. Sinon G opère transitivement sur l'ensemble à $n_p > 1$ éléments de ses p-Sylow. On obtient aussi un morphisme
$$\varphi \colon \mathrm{G} \to \mathfrak{S}_{n_p}$$
qui n'est pas trivial (*i.e.* n'envoie pas G sur $\{\mathrm{id}\}$) car l'opération est transtive et $n_p > 1$. Puisque n ne divise pas $n_p!$, le morphisme φ ne peut être injectif. Son noyau $\ker \varphi$ est donc un sous-groupe distingué non trivial de G.
2. Supposons par exemple que n ne divise pas $q^\beta!$. D'après les théorèmes de Sylow n_p divise q^β donc est plus petit que q^β. Comme n ne divise pas $q^\beta!$ il ne divise pas non plus [28] $n_p!$ et on conclut par 1.
3. Soit G un groupe d'ordre 72. Notons que $72 = 2^3 \times 3^2$. Soit n_3 le nombre de 3-Sylow. D'après les théorèmes de Sylow d'une part n_3 divise $2^3 = 8$, d'autre part $n_3 \equiv 1 \bmod 3$. Par suite n_3 vaut 1 ou 4. Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué ; en particulier G n'est pas simple. Si $n_3 = 4$, alors 72 ne divise pas $n_3! = 24$ et G n'est pas simple d'après 1.

28. Si $a < b$, alors $a!$ divise $b!$.

Exercice 606 Soit G un groupe fini simple non abélien.

1. Soit H un sous-groupe propre de G. Montrer que |G| divise [G : H]! (indication : montrer que G est isomorphe à un sous-groupe du groupe alterné $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$). Puisque H est distinct de G on peut même dire que G divise $\frac{1}{2}$[G : H]!.
2. Soit p un diviseur premier de |G|. Désignons par n_p le nombre de p-Sylow de G. L'entier |G| divise alors n_p!.

Éléments de réponse 606

1. Notons φ le morphisme de G dans $\mathfrak{S}_{\mathrm{G}/\mathrm{H}}$ induit par l'action de G sur l'ensemble G/H des classes à droite de G modulo H. Le noyau de cette action est exactement l'intersection des conjugués de H dans G. C'est un sous-groupe propre de G car H l'est par hypothèse. Puisque G est simple $\ker\varphi = \{\mathrm{id}\}$, *i.e.* φ est injectif.

   Intéressons-nous alors au morphisme $\mathrm{sgn}\circ\varphi\colon \mathrm{G}\to\{-1,1\}$ obtenu à partir de φ par composition par la signature $\mathrm{sgn}\colon \mathfrak{S}_{\mathrm{G}/\mathrm{H}}\to\{-1,1\}$. Si $\mathrm{sgn}\circ\varphi$ pouvait prendre la valeur -1, le groupe G possèderait un sous-groupe distingué d'indice 2 et ne serait pas simple non abélien. Par conséquent le morphisme $\mathrm{sgn}\circ\varphi$ est trivial et φ plonge donc G dans $\mathcal{A}_{\mathrm{G}/\mathrm{H}}$. En particulier |G| divise $|\mathfrak{S}_{\mathrm{G}/\mathrm{H}}| = [\mathrm{G} : \mathrm{H}]!$.
2. Soit P un p-Sylow de G. Puisque G est simple non abélien, le normalisateur [29] $N_{\mathrm{G}}(\mathrm{P})$ de P dans G est un sous-groupe propre de G. D'après le 1. nous avons donc : |G| divise $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]!$. Les théorèmes de Sylowassure que $[\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]! = n_p!$ d'où le résultat.

1.16. Structure des groupes abéliens de type fini

Exercice 607

Soit G un groupe de type fini.

Un sous-groupe H de G est-il nécessairement de type fini ? Justifiez votre réponse.

Éléments de réponse 607

Soit G est un groupe de type fini ; G peut contenir un sous-groupe H qui n'est pas de type fini.

Considérons le sous-groupe G de $\mathrm{GL}(2,\mathbb{Q})$ engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

29. dans un groupe G, le normalisateur d'une partie X est l'ensemble, noté $N_{\mathrm{G}}(X)$, des éléments g de G qui normalisent X, c'est-à-dire qui vérifient $gXg^{-1} = X$: $N_{\mathrm{G}}(X) = \left\{g\in\mathrm{G}\,|\,gXg^{-1}=X\right\} = \left\{g\in\mathrm{G}\,|\,gX=Xg\right\}$

Soit H le sous-groupe de G formé des matrices de G avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que H soit de type fini, *i.e.* $\mathrm{H} = \langle M_1, M_2, \ldots, M_r \rangle$ avec $M_i = \begin{pmatrix} 1 & m_i \\ 0 & 1 \end{pmatrix}$. Puisque $M_i^{-1} = \begin{pmatrix} 1 & -m_i \\ 0 & 1 \end{pmatrix}$ et $M_i M_j = \begin{pmatrix} 1 & m_i + m_j \\ 0 & 1 \end{pmatrix}$, il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}(2, \mathbb{Q})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or $A^{-N} B A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$: contradiction ($2^N > N$). Ainsi H n'est pas de type fini alors que G l'est.

Considérons par exemple le groupe libre G sur deux générateurs a et b. Soit H le sous-groupe engendré par tous les éléments de la forme ab^n avec $n \in \mathbb{N}$. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H le nombre de b consécutifs soit toujours strictement inférieur à N. Or ab^N appartient à H : contradiction. Le sous-groupe H de G n'est donc pas de type fini.

Exercice 608

Soit G un groupe abélien.

Montrer que $T(\mathrm{G}) = \{g \in \mathrm{G} \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Donner un exemple explicite pour lequel $T(\mathrm{G})$ n'est pas un sous-groupe de G si G n'est pas abélien.

Éléments de réponse 608

Soit G un groupe abélien.

Montrons que $T(\mathrm{G}) = \{g \in G \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Clairement $T(\mathrm{G})$ est contenu dans G. On a

- $o(e) = 1 < \infty$ donc $e \in T(\mathrm{G})$;
- soient g et h dans $T(\mathrm{G})$. Notons n (respectivement m) l'ordre de g (respectivement h). Par hypothèse $n < \infty$ et $m < \infty$. On a bien sûr $o(h^{-1}) = m$. Puisque G est abélien on a

  $$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn}$$

  Par suite $(gh^{-1})^{mn} = (g^n)^m((h^{-1})^m)^n = e^m e^n = e$. Ainsi $o(gh^{-1}) \leq mn < \infty$ et gh^{-1} appartient à $T(\mathrm{G})$.

Ainsi $T(\mathrm{G})$ est un sous-groupe de G.

Montrons que si G n'est pas abélien, alors $T(\mathrm{G})$ n'est pas forcément un sous-groupe de G.

Considérons $\mathrm{G} = \mathrm{O}(2)$. Soit ρ la rotation d'angle θ où θ/π est irrationnel. Alors ρ n'appartient pas à $T(\mathrm{G})$. Mais $\rho = s_2 \circ s_1$ avec s_1, s_2 réflexions ; en particulier $o(s_1) = o(s_2) = 2$ et donc s_1, s_2 appartiennent à $T(\mathrm{G})$.

Exercice 609

Soit $n \in \mathbb{N}$, $n \geq 2$. Trouver le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 609

Soit $n \in \mathbb{N}$, $n \geq 2$. Déterminons le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} T\left(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right) &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, o(a,b) < \infty\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, \exists\, k \in \mathbb{N}^*,\ o(a,b) = k\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, (ka, kb) = (0, \bar{0})\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, a = 0 \text{ et } b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \{0\} \times \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Montrons que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Soient $(1,1)$ et $(-1,0)$ deux éléments de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ils sont d'ordre infini mais $(1,1) + (-1,0) = (0,1)$ est d'ordre fini.

Exercice 610

a) Donner un exemple de groupe abélien qui n'est pas de type fini.

b) Si p est un nombre premier, quel est le groupe sous-jacent au corps $\mathbb{F}_{p^n}$?

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$.
Montrer que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

d) Montrer qu'un groupe abélien de type fini et de torsion est fini (ceci n'est plus vrai pour les groupes non-abéliens : voir par exemple [Calais, p. 294]).

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Éléments de réponse 610

a) $(\mathbb{Q}, +)$ est un groupe abélien qui n'est pas de type fini (pour le vérifier raisonner par l'absurde).

b) Soit p un nombre premier.
Si $n = 1$, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et le groupe sous-jacent est $\mathbb{Z}/p\mathbb{Z}$.
Si $n = 2$, alors le groupe sous-jacent à $\mathbb{F}_{p^2}$ est $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ car $\mathbb{Z}/p^2\mathbb{Z}$ possède un élément d'ordre p^2 alors que $\mathbb{F}_{p^2}$ est de caractéristique p donc sans élément d'ordre p^2.
De même pour n quelconque le groupe sous-jacent à $\mathbb{F}_{p^n}$ est $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$. Montrons que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

Écrivons les décompositions de m et n en nombre premiers :

$$m = \prod_i p_i^{\alpha_i} \qquad\qquad n = \prod_i p_i^{\beta_i}$$

Alors

$$\delta = \prod_i p_i^{\min(\alpha_i,\beta_i)} \qquad\qquad \mu = \prod_i p_i^{\max(\alpha_i,\beta_i)}$$

D'une part

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d'autre part

$$\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

Si $\min(\alpha_i,\beta_i) = \alpha_i$, alors $\max(\alpha_i,\beta_i) = \beta_i$; réciproquement si $\min(\alpha_i,\beta_i) = \beta_i$ alors $\max(\alpha_i,\beta_i) = \alpha_i$. Par conséquent tous les α_i et β_i apparaissent une fois et une seule dans le produit

$$\prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

qui est donc isomorphe à

$$\prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d) Montrons qu'un groupe abélien de type fini et de torsion est fini.

Soit G un groupe abélien de type fini et sans torsion. Puisque G est abélien de type fini on a

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

où $r \geq 0$, $n_j \geq 0$ pour tout $1 \leq j \leq s$ et n_{i+1} divise n_i pour tout $1 \leq i \leq s-1$.

De plus G est de torsion, *i.e.* tout élément est d'ordre fini. Il en résulte que $r = 0$, c'est-à-dire que

$$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

En particulier $|\mathrm{G}| = n_1 n_2 \ldots n_s < \infty$.

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Soient G un groupe abélien et $(\mathrm{H}_i)_{1\leq i\leq r}$ une famille de sous-groupes d'ordre 2 à 2 premiers entre eux. Alors ces groupes sont en somme directe dans G. En effet soit d_i l'ordre de H_i. Rappelons que dans un groupe abélien si G est d'ordre m et h d'ordre n avec n, m premiers entre eux, alors gh est d'ordre mn. Ainsi pour tout i l'ordre de tout

élément de $\sum_{j\neq i} \mathrm{H}_j$ divise $\mathrm{ppcm}_{j\neq i}(d_j)$ donc est premier avec d_i. Il en résulte que nous avons pour tout i

$$\mathrm{H}_i \cap \Big(\sum_{j\neq i} \mathrm{H}_j\Big) = \{1\}$$

Par conséquent les H_i, $1 \leq i \leq r$, sont en somme directe.

D'après ce qui précède les différents p-Sylow d'un groupe abélien fini G sont en somme directe. L'égalité des cardinaux assure que G est la somme directe de ses sous-groupes de Sylow.

Exercice 611

Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G.

Éléments de réponse 611

Soit G un groupe abélien fini. Montrons qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G. Le théorème de structure assure que

$$\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{d_2\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{d_r\mathbb{Z}}$$

où d_i divise d_{i+1} pour tout $1 \leq i \leq r-1$.

L'exposant de G est d_r et $(0, 0, \ldots, 0, 1)$ est d'ordre d_r.

Exercice 612

Montrer qu'il existe exactement 20 groupes abéliens d'ordre ≤ 15 à isomorphisme près. On donnera leur forme canonique successivement sous forme « facteurs invariants » et sous forme « facteurs élémentaires ».

Éléments de réponse 612

Il y a 15 groupes cycliques d'ordre $n \leq 15$. Pour chacun

- ◇ la décomposition en facteurs invariants consiste juste à écrire ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$;
- ◇ la décomposition en facteurs élémentaires consiste à écrire la décomposition en facteurs premiers de n.

Par exemple

Exercice 613

a) Donner la décomposition primaire du groupe ${}^{\mathbb{Z}}\!/_{8\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{24\mathbb{Z}}$. En déduire ses facteurs invariants.

b) Donner la décomposition primaire du groupe ${}^{\mathbb{Z}}\!/_{54\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{26\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{15\mathbb{Z}}$. En déduire ses facteurs invariants.

Éléments de réponse 613

a) Donnons la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

Notons que $8 = 2^3$, $12 = 2^2 \times 3$ et $24 = 2^3 \times 3$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2^3, 2^2, 3, 2^3 et 3.

Déterminons les facteurs invariants de G. Réordonnons les diviseurs élémentaires comme suit

$$\begin{array}{r} 2^2 \mid 2^3 \mid 2^3 \\ 3 \mid 3 \end{array}$$

Les facteurs invariants de G sont donc $2^2 \times 1 = 4$, $2^3 \times 3 = 24$ et $2^3 \times 3 = 24$.

Par conséquent

$$\mathrm{G} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}.$$

b) Donnons la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

Notons que $54 = 2 \times 3^3$, $26 = 2 \times 13$ et $15 = 3 \times 5$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2, 3^3, 2, 13, 3 et 5.

Donnons ses facteurs invariants. On ordonne les diviseurs élémentaires comme suit

$$\begin{array}{r} 2 \mid 2 \\ 3 \mid 3^3 \\ 5 \\ 13 \end{array}$$

Les facteurs invariants de G sont donc $2 \times 3 = 6$ et $2 \times 3^3 \times 5 \times 13 = 3510$.

Exercice 614

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathfrak{S}_n$.

Éléments de réponse 614

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Expliquons pourquoi. Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ et le nombre de groupes abéliens de cardinal 32 à isomorphisme près sont chacun en bijection avec l'ensemble des partitions de 5 (rappelons qu'une partition d'un entier est une décomposition de cet entier en une somme d'entiers strictement positifs à l'ordre près des termes).

b) Généralisons au nombre de classes de conjugaison dans $\mathfrak{S}_n$. Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphismes de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$. Considérons

$$\varphi\colon P_n \to G_n \qquad (n_1, n_2, \dots, n_r) \mapsto \text{ classe d'isomorphisme de } \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

et

$$\psi\colon P_n \to C_n \qquad (n_1, n_2, \dots, n_r) \mapsto \text{ classe de conjugaison de la permutation } (1, 2, \dots, n_1)(n_1+1, \dots, n_1+n_2)\dots(n_1+n_2+n_{r-1}+1, \dots, n)$$

φ et ψ sont des bijections donc $|C_n| = |G_n|$: il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 615

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1, 3)$ et $(2, 0)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

◇ Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(1, 1)$ et $(1, -1)$. Déterminer la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$.

Éléments de réponse 615

◇ Déterminons la structure du groupe abélien de type fini $\mathbb{Z}^2/\mathrm{H}$. On a

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Par suite $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/6\mathbb{Z}$.

◇ On a

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Par conséquent $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 616

Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2, 5)$, $(5, -1)$ et $(1, -2)$. Déterminer une base de H et décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

Éléments de réponse 616

On a

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 9 & 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}$$

donc $\mathrm{H} = \langle (0,9),\, (1,-2) \rangle$ est de rang 2.

De plus $\begin{pmatrix} 0 & 1 \\ 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 9 & 0 \end{pmatrix}$; par suite ${}^{\mathbb{Z}^2}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$.

Exercice 617

Trouver une base du groupe suivant :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases} \right\}$$

Éléments de réponse 617

Soit G le groupe donné par :

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases} \right\}$$

On a

$$\mathrm{G} = \left\{ (x,y,z) \in \mathbb{Z}^3 \,\middle|\, \begin{cases} 2x+3y+5z=0 \\ 7x+12z=0 \end{cases} \right\}$$

Comme $7x+12z=0$ on écrit $x=12k$ et $z=-7k$. Alors $2x+3y+5z=0$ conduit à $3y=11k$. On pose donc $k=3l$ alors

$$x = 36\ell, \qquad y = 11\ell, \qquad z = -21\ell$$

Finalement

$$\mathrm{G} = \{\ell(36,11,-21) \,|\, \ell \in \mathbb{Z}\} = \mathrm{Vect}(36,11,-21)$$

et $\{(36,11,-21)\}$ est une base de G.

Exercice 618

Les groupes

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \qquad\qquad {}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$$

sont-ils isomorphes ? Justifier votre réponse.

Éléments de réponse 618

D'une part $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$ et $25 = 5^2$ donc

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5^2\mathbb{Z}};$$

d'autre part $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$ donc

$${}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2^2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3^2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5^2\mathbb{Z}}.$$

En particulier les groupes

$${}^{\mathbb{Z}}\!/_{12\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{90\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{25\mathbb{Z}} \qquad\qquad {}^{\mathbb{Z}}\!/_{100\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{30\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}}$$

sont isomorphes.

Exercice 619

Soit G un groupe abélien fini.

Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Éléments de réponse 619

Raisonnons par l'absurde. Supposons que G ne soit pas cyclique. Alors G est isomorphe à $\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \ldots \times \mathbb{Z}/q_k\mathbb{Z}$ où $q_1|q_2|\ldots|q_k$ sont les facteurs invariants de G et $k \geq 2$. Il y a alors (au moins) deux sous-groupes distincts d'ordre q_1 : d'une part le facteur $\mathbb{Z}/q_1\mathbb{Z}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/q_2\mathbb{Z}$ associé au diviseur q_1 de q_2.

Exercice 620

Soit p un nombre premier. Soit G un groupe abélien fini d'ordre n tel que tous les éléments de G soient d'ordre une puissance de p.

1. Soit g un élément de $G \setminus \{id\}$. Soit $H = \langle g \rangle$ le sous-groupe cyclique engendré par g.
   Montrer que tous les éléments de G/H sont d'ordre une puissance de p.
2. En déduire par récurrence sur n que G est d'ordre une puissance de p.
   (Indication : prendre comme hypothèse de récurrence que tous les groupes d'ordre $< n$ dont tous les éléments sont d'ordre une puissance de p sont d'ordre une puissance de p).
3. Soit G un groupe fini abélien d'ordre 12.
   Montrer que si G ne contient pas d'élément d'ordre 3, il ne contient que des éléments d'ordre 1, 2 ou 4.
   En déduire que G possède un élément d'ordre 3.
4. Supposons désormais que G est un groupe abélien d'ordre 12 non cyclique. Soit $g \in G$ un élement d'ordre 3. Soit $H = \langle g \rangle$ le sous-groupe cyclique engendré par $\langle g \rangle$. Montrer que G/H ne peut être cyclique.
5. En déduire que $G/H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
6. Montrer que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Éléments de réponse 620

Exercice 621

1. Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?
   Montrer que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, alors il y a exactement $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1)$ sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que dans un groupe cyclique tous les sous-groupes sont caractéristiques [30].

30. Soit G un groupe. Un sous-groupe de G qui est stable par tout automorphisme de G est dit caractéristique.

3. Déduire de l'existence d'un p-Sylow dans un groupe G d'ordre $p^\alpha n$ (où p désigne un entier premier, n un entier premier avec p et $\alpha \geq 1$), le théorème de Cauchy, *i.e.* l'existence d'un élément d'ordre p.
4. Montrer qu'un groupe fini G a pour ordre une puissance d'un nombre premier p si et seulement si tout élément du groupe G a pour ordre une puissance de p.

Éléments de réponse 621

Exercice 622

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ sont-ils isomorphes ?
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont-ils isomorphes ?

Éléments de réponse 622

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ ne sont pas isomorphes. En effet posons
$$\mathrm{G}_1 = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}.$$
Nous avons $12 = 2^2 \times 3$, $72 = 2^3 \times 3^2$, $18 = 2 \times 3^2$ et $48 = 2^4 \times 3$. Les groupes G_1 et G_2 sont tous deux d'ordre $2^5 \times 3^3$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i$ pour $i = 1, 2$ où A_i est un groupe abélien d'ordre 2^5 et B_i un groupe abélien d'ordre 3^3. Le groupe A_1 est associé à la partition $(3, 2)$ de 5 et le groupe A_2 est associé à la partition $(4, 1)$ de 5 ; ils ne sont donc pas isomorphes. Par suite les groupes G_1 et G_2 ne sont pas isomorphes.
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont isomorphes. En effet posons
$$\mathrm{G}_1 = \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

Nous avons $72 = 2^3 \times 3^2$, $84 = 2^2 \times 3 \times 7$, $36 = 2^2 \times 3^2$ et $168 = 2^3 \times 3 \times 7$. Les groupes G_1 et G_2 sont donc de même ordre $2^5 \times 3^3 \times 7$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i \times \mathrm{C}_i$ où A_i est un groupe abélien d'ordre 2^5, B_i est un groupe abélien d'ordre 3^3 et C_i est un groupe abélien d'ordre 7. Les groupes A_1 et A_2 sont associés à la partition $(3, 2)$ de 5, ils sont isomorphes. Les groupes B_1 et B_2 sont associés à la partition $(2, 1)$ de 3 ; ils sont donc isomorphes. Les groupes C_1 et C_2 sont isomorphes. Il en résulte que G_1 et G_2 sont isomorphes.

Exercice 623

Trouver tous les couples d'entiers naturels (a, b) tels que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Éléments de réponse 623

Exercice 624

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrer que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Éléments de réponse 624

Soient a, b, c et d quatre entiers deux à deux premiers entre eux.

Montrons que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Les nombres a, b, c et d étant premiers entre deux à deux nous avons

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

$$\mathbb{Z}/cd\mathbb{Z} \simeq \mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

$$\mathbb{Z}/ac\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$$

$$\mathbb{Z}/bd\mathbb{Z} \simeq \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

Par suite les deux groupes $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ et $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$ sont isomorphes.

Exercice 625

Soit $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Considérons les deux sous-groupes suivants de G :

$$\mathrm{H} = \mathbb{Z}/2\mathbb{Z} \times \{0\} \qquad\qquad \mathrm{K} = \{0\} \times \{0, 6\}.$$

Remarquons que $\mathrm{H} \simeq \mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z}$ mais avons-nous $\mathrm{G}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$?

Éléments de réponse 625

D'une part $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, d'autre part $\mathrm{G}/\mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \times \mathbb{Z}/3\mathbb{Z}$.

Les deux premiers facteurs ne sont pas isomorphes donc les deux groupes ne sont pas isomorphes.

Exercice 626

Soient G, H et K des groupes abéliens finis.

1. Montrer que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$.
2. Montrer que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

Éléments de réponse 626

Soient G, H et K des groupes abéliens finis. Montrons que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$et que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

La décomposition primaire de G est $\prod_{i=1}^{s} \mathrm{A}_i$, celle de $\mathrm{G} \times \mathrm{G}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \mathrm{A}_i$.

La décomposition primaire de H est $\prod_{i=1}^{t} \mathrm{B}_i$, celle de $\mathrm{H} \times \mathrm{H}$ est donc $\prod_{i=1}^{t} \mathrm{B}_i \times \mathrm{B}_i$.

La décomposition primaire de K est $\prod_{i=1}^{u} \mathrm{C}_i$, celle de $\mathrm{G} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \prod_{i=1}^{u} \mathrm{C}_i$ et celle de $\mathrm{H} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{B}_i \times \prod_{i=1}^{u} \mathrm{C}_i$.

Si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par suite $\mathrm{G} \simeq \mathrm{H}$.

Si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par conséquent $\mathrm{G} \simeq \mathrm{H}$.

Exercice 627

1. Exprimer tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.
2. Exprimer tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques.

Éléments de réponse 627

1. Exprimons tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.

   Les groupes abéliens d'ordre $99 = 3^2 \times 11$ sont isomorphes

   - soit à $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$,
   - soit à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

2. Exprimons tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques. Les groupes abéliens d'ordre $100 = 2^2 \times 5^2$ sont isomorphes

   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 628

Combien existe-t-il, à isomorphisme près, de groupes abéliens d'ordre 10^6 ?

Éléments de réponse 628

Nous avons $10^6 = 2^6 \times 5^6$. Les partitions de 6 sont

$$(6)$$
$$(5,1)$$
$$(4,2)$$
$$(4,1,1)$$
$$(3,3)$$
$$(3,2,1)$$
$$(3,1,1,1)$$
$$(2,2,2)$$
$$(2,2,1,1)$$
$$(2,1,1,1,1)$$
$$(1,1,1,1,1,1)$$

Elles sont donc au nombre de 11. Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 629

1. Soient G, H, G′ et H′ des groupes finis tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. Nous allons montrer qu'alors $H \simeq H'$.
   Étant donnés deux groupes finis G_1 et G_2, notons $m(G_1, G_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(G_1, G_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.
   a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(G_1, G_2) = \sum_{N \trianglelefteq G_1} i\Big({}^{G_1}\!/_{N}, G_2\Big). \tag{1.16.1}$$

   b) Montrer pour tout groupe fini L que

$$m(L, G) \cdot m(L, H) = m(L, G \times H).$$

   c) En déduire que pour tout groupe fini L on a l'égalité $m(L, H) = m(L, H')$.
   d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (3.6.2) que

$$i(L, H) = i(L, H'). \tag{1.16.2}$$

   e) Appliquer l'équation (1.16.4) à H pour en déduire que $H \simeq H'$.
   f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors en général H et H′ ne sont pas isomorphes.

2. Nous allons appliquer le résultat obtenu dans la partie 1. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
   Soit G un groupe abélien fini. Supposons que
   $$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$
   avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.
   a) Montrer que l'exposant de G est égal à n_1.
   b) Utiliser le résultat obtenu dans la partie 1. pour montrer que cette décomposition est unique.

Éléments de réponse 629

Exercice 630

Soit G un groupe abélien fini. Les assertions suivantes sont-elles vraies ou fausses ?

a) Pour tout d qui divise l'ordre de G, le groupe G admet un élément d'ordre d.

b) Pour tout d qui divise l'ordre de G, le groupe G admet un sous-groupe d'ordre d.

Éléments de réponse 630

Exercice 631

a) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12 et 72.

b) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Éléments de réponse 631

a) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 12.
   Nous avons $12 = 2^2 \times 3$. De plus les partitions de 2 sont

   2 1, 1

   Par conséquent il y a à isomorphisme près 2 groupes abéliens d'ordre 12 :
   $$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
   Déterminons à isomorphisme près tous les groupes abéliens d'ordre 72.
   Nous avons $72 = 2^3 \times 3^2$. De plus les partitions de 2 sont

   2 1, 1

   et celles de 3 sont

   3 2, 1 1, 1, 1

Par conséquent il y a à isomorphisme près $2 \times 3 = 6$ groupes abéliens d'ordre 72 :

$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

b) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Nous avons $10^6 = 2^6 \times 5^6$. De plus les partitions de 6 sont

6
5, 1
4, 2
4, 1, 1
3, 3
3, 2, 1
3, 1, 1, 1
2, 2, 2
2, 2, 1, 1
2, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 1

Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 632

a) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3 \mid 5g_1 - 2g_2 + 12g_3 = 3g_1 + 4g_3 = 0 \rangle.$$

Déterminer la structure de ce groupe.

b) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3, g_4 \mid 2g_1 + 4g_2 - 4g_4 = 6g_1 - 12g_3 + 3g_4 = 0 \rangle.$$

Déterminer la structure de ce groupe.

Éléments de réponse 632

Exercice 633

Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Éléments de réponse 633

Nous utilisons le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}\right) \times \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}\right)$$

Notons que cette écriture est la décomposition en composantes p-primaires. En effet $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$, $25 = 5^2$, $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$.

Nous pouvons aussi écrire la décomposition en facteurs invariants de ces deux groupes, nous trouvons

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}.$$

Exercice 634

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Éléments de réponse 634

Montrons qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Soit G un groupe abélien fini non cyclique. Il est isomorphe à un produit

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_i \geq 2$ et $d_i \,|\, d_{i+1}$. Puisque G n'est pas cyclique, $r \geq 2$. Soit p un facteur premier de d_1 alors p disvise tous les d_i et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Le sous-groupe de p torsion de G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^r$ qui contient un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 635

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.

b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Éléments de réponse 635

a) La décomposition de 360 en facteurs premiers est $2^3 \times 3^2 \times 5$. Ainsi si G est un groupe de cardinal 360, alors le sous-groupe

$$T_2(\mathrm{G}) = \{g \in \mathrm{G} \,|\, \exists\, n \in \mathbb{N} \quad 2^n g = 0\}$$

de 2-torsion de G est un groupe abélien de cardinal 2^3, il y a donc trois classes d'isomorphisme de tels groupes : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. De même il y a exactement deux classes d'isomorphisme possibles pour $T_3(\mathrm{G})$ à savoir $\mathbb{Z}/9\mathbb{Z}$ et $\left(\mathbb{Z}/3\mathbb{Z}\right)^2$. Par ailleurs $T_5(\mathrm{G})$

est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Il y a donc exactement six classes d'isomorphisme de groupes abéliens d'ordre 360 donc les décompositions p-primaires et les décompositions en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/360\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times 4\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

b) Plus généralement, pour tout entier n, déterminons le nombre de groupes abéliens de cardinal n. Nous utilisons la classification des classes d'isomorphisme de groupes abéliens finis. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. La classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, d_2, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i \mid d_{i+1}$ et $d_1 d_2 \dots d_s = n$. Par suite chaque d_i se décompose comme suit : $d_i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \dots p_r^{\alpha_{r,i}}$ avec les contraintes suivantes : $\alpha_{i,j} \leq \alpha_{i+1,j}$ pour tout j, pour tout i et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$ et $\sum_{i=1}^{q} \alpha_{i,j} = \alpha_j$.

Il s'en suit que le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$ où $p(\alpha)$ désigne le nombre de partitions de α, *i.e.* le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 636

a) On considère $\mathrm{H} = \{(a,b) \in \mathbb{Z}^2 \mid a - b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$. Calculer le rang de H. Donner une base de H. Décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

b) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4, 8, 10)$ et $(6, 2, 0)$. Déterminer la structure du groupe H.

Éléments de réponse 636

a) Soit φ le morphisme de groupes donné par

$$\varphi \colon \mathbb{Z}^2 \to \mathbb{Z}/10\mathbb{Z}, \qquad (a,b) \mapsto a - b$$

Son noyau est H. En particulier H est un sous-groupe distingué de $\mathbb{Z}^2$.

D'une part H contient $(1,1)$ et $(0,10)$ donc $\operatorname{rg} \mathrm{H} \geq 2$. D'autre part $\mathrm{H} \subset \mathbb{Z}^2$ donc $\operatorname{rg} \mathrm{H} \leq 2$. Finalement $\operatorname{rg} \mathrm{H} = 2$.

Soit (a, b) dans H. Il existe n dans $\mathbb{Z}$ tel que $a = b + 10n$ et

$$(a, b) = (a, a - 10n) = a(1, 1) + (-n)(0, 10).$$

Autrement dit $((1, 1), (0, 10))$ est une base de H.

Par ailleurs

$$\mathbb{Z}^2/\mathrm{H} = \langle (g_1, g_2) \,|\, g_1 + g_2 = 0,\ 10g_2 = 0 \rangle.$$

Puisque $\begin{pmatrix} 1 & 0 \\ 1 & 10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$ les facteurs invariants de $\mathbb{Z}^2/\mathrm{H}$ sont 1 et 10 et $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/10\mathbb{Z}$.

b) Notons H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4, 8, 10)$ et $(6, 2, 0)$. Déterminons la structure du groupe H. Nous avons

$$\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix}$$

Ainsi les facteurs invariants de $\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix}$ sont 2 et 10 et $\mathrm{H} \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Exercice 637

Soit $n \geq 1$ un entier. Montrer que tout système libre maximal dans $\mathbb{Z}^n$ est de cardinal n. Donner un exemple où un tel système n'est pas une base.

Éléments de réponse 637

Exercice 638

Soit $e_1 = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ un vecteur tel que le pgcd de ses coordonnées vaut 1. Montrer que l'on peut compléter e_1 en une base $(e_1, e_2, \ldots, e_n)$ de $\mathbb{Z}^n$.

Éléments de réponse 638

Exercice 639

Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

a) $\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}$;

b) $\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}$;

c) $\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}$.

Éléments de réponse 639

Nous pouvons procéder de deux manières différentes :

- soit en calculer le pgcd des coefficients de la matrice puis le pgcd des mineurs de taille 2, etc
- soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes.

Dans les deux cas nous obtenons ($\sim$ désigne l'équivalence des matrices à coefficients entiers) :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Les facteurs invariants sont donc respectivement $(1, 6)$, $(3, 9)$ et $(1, 2, 16)$.

Détaillons la première équivalence :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Détaillons la seconde équivalence :

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 12 & -27 \\ 69 & -153 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -27 \\ 9 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & -3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 12 & 3 \\ 9 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 12 \\ 0 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}.$$

Détaillons la dernière équivalence :

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -75 & 41 & -13 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -3 & 5 & -1 \\ 12 & -6 & 2 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -12 & 6 & -2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 0 & -14 & 2 \\ -3 & 5 & -1 \\ 19 & -3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -19 & 3 & -3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & -27 & 3 \\ -3 & 5 & -1 \\ 0 & -14 & 2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 3 & -5 & 1 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & -86 & 10 \\ -1 & -27 & 3 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 27 & -3 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -86 & 10 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -14 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & -2 \\ 0 & -2 & -2 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -16 \\ 0 & -2 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -16 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -16 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Exercice 640

a) Soit G un groupe abélien de type fini. Soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme surjectif. Montrer que f est un isomorphisme.

Ceci est-il nécessairement vrai si on remplace surjectif par injectif ?

b) Soit G un groupe abélien libre de type fini et soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme. Définir le déterminant $\det(f) \in \mathbb{Z}$ de f. Montrer que f est injectif si et seulement si $\det(f) \neq 0$. Dans ce cas montrer que $|\det(f)| = |\mathrm{coker}(f)|$.

Éléments de réponse 640

Exercice 641

Le but de cet exercice est de redémontrer le théorème de structure des groupes abéliens finis. On rappelle qu'un caractère d'un groupe abélien fini G est un morphisme $\mathrm{G} \to \mathbb{C}^*$.

a) Si H est un sous-groupe d'un groupe abélien fini G, montrer que tout caractère de H se prolonge en un caractère de G.

b) Soit G un groupe abélien fini. On désigne par H un sous-groupe de G engendré par un élément de G d'ordre maximal. Montrer qu'on a l'isomorphisme $\mathrm{G} \simeq \mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

c) Conclure.

Éléments de réponse 641

Exercice 642 [Propriété d'annulation de groupes dans un produit direct (démonstration de Vipul Naik)]

A. Soient G, H, G′ et H′ des groupes finis tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. Nous allons montrer qu'alors $H \simeq H'$.
Étant donnés deux groupes finis G_1 et G_2, notons $m(G_1, G_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(G_1, G_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.

a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(G_1, G_2) = \sum_{N \trianglelefteq G_1} i\Big(G_1/N, G_2\Big). \tag{1.16.3}$$

b) Montrer pour tout groupe fini L que

$$m(L, G) \cdot m(L, H) = m(L, G \times H).$$

c) En déduire que pour tout groupe fini L on a l'égalité $m(L, H) = m(L, H')$.

d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (3.6.2) que

$$i(L, H) = i(L, H'). \tag{1.16.4}$$

e) Appliquer l'équation (1.16.4) à H pour en déduire que $H \simeq H'$.

f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors en général H et H′ ne sont pas isomorphes.

B. Nous allons appliquer le résultat obtenu dans la partie A. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
Soit G un groupe abélien fini. Supposons que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.

a) Montrer que l'exposant de G est égal à n_1.

b) Utiliser le résultat obtenu dans la partie A. pour montrer que cette décomposition est unique.

Éléments de réponse 642

Exercice 643

Soit $\Bbbk$ un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif $\Bbbk^\times = \Bbbk \setminus \{0\}$ de $\Bbbk$. Montrer que G est cyclique.

Éléments de réponse 643

Nous utilisons le théorème de structure des groupes abéliens finis. Si $|\mathrm{G}| > 1$, alors il existe une suite d'entiers $1 < a_1 \,|\, a_2 \,|\, \ldots \,|\, a_r$ tels que

$$\mathrm{G} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_r\mathbb{Z}$$

Montrons que $r = 1$. Puisque $a_r\mathrm{G} = \{0\}$ nous avons

$$\#\{z \in \Bbbk \,|\, z^{a_r} = 1\} \geq |\mathrm{G}| = a_1 a_2 \ldots a_r.$$

Par ailleurs le nombre de racines dans $\Bbbk$ du polynôme $X^{a_r} - 1 \in \Bbbk[X]$ est inférieur ou égal à son degré parce que $\Bbbk$ est commutatif. Il en résulte l'inégalité $a_1 a_2 \ldots a_r \leq a_r$ qui conduit à $r = 1$.

1.17. Produits semi-directs

Exercice 644

Soient N et H des groupes et soit $\phi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ un morphisme de groupes. Notons $\mathrm{N} \rtimes_\phi \mathrm{H}$ l'ensemble $\mathrm{N} \times \mathrm{H}$ muni de la loi de composition définie par

$$(n_1, h_1) \rtimes_\phi (n_2, h_2) = \big(n_1\phi(h_1)(n_2), h_1h_2\big).$$

1. Montrer que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe appelé produit semi-direct de H par N relativement à ϕ.
2. Montrer que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.
3. Identifier le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Éléments de réponse 644

1. Montrons que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe.
   - Commençons par montrer que la loi est associative.
     Soient n_1, n_2 et n_3 dans N. Soient h_1, h_2 et h_3 dans H. Par définition du produit nous avons

$$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = \big(n_1\phi(h_1)(n_2), h_1h_2\big) \rtimes_\phi (n_3, h_3) = \big(n_1\phi(h_1)(n_2)\phi(h_1h_2)(n_3), h_1h_2h_3\big).$$

     De même nous avons

$$(n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big) = (n_1, h_1) \rtimes_\phi \big(n_2\phi(h_2)(n_3), h_2h_3\big) = \big(n_1\phi(h_1)(n_2\phi(h_2)(n_3))\big), h_1h_2h_3\big).$$

     Or $\phi(h_1)$ et ϕ sont des morphismes donc

$$\phi(h_1)(n_2\phi(h_2)(n_3)) = \phi(h_1)(n_2)(\phi(h_1) \circ \phi(h_2))(n_3) = \phi(h_1)(n_2)(\phi(h_1h_2))(n_3)$$

dont on déduit que

$$((n_1,h_1)\rtimes_\phi(n_2,h_2))\rtimes_\phi(n_3,h_3)=(n_1,h_1)\rtimes_\phi((n_2,h_2)\rtimes_\phi(n_3,h_3)).$$

Par conséquent le produit $\rtimes_\phi$ est associatif.

- On voit tout de suite que l'élément $(e_{\mathrm{N}},e_{\mathrm{H}})$ est neutre pour la loi $\rtimes_\phi$.
- Montrons que tout élément admet un inverse.
  Soient $n\in\mathrm{N}$ et $h\in\mathrm{H}$. Pour tous $n'\in\mathrm{N}$ et $h'\in\mathrm{H}$ nous avons
  $$(n,h)\rtimes_\phi(n',h')=(e_{\mathrm{N}},e_{\mathrm{H}})$$
  si et seulement si
  $$(n\phi(n')(h'),hh')=(e_{\mathrm{N}},e_{\mathrm{H}})$$
  si et seulement si $h'=h^{-1}$ et $n'=\phi(h^{-1})(n^{-1})$. Le calcul de $(n',h')\rtimes_\phi(n,h)$ est similaire ce qui assure que (n,h) est inversible et que son inverse est $(n,h)^{-1}=(\phi(h^{-1})(n^{-1}),h^{-1})$.

Ainsi $\mathrm{N}\rtimes_\phi\mathrm{H}$ est bien un groupe.

2. Montrons que $\mathrm{N}\times\{e_{\mathrm{H}}\}\lhd\mathrm{N}\rtimes_\phi\mathrm{H}$ et $\{e_{\mathrm{N}}\}\times\mathrm{H}\subset\mathrm{N}\rtimes_\phi\mathrm{H}$.

   Les formules définissant le produit assurent que $\mathrm{N}\times\{e_{\mathrm{H}}\}$ et $\{e_{\mathrm{N}}\}\times\mathrm{H}$ sont bien des sous-groupes de $\mathrm{N}\rtimes_\phi\mathrm{H}$ car $\phi(h)(e_{\mathrm{N}})=e_{\mathrm{N}}$ pour tout $h\in\mathrm{H}$.

   Montrons que $\mathrm{N}\times\{e_{\mathrm{H}}\}$ est distingué dans $\mathrm{N}\rtimes_\phi\mathrm{H}$. Soient n, n' dans N et h' dans H. Alors

$$\begin{aligned}(n,h)\rtimes_\phi(n',e_{\mathrm{H}})\rtimes_\phi(n,h)^{-1} &= (n,h)\rtimes_\phi(n',e_{\mathrm{H}})\rtimes_\phi(\phi(h^{-1})(n^{-1}),h^{-1})\\ &= n\phi(h)(n'),h()\rtimes_\phi(\phi(h^{-1})(n^{-1}),h^{-1})\\ &= (n\phi(h)(n')\phi(h)(\phi(h^{-1})(n^{-1})),e_{\mathrm{H}})\\ &= (n\phi(h)(n')n^{-1},e_{\mathrm{H}})\in\mathrm{N}\times\{e_{\mathrm{H}}\}\end{aligned}$$

   Ainsi $\mathrm{N}\times\{e_{\mathrm{H}}\}$ est distingué dans $\mathrm{N}\rtimes_\phi\mathrm{H}$.

   Un calcul analogue montre que $\{e_{\mathrm{N}}\}\times\mathrm{H}$ n'est pas distingué en général.

3. Identifions le quotient de $\mathrm{N}\rtimes_\phi\mathrm{H}$ par $\mathrm{N}\times\{e_{\mathrm{H}}\}$.

   Considérons l'application naturelle $\pi\colon\mathrm{N}\rtimes_\phi\mathrm{H}\to\mathrm{H}$ donnée par la seconde projection, *i.e.* $\pi(n,h)=h$.

   Il est clair que π est surjective.

   La définition de la loi de groupes assure que π est un morphisme de groupes.

   Déterminons son noyau. Soient $n\in\mathrm{N}$ et $h\in\mathrm{H}$. Nous avons $\pi(n,h)=e_{\mathrm{H}}$ si et seulement si $h=e_{\mathrm{H}}$; ainsi $\ker\pi=\mathrm{N}\times\{e_{\mathrm{H}}\}$.

   Finalement l'application π passe au quotient par son noyau et induit un isomorphisme de groupes :
   $$\overline{\pi}\colon{}^{\mathrm{N}\rtimes_\phi\mathrm{H}}\!\diagup_{\mathrm{N}\times\{e_{\mathrm{H}}\}}\xrightarrow{\sim}\mathrm{H}$$

Exercice 645

Soit G un groupe. Soient N et H deux sous-groupes de G tels que $\mathrm{N} \cap \mathrm{H} = \{e\}$, $\mathrm{G} = \mathrm{NH}$ et $\mathrm{N} \triangleleft \mathrm{G}$.

1. Montrer que l'application
$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$
est un morphisme de groupes.
2. Montrer que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un isomorphisme de groupes.

On dit alors que G est le produit semi-direct de H par N.

Éléments de réponse 645

1. Montrons que l'application
$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$
est un morphisme de groupes.

   L'application i est bien définie car $\mathrm{N} \triangleleft \mathrm{G}$. On vérifie directement que c'est un morphisme de groupes.
2. Montrons que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un morphisme de groupes. Soient n, n' dans N et h, h' dans H. On a
$$f(n,h)f(n',h') = nhn'h'$$
et
$$f\big((n,h) \rtimes_i (n',h')\big) = f\big(ni(h)(n'), hh'\big) = f(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h'$$
ce qui assure que $f\big((n,h) \rtimes_i (n',h')\big) = f(n,h)f(n',h')$. Ainsi f est bien un morphisme de groupes.

   Montrons maintenant que f est un isomorphisme de groupes. L'hypothèse $\mathrm{NH} = \mathrm{G}$ assure que f est surjectif et l'hypothèse $\mathrm{N} \cap \mathrm{H} = \{e\}$ assure que le noyau de f est trivial. Par suite f est un isomorphisme.

Exercice 646

Montrer que le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Éléments de réponse 646

Le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si pour tous n, $n' \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (n',h') = (n', hh')$$

si et seulement si pour tous n, $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $\phi(h)(n') = nn'$ si et seulement si ϕ est le morphisme trivial.

Pour tous $n \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (e_\mathrm{N}, h') \rtimes_\phi (n,h)^{-1} = (n\phi(hh'h^{-1})(n^{-1}), hh'h^{-1}).$$

Ainsi le morphisme ϕ est trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Exercice 647

Soit

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

une suite exacte (courte).

1. Montrer que si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.
2. Réciproquement soit une telle suite exacte. Si p possède une section, c'est-à-dire s'il existe un morphisme de groupes $s\colon \mathrm{H} \to \mathrm{G}$ tel que $p \circ s = \mathrm{id}_\mathrm{H}$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.
3. Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Éléments de réponse 647

1. Supposons que $\mathrm{G} = \mathrm{N} \rtimes_\phi \mathrm{H}$. D'après l'Exercice **??** 3. on dispose d'un morphisme surjectif $\pi\colon \mathrm{G} \to \mathrm{H}$ dont le noyau est le sous-groupe $\mathrm{N} \rtimes_\phi \{e_\mathrm{H}\}$ qui est isomorphe à N. Par suite on a bien une suite exacte

   $$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

   où $i\colon \mathrm{N} \to \mathrm{G}$ est défini par $i(n) = (n, e_\mathrm{H})$. De plus on peut vérifier que l'application

   $$\mathrm{H} \to \mathrm{G} \qquad\qquad h \mapsto (e_\mathrm{N}, h)$$

   est une section de π.

2. C'est une conséquence de l'Exercice **??** appliqué aux sous-groupes $\mathrm{N}' = i(\mathrm{N})$ et $\mathrm{H}' = s(\mathrm{H})$ de G. Il suffit donc de vérifier que N' et G' satisfont les hypothèses de l'Exercice **??**. Le groupe N' est distingué dans G car $\mathrm{N}' = \ker p$. Soit $g \in \mathrm{G}$. Posons $h = s(\pi(g)) \in \mathrm{H}'$. Alors
$$\pi(h) = \pi(s(\pi(g))) = \pi(g)$$
donc $n = gh^{-1}$ appartient à $\ker \pi = \mathrm{N}'$. Finalement nous avons bien $\underbrace{g}_{\in \mathrm{G}} = \underbrace{n}_{\in \mathrm{N}'}\underbrace{h}_{\in \mathrm{H}'}$ ce qui assure que $\mathrm{G} = \mathrm{N}'\mathrm{H}'$. Soit $g \in \mathrm{N}' \cap \mathrm{H}'$. Puisque $g \in \mathrm{H}'$ il existe $h \in \mathrm{H}$ tel que $g = s(h)$. Comme $g \in \mathrm{N}'$ nous avons $\pi(g) = e_{\mathrm{H}}$. Par suite $\pi(s(h)) = e_{\mathrm{H}}$, *i.e.* $h = e_{\mathrm{H}}$, donc $g = s(e_{\mathrm{H}}) = e_{\mathrm{G}}$. Il s'en suit que $\mathrm{N}' \cap \mathrm{H}' = \{e_{\mathrm{G}}\}$. Nous pouvons donc bien appliquer l'Exercice **??** pour conclure.

3. Considérons la suite exacte courte
$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$
où p est la réduction modulo 2. C'est bien une suite exacte courte, en revanche p n'admet pas de section puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2 alors que tous ses antécédents par p sont d'ordre 4. Il s'en suit que $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

   Un autre exemple est donné par le groupe des quaternions $\mathbb{H}_8$ dont le centre $Z(\mathbb{H}_8)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $\mathbb{H}_8/Z(\mathbb{H}_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ce qui fournit une suite exacte
$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$
telle que p n'admet pas de section (on peut par exemple le voir en listant les éléments d'ordre 2 dans $\mathbb{H}_8$). Il en résulte que $\mathbb{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 648

Nous avons vu en cours que
$$\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*.$$
Ces produits semi-directs sont-ils directs ?

Éléments de réponse 648

On peut vérifier que les produits
$$\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$
ne sont pas directs (sauf pour $n = 2$) quelle que soit la section choisie. On peut en fait vérifier qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

Le cas $\mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*$ est moins évident pour $n \geq 2$. Si $x \mapsto x^n$ est un automorphisme de $\Bbbk^*$, on note $a\colon \Bbbk^\times \to \Bbbk^\times$ son inverse. L'application

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto A\mathrm{diag}(a(t),a(t),\dots,a(t))$$

est un isomorphisme.

Réciproquement supposons qu'il existe un isomorphisme de groupes

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto \phi(A)s(t).$$

Le sous-groupe dérivé de $\mathrm{SL}(n,\Bbbk) \times \Bbbk^*$ est $\mathrm{SL}(n,\Bbbk) \times \{1\}$ et celui de $\mathrm{GL}(n,\Bbbk)$ est $\mathrm{SL}(n,\Bbbk)$. Par conséquent ϕ est un automorphisme de $\mathrm{SL}(n,\Bbbk)$. De plus $\alpha(\Bbbk^*) = s(\Bbbk^*)$ commute avec tout élément de $\mathrm{GL}(n,\Bbbk)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}(n,\Bbbk)$ est formé des homothéties). Ainsi l'application $t \mapsto s(t)$ est un morphisme injectif de $\Bbbk^*$ vers $\mathrm{GL}(n,\Bbbk)$ de la forme $t \mapsto \mathrm{diag}(a(t),a(t),\dots,a(t))$.

Le noyau de det étant $\mathrm{SL}(n,\Bbbk)$ on a $a(t)^n = 1$ si et seulement si $a(t) = 1$. Puisque $t \mapsto a(t)$ est injectif, $t \mapsto a(t)^n$ l'est aussi. Or det est surjectif sur $\Bbbk^*$ donc $t \mapsto a(t)^n = a(t^n)$ est bijectif. Il en résulte que $x \mapsto x^n$ est bijectif et donc un automorphisme de $\Bbbk^*$.

Ainsi $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$ si et seulement si le morphisme $(\cdot)^n\colon \Bbbk^* \to \Bbbk^*$ est un automorphisme. En particulier

- si $\Bbbk = \mathbb{R}$ et n est impair, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$;
- si $\Bbbk$ est un corps fini de caractéristique p et si n est égal à une puissance de p, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$.

Exercice 649

Soit $\mathrm{G} = \mathrm{N} \rtimes \mathrm{H}$. Soit K un sous-groupe de G contenant N. Montrer que $\mathrm{K} = \mathrm{N} \rtimes (\mathrm{K} \cap \mathrm{H})$.

Éléments de réponse 649

On va appliquer ce qu'on a vu dans l'Exercice **??** :

— $\mathrm{N} \lhd \mathrm{G}$ et $\mathrm{N} \subset \mathrm{K}$ donc $\mathrm{N} \lhd \mathrm{K}$;

— $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{K} \subset \mathrm{G}$ donc $\mathrm{H} \cap \mathrm{K} \subset \mathrm{K}$;

— $\mathrm{N} \cap \mathrm{H} = \{e\}$ donc $\mathrm{N} \cap (\mathrm{K} \cap \mathrm{N}) = \{e\}$;

— $\mathrm{NH} = \mathrm{G}$ donc si $k \in \mathrm{K}$, alors $k = nh$ avec $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Puisque $\mathrm{N} \subset \mathrm{K}$ nous en déduisons que $h \in \mathrm{H} \cap \mathrm{K}$. D'où $\mathrm{N}(\mathrm{H} \cap \mathrm{K}) = \mathrm{K}$.

Exercice 650

Soient H et N des groupes. Soient φ, $\psi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ soient isomorphes.

1. S'il existe un automorphisme α de H tel que $\psi = \varphi \circ \alpha$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.

2. S'il existe un automorphisme u de N tel que
$$\forall\, h \in \mathrm{H} \qquad \phi(h) = u\psi(h)u^{-1}$$
montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.
3. Si H est cyclique et si $\varphi(\mathrm{H}) = \psi(\mathrm{H})$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.

Éléments de réponse 650

1. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (n, \alpha(h))$$
est un isomorphisme.
2. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (u(n), h)$$
est l'isomorphisme.
3. Le groupe H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{im}\varphi = \operatorname{im}\psi$ est isomorphe à $\mathbb{Z}/m\mathrm{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$
est surjective, il existe $d' \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ qui s'envoie sur d.

   La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait les conditions de 1. d'où le résultat.

Exercice 651

Soit p un nombre premier.

a) Quel est l'ordre d'un p-Sylow de $\mathfrak{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathfrak{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire
$$(p-1)! \equiv -1 \bmod p.$$

Éléments de réponse 651

a) L'ordre de $\mathfrak{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathfrak{S}_p$ est d'ordre p.

b) Une rédaction possible :

Pour déterminer le nombre de p-Sylow de $\mathfrak{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathfrak{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur Z_σ de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in Z_\sigma$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de Z_σ est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathfrak{S}_p$ car $\mathfrak{S}_p/Z_\sigma$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathfrak{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible :

Un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathfrak{S}_p$ [31]. Par ailleurs tout élément d'ordre p de $\mathfrak{S}_p$ vit dans un p-sous-groupe de Sylow ; réciproquement, comme p est premier et qu'un p-sous-groupe de Sylow de $\mathfrak{S}_p$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il existe exactement $p-1$ éléments d'ordre p dans chaque p-sous-groupe de Sylow de $\mathfrak{S}_p$ (puisque dans $\mathbb{Z}/p\mathbb{Z}$ tous les éléments non nuls sont générateurs). Ainsi, il y a $n_p = \frac{(p-1)!}{p-1} = (p-2)!$ p-sous-groupes de Sylow dans $\mathfrak{S}_p$.

c) Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 652

Montrer que tout groupe d'ordre 255 est cyclique.

Éléments de réponse 652

Soit G un groupe d'ordre $255 = 3 \times 5 \times 17$. Soit n_3 (respectivement n_5, respectivement n_{17}) le nombre de 3-Sylow (respectivement 5-Sylow, respectivement 17-Sylow) de G. Les théorèmes de Sylow assurent que

$$n_3 \in \{1, 85\}, \qquad n_5 \in \{1, 51\} \qquad n_{17} = 1.$$

On ne peut pas avoir $(n_3, n_5) = (85, 51)$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$.

31. Le nombre de k-cycles dans $\mathfrak{S}_p$ est le nombre d'arrangements de k parmi p divisé par k (car un k-cycle s'écrit de k façons différentes) ce qui donne : $\frac{p!}{k(p-k)!}$

Supposons que $n_3 = 1$ (le cas $n_5 = 1$ se résoud de manière analogue). Notons S_3 le seul 3-Sylow de G, S_{17} le seul 17-Sylow de G et S_5 un 5-Sylow quelconque. Nous avons

— $S_3S_{17} \simeq S_3 \times S_{17} \lhd \mathrm{G}$;

— $S_3S_{17} \cap S_5 = \{e\}$;

— $S_3S_{17}S_5 = \mathrm{G}$.

L'exercice **??** assure que $\mathrm{G} \simeq S_3S_{17} \rtimes S_5$. Soit $\phi\colon S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{16\mathbb{Z}}$ donc ϕ est trivial et le produit semi-direct. On conclut par le lemme chinois.

Exercice 653

Soit p un nombre premier impair.

1. Déterminer les p-Sylow de $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$.
2. Soient ϕ et ψ des morphismes non triviaux de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$. Pour tout entier k notons ϕ_k le morphisme ϕ_k défini par $\phi_k(x) = \phi(kx)$. Montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$ tels que $\psi = P\phi_k P^{-1}$.
3. Montrer qu'il existe un produit semi-direct non trivial $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^2 \rtimes {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.
4. Montrer que le centre de ce dernier groupe est isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. (On rappelle que si G est un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène, alors G est abélien.)
5. Supposons que G est un groupe fini. Notons p le plus petit nombre premier divisant le cardinal de G.

   Montrer que tout sous-groupe de G d'indice p est distingué (indication : commencer par montrer que tout sous-groupe H de G d'indice p agit trivialement sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$, en déduire que H est distingué dans G).
6. Soit G un groupe d'ordre p^3 non cyclique contenant un élément g d'ordre p^2. Montrer que $\langle g \rangle$ est distingué dans G et que G est un produit semi-direct de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ par $\langle g \rangle \simeq {}^{\mathbb{Z}}\!/_{p^2\mathbb{Z}}$.

Éléments de réponse 653

1. Les p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe
$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p \right\}$$
des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ et que tous sont conjugués, une matrice de $\mathrm{GL}(2, \mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre p^2 telles matrices (à la main...) et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). Remarquons que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2. Puisque les images de ψ et φ sont des p-Sylow de $\mathrm{GL}(2,\mathbb{F}_p)$ elles sont conjuguées par une matrice $P \in \mathrm{GL}(2,\mathbb{F}_p)$. Notons

$$\varphi_{(P)} \colon \mathbb{Z}/p\mathbb{Z} \to \psi\left(\mathbb{Z}/p\mathbb{Z}\right) \qquad\qquad x \mapsto P\varphi(x)P^{-1}$$

c'est un isomorphisme. Dès lors $(\varphi_{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, *i.e.* de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

3. Puisque $\mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\right) \simeq \mathrm{GL}(2,\mathbb{F}_p)$ le 1. assure l'existence d'un produit semi-direct non trivial $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

4. Comme le centre d'un p-groupe est non trivial, le centre de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ est d'ordre p, p^2 ou p^3. Si $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ était d'ordre p^2 ou p^3, alors $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ serait abélien (en effet si G est un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est monogène, alors G est abélien) : contradiction avec le fait que le produit semi-direct n'est pas trivial. Il s'en suit que $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

5. Notons p le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de G d'indice p. Posons $X = \mathrm{G}/\mathrm{H}$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi \colon \mathrm{G} \to \mathfrak{S}_X$. Intéressons-nous à la restriction de cette action au sous-groupe H, autrement dit au morphisme $\varphi \colon \mathrm{H} \to \mathfrak{S}_X$. Puisque H agit trivialement sur la classe x_0 de H dans $X = \mathrm{G}/\mathrm{H}$ l'action de H sur X induit une action de H sur $X' = X \smallsetminus \{x_0\}$ c'est-à-dire un morphisme de groupes $\psi \colon \mathrm{H} \to \mathfrak{S}_{X'}$. Or $|X'| = p - 1$ donc tous les facteurs premiers de $|\mathfrak{S}_{X'}|$ sont strictement inférieurs à p. Or les facteurs premiers de $|\mathrm{H}|$ sont par hypothèse tous supérieurs ou égaux à p. Par suite $|\mathrm{H}|$ et $|\mathfrak{S}_{X'}|$ sont premiers entre eux. Le morphisme ψ est donc trivial. Il en résulte que H agit trivialement sur X' et donc aussi sur X.

   Montrons que cela implique que G est distingué dans G. Soit $h \in \mathrm{H}$ et soit $g \in \mathrm{G}$. Puisque H agit trivialement sur X on a $h \cdot (g\mathrm{H}) = g\mathrm{H}$ donc $(g^{-1}hg)\mathrm{H} = \mathrm{H}$, par suite $g^{-1}hg$ appartient à H, *i.e.* H est distingué dans G.

6. Le sous-groupe $\langle g \rangle$ est d'indice p dans un groupe d'ordre p^3. D'après 5. le groupe $\langle g \rangle$ est donc distingué dans G.

   De plus le quotient $\mathrm{G}/\langle g \rangle$ est d'ordre p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

   Soit $y \in \mathrm{G} \smallsetminus \langle g \rangle$. Alors y^p appartient à $\langle g \rangle$ et $y^{p^2} = e$. Il existe donc $k \in \mathbb{Z}$ tel que $y^p = g^{pk}$. Comme $\langle g \rangle$ est distingué dans G il existe un entier $r \geq 0$ tel que $y^{-1}gy = g^r$. Alors pour tout $\ell \in \mathbb{N}$ nous avons $g^\ell y = yg^{\ell r}$. On cherche $z \in \mathrm{G} \smallsetminus \langle g \rangle$ d'ordre p ; plus précisément on cherche $z \in \mathrm{G} \smallsetminus \langle g \rangle$ d'ordre p sous la forme $z = yg^n$. Alors

$$z^p = (yg^n)^p = yg^nyg^n \dots yg^n;$$

une simple récurrence assure que

$$z^p = y^p g^{n(r^{p-1}+r^{p-2}+\ldots+r+1)} = g^{pk+n(r^{p-1}+r^{p-2}+\ldots+r+1)}.$$

Par suite z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + r^{p-2} + \ldots + r + 1) \equiv 0 \mod p^2. \tag{1.17.1}$$

On cherche donc à résoudre (1.17.1) dont l'inconnue est $n \in \mathbb{Z}$. Posons $S := r^{p-1} + r^{p-2} + \ldots + r + 1$. Alors $(r-1)S \equiv r - 1 \bmod p$ donc

— soit $r \not\equiv 1 \bmod p$ et $S \equiv 1 \bmod p$;

— soit $r \equiv 1 \bmod p$ et on vérifie que dans ce cas $S \equiv p \bmod p^2$ (utiliser que p est impair).

Dans les deux cas l'équation (1.17.1) admet une solution $n_0 \in \mathbb{Z}$. Ainsi $z_0 = yg^{n_0} \in \mathrm{G} \smallsetminus \langle g \rangle$ est d'ordre p. Les deux sous-groupes $\mathrm{N} = \langle g \rangle$ et $\mathrm{H} = \langle z \rangle$ satisfont les hypothèses de l'Exercice **??** ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^2\mathbb{Z}$.

1.18. Groupes libres

Exercice 654

Soient r et s deux entiers > 1 premiers entre eux. Quel est l'ordre du groupe de présentation $\langle a \,|\, a^r,\, a^s \rangle$?

Éléments de réponse 654

L'ordre de a est un diviseur de r et s qui sont premiers entre eux donc a est d'ordre 1. Puisque G est engendré par a, le groupe G est d'ordre 1. Ainsi $\mathrm{G} = \{e_\mathrm{G}\}$.

Exercice 655

Soit G le groupe de présentation

$$\langle a,\, b,\, c \,|\, a^3 = b^3 = c^4 = e_\mathrm{G},\, ac = ca^{-1},\, aba^{-1} = bcb^{-1} \rangle.$$

Montrer que $ab^3a^{-1} = bc^3b^{-1}$ puis que $c = e_\mathrm{G}$; en déduire G.

Éléments de réponse 655

Nous avons

$$\begin{aligned} ab^3a^{-1} &= ab(a^{-1}a)b(a^{-1}a)ba^{-1} \\ &= (aba^{-1})(aba^{-1})(aba^{-1}) \\ &= (bcb^{-1})(bcb^{-1})(bcb^{-1}) \\ &= bc(b^{-1}b)c(b^{-1}b)cb^{-1} \\ &= bc^3b^{-1} \end{aligned}$$

Puisque $b^3 = e$, nous avons $ab^3a^{-1} = aa^{-1} = e_\mathrm{G}$. Comme $bc^3b^{-1} = ab^3a^{-1}$ nous obtenons que $bc^3b^{-1} = e_\mathrm{G}$ et que $c^3 = e_\mathrm{G}$. Par suite $c = c^4(c^3)^{-1} = e_\mathrm{G}(e_\mathrm{G})^{-1} = e_\mathrm{G}$.

Puisque $c = e$, la relation $ac = ca^{-1}$ devient $a = a^{-1}$ ou encore $a^2 = e$. Comme $a^3 = e$ nous obtenons $a = e$.

Enfin puisque $a = c = e_{\mathrm{G}}$ la relation $aba^{-1} = bcb^{-1}$ se réduit à $b = e_{\mathrm{G}}$. Comme a, b et c engendrent G nous obtenons $\mathrm{G} = \{e_{\mathrm{G}}\}$.

Exercice 656

Montrer que tout élément non trivial d'un groupe libre est d'ordre infini.

Éléments de réponse 656

Soit G un groupe libre. Soit g un élément non trivial de G. Raisonnons par l'absurde, *i.e.* supposons que g soit d'ordre fini n ; alors $g^n = e$. Or g^n est un mot formé avec les générateurs de G, la relation $g^n = e$ fournit donc une relation entre ces générateurs ce qui contredit le fait que G est un groupe libre.

Exercice 657

Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$x^3 = y^2 = (xy)^2 = 1\,?$$

Quels sont les sous-groupes de G ?

Éléments de réponse 657

Supposons que G ne soit pas trivial. Ceci implique que $x \neq y$ (en effet si $x = y$ alors $x^3 = 1$ se réécrirait $y^3 = 1$ et combiné à $y^2 = 1$ on obtiendrait $x = y = 1$.

L'ordre de x est 3 ; celui de y est 2. Il en résulte que $|\mathrm{G}|$ est un multiple de $2 \times 3 = 6$. Le groupe G contient e, x, x^2, y, xy et xy^2. Montrons qu'il n'y a pas d'autres éléments dans G. Commençons à écrire la table de G en utilisant ces six éléments

	e	x	x^2	y	xy	x^2y
e	e	x	x^2	y	xy	x^2y
x	x	x^2	e	xy	x^2y	y
x^2	x^2	e	x	x^2y	y	xy
y	y	x^2y	xy	e	x^2	x
xy	xy	y	x^2y	x	e	x^2
x^2y	x^2y	xy	y	x^2	x	e

Par suite cette table est complète et le groupe G compte 6 éléments.

Les sous-groupes de G sont

- ◇ le sous-groupe trivial,
- ◇ le groupe G lui-même,
- ◇ un unique (théorème de Sylow) sous-groupe d'ordre 3 : $\langle x \rangle$,

◇ trois sous-groupes d'ordre 2 exactement (théorème de Sylow) : $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$.

Exercice 658

Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$xy^2 = y^3x \qquad\qquad yx^3 = x^2y\,?$$

Éléments de réponse 658

À partir de $xy^2 = y^3x$ nous obtenons

$$y^2 = x^{-1}y^3x \qquad\qquad y^3 = xy^2x^{-1}$$

et

$$y^4 = x^{-1}y^6x \qquad\qquad y^6 = xy^4x^{-1}.$$

Par suite d'une part

$$y^9 = (y^3)^3 = (xy^2x^{-1})^3 = xy^6x^{-1}$$

et d'autre part

$$xy^6x^{-1} = x(y^6)x^{-1} = x(xy^4x^{-1})x^{-1} = x^2y^4x^{-2}.$$

On en déduit que $y^9 = x^2y^4x^{-2}$. De plus

$$y^9 = y^{-1}(y^9)y = y^{-1}(x^2y^4x^{-2})y = y^{-1}(x^2y)y^4(y^{-1}x^{-2})y = y^{-1}(x^2y)y^4(x^2y)^{-1}y$$

Mais $yx^3 = x^2y$ donc

$$y^9 = y^{-1}(x^2y)y^4(x^2y)^{-1}y = y^{-1}(yx^3)y^4(yx^3)^{-1}y = x^3y^4x^{-3}$$

Puisque $y^9 = x^2y^4x^{-2}$ nous obtenons

$$x^2y^4x^{-2} = x^3y^4x^{-3}$$

soit $y^4 = xy^4x^{-1}$. Mais on a vu précédemment que $y^6 = xy^4x^{-1}$ donc $y^4 = y^6$ soit $y^2 = e$. À partir de $xy^2 = y^3x$ on a $y^3 = e$ et finalement $y = e$. De plus $yx^3 = x^2y$ se réécrit $x^3 = x^2$ d'où $x = e$. Finalement G est le groupe trivial.

Exercice 659

Le groupe de FIBONNACCI [32] G est engendré par les éléments a, b, c et d vérifiant les relations

$$ab = c \qquad\qquad bc = d \qquad\qquad cd = a \qquad\qquad da = b.$$

Quel est l'ordre de G ?

Éléments de réponse 659

À partir de $a = cd$ nous obtenons

$$a^2 = acd = cda = cb = ab^2$$

32. Les groupes de FIBONNACCI ont été introduits par John CONWAY en 1965.

d'où $a = b^2$.

De même nous obtenons que $c^2 = b$, $d^2 = c$ et $a^2 = d$.

Par suite

$$d = a^2 = b^4 = c^8 = d^{16}$$

et $d^{15} = e$.

De la même façon nous obtenons que $a^{15} = b^{15} = c^{15} = e$.

A partir de $ab = c$ nous obtenons que $ab = a^4$ d'où $aa^8 = a^4$ et $a^5 = e$. De même $b^5 = c^5 = d^5 = e$. Par conséquent $d = a^2$, $b = a^3$, $c = a^4$ et $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$.

Exercice 660

Exprimer comme produit direct de sous-groupes monogènes le sous-groupe multiplicatif de $\mathbb{Q}^*$ engendré par $\{-6, 6\}$.

Éléments de réponse 660

Le sous-groupe $\mathrm{H} = \langle 6\rangle$ de $\mathrm{G} = \langle 6, -6\rangle \subset \mathbb{Q}^*$ est monogène.

Le groupe ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est monogène engendré par $(-6)\mathrm{H}$.

Le sous-groupe H est distingué dans G : il suffit de vérifier que $(-6) \times 6 \times (-6)^{-1}$ appartient à H ce qui est vrai puisque ce nombre vaut 6

Ainsi G est produit direct de deux groupes monogènes : $\mathrm{G} \simeq \mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Exercice 661

Montrer que le groupe multiplicatif engendré par les matrices

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

est abélien.

Exprimer ce groupe, de deux façons différentes, comme produit direct de sous-groupes monogènes.

Éléments de réponse 661

Soit G le groupe multiplicatif engendré par les matrices

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

On peut vérifier que $AB = BA = -2\mathrm{id}$;

le groupe G est donc abélien. Le sous-groupe $\mathrm{H} = \langle A\rangle$ de G est monogène.

Le groupe ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est monogène engendré par $B\mathrm{H}$.

Notons que $BAB^{-1} = A$; en particulier BAB^{-1} appartient à H et H est un sous-groupe distingué de G.

Il en résulte que G est isomorphe au produit direct des deux groupes monogènes H et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Exercice 662 [Présentation de $\mathfrak{S}_n$]

Montrer que

$$\mathfrak{S}_n = \langle t_1,\, t_2,\, \ldots,\, t_{n-1} \,|\, t_i^2 = 1,\, (t_i t_{i+1})^3 = 1,\, [t_i, t_j] = 1 \text{ pour } 2 \leq |i-j| \rangle$$

(Indication : le groupe $\mathfrak{S}_n$ est engendré par (1 2), (2 3), ..., $(n-1\ n)$).

Éléments de réponse 662

Pour $1 \leq i \leq n-1$ posons $t_i = (i\ i+1)$. Le groupe $\mathfrak{S}_n$ est engendré par ces transpositions. Cet ensemble de transpositions vérifie les relations données car une transposition est d'ordre 2, deux transpositions disjointes commutent (et pour les transpositions considérées t_i et t_j sont disjointes si et seulement si $|i-j| > 1$), le produit $t_i t_{i+1}$ est égal au 3-cycles $(i\ i+1\ i+2)$ et est donc d'ordre 3. Par suite

$$\mathfrak{S}_n = \langle t_1,\, t_2,\, \ldots,\, t_{n-1} \,|\, t_i^2 = \mathrm{id},\, (t_i t_{i+1})^3 = \mathrm{id},\, [t_i, t_j] = \mathrm{id} \text{ pour } |i-j| > 1 \rangle$$

En effet soit H le sous-groupe de $\mathfrak{S}_n$ engendré par les t_i. Le groupe H est distingué dans $\mathfrak{S}_n$ car

$$\sigma t_i \sigma^{-1} = (\sigma(i)\ \sigma(i+1))$$

et toute transposition est dans H : si $|i-k| > 1$,

$$(i\ k) = (k-1\ k)(i\ k)(k-1\ k).$$

Ainsi H contient $\mathcal{A}_n$ car tout sous-groupe distingué non trivial de $\mathfrak{S}_n$ contient $\mathcal{A}_n$.

Mais H contient strictement $\mathcal{A}_n$ car les transpositions ne sont pas des permutations paires. L'indice de $\mathcal{A}_n$ dans $\mathfrak{S}_n$ étant 2 nous obtenons que l'indice de H dans $\mathfrak{S}_n$ est 1. Il s'ensuit que $\mathfrak{S}_n = \mathrm{H}$.

Exercice 663

Rappelons que le groupe des quaternions $\mathbb{H}_8$ est le sous-groupe du groupe des matrices 2×2 inversibles à coefficients complexes engendré par

$$A = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$$

Montrer que ce groupe admet les deux présentations suivantes

$$\langle A,\, B \,|\, A^2 = B^2 = (AB)^2 \rangle \qquad \langle R,\, S,\, T \,|\, R^2 = S^2 = T^2 = RST \rangle.$$

Éléments de réponse 663

On peut vérifier que $A^2 = B^2 = (AB)^2 = -\mathrm{id}$ d'où la première présentation pour $\mathbb{H}_8$ (en effet un groupe qui a cette présentation est d'ordre 8).

Posons $R = A$, $S = B$ et $T = AB$; alors $R^2 = S^2 = -\mathrm{id}$ d'après ce qu'on vient de voir. Par ailleurs $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ donc $T^2 = -\mathrm{id}$. Et $RST = ABAB = (AB)^2 = -\mathrm{id}$ d'où la deuxième présentation proposée.

Exercice 664 [Présentation de $\mathcal{A}_4$]

1. Soient $a = (2\ 3\ 4)$ et $b = (1\ 2)(3\ 4)$ deux éléments de $\mathcal{A}_4$. Montrer que
$$\langle a,\, b \,|\, a^3 = b^2 = (ab)^3 = e \rangle$$
est une présentation de $\mathcal{A}_4$.
2. Donner une seconde présentation de $\mathcal{A}_4$ en utilisant les deux 3-cycles $(2\ 3\ 4)$ et $(1\ 3\ 2)$.

Éléments de réponse 664

1. Rappelons que $\mathcal{A}_4$ est d'ordre 12. Le groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^2 = (ab)^3 = e \rangle$$
est d'ordre 12 ; en effet ses éléments sont
$$e,\ a,\ a^2,\ b,\ ab,\ a^2b,\ ba,\ ba^2,\ aba,\ a^2ba,\ aba^2,\ a^2ba^2.$$
Le morphisme φ de G dans $\mathcal{A}_4$ défini par
$$\varphi(a) = (1\ 2\ 3) \qquad\qquad \varphi(b) = (1\ 2)(3\ 4)$$
réalise un isomorphisme entre G et $\mathcal{A}_4$.
2. Posons $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2)$; alors $\alpha\beta = (1\ 4\ 2)$ et
$$\alpha^3 = \mathrm{id} \qquad\qquad \beta^3 = \mathrm{id} \qquad\qquad (\alpha\beta)^3 = \mathrm{id}$$
On peut vérifier que le groupe G de présentation
$$\langle \alpha,\, \beta,\, | \, \alpha^3 = \beta^3 = (\alpha\beta)^3 = e \rangle$$
est d'ordre 12. On en déduit que G et $\mathcal{A}_4$ sont isomorphes.

Exercice 665 [Présentation de $\mathfrak{S}_4$]
Nous allons montrer que le groupe $\mathfrak{S}_4$ est isomorphe au groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^4 = (ab)^2 = e \rangle.$$
1. En utilisant les éléments $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2\ 4)$ de $\mathfrak{S}_4$ montrer qu'il existe un morphisme de G sur $\mathfrak{S}_4$. Désignons par H le sous-groupe de G engendré par a et b^2.
2. Montrer que bab^{-1} est un élément de H ; en déduire que H est un sous-groupe distingué de G.
3. Montrer que G/H a au plus deux éléments : les classes H et bH.
4. Montrer que $(ab^2)^3 = e$.
5. Conclure en utilisant la présentation de $\mathcal{A}_4$ obtenue précédemment.

Éléments de réponse 665

1. Remarquons que les permutations α et β considérées vérifient les relations
$$\alpha^3 = \mathrm{id}, \qquad \beta^4 = \mathrm{id}, \qquad (\alpha\beta)^2 = \mathrm{id}.$$
Il existe donc un morphisme φ de G sur $\mathfrak{S}_4$ qui envoie a sur α et b sur β. C'est de plus un morphisme injectif.
2. Nous avons
$$bab^{-1} = bab^3 = (bab)b^2, \qquad bab = a^{-1} = a^2.$$
Donc $bab^{-1} = a^2b^2$ appartient à H. Puisque G est engendré par a et b, cette relation implique que H est distingué dans G.
3. Puisque G est engendré par a et b, G/H est engendré par aH et bH, donc par bH car aH = H. Or b^2H = H donc G/H contient au plus les deux éléments H et bH.
4. Nous avons $abba = b^3a^2a^2b^3 = b^3ab^3$ car $ab = b^{-1}a^{-1} = b^3a^2$ et $ba = a^{-1}b^{-1} = a^2b^3$. Il en résulte que
$$(ab^2)^3 = abbabbabb = b^3ab^3b^2ab^2 = b^3abab^2 = b^3(abab)b = b^4 = e.$$
5. Le sous-groupe H de G a pour présentation
$$\langle a,\, c \,|\, a^3 = c^2 = (ac)^3 \rangle$$
(poser $c = b^2$). Les groupes H et $\mathcal{A}_4$ ont même présentation et $\varphi(\mathrm{H}) \subset \mathcal{A}_4$ donc $\varphi(\mathrm{H}) = \mathcal{A}_4$; en particulier H et $\mathcal{A}_4$ sont isomorphes. Le sous-groupe H est d'indice 2 dans G et $\mathcal{A}_4$ est d'indice 2 dans $\mathfrak{S}_4$. Ainsi $|\mathrm{G}| = |\mathfrak{S}_4|$. Finalement φ est un morphisme injectif de G dans $\mathfrak{S}_4$ et $|\mathrm{G}| = |\mathfrak{S}_4|$ donc φ réalise un isomorphisme entre G et $\mathfrak{S}_4$.

Exercice 666 [Présentation d'un produit semi-direct de groupes cycliques]

Notation : $[a]_m$ désigne un élément de $\mathbb{Z}/m\mathbb{Z}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq m-1$. De même $[a]_n$ désigne un élément de $\mathbb{Z}/n\mathbb{Z}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq n-1$.

Soient m, n des entiers ≥ 2 et
$$\tau \colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$$
un morphisme. Désignons par G le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\tau \mathbb{Z}/m\mathbb{Z}$ défini par τ.

Posons
$$[i]_n = \tau([1]_m)([1]_n) \qquad h = ([1]_n, [0]_m) \qquad k = ([0]_n, [1]_m).$$
Vérifions que
$$i^m \equiv 1 (\mathrm{mod\ n}) \qquad h^n = k^m = ([0]_n, [0]_m) \qquad khk^{-1} = h^i.$$
En déduire que G admet pour présentation
$$\langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i \rangle.$$

Éléments de réponse 666

Un morphisme $\tau\colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est entièrement déterminé par l'image $\tau([1]_m)$ de $[1]_m$ dans $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Cette image est elle-même déterminée par l'image de $[1]_n$ par $\tau([1]_m)$. Par suite un morphisme $\tau\colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est entièrement déterminé par $[i]_n = \tau([1]_m)([1]_n)$. Comme $[1]_m$ est d'ordre m, on a $\tau([1]_m)^m = \mathrm{id}$. Ainsi $i^m \equiv 1 \pmod{n}$.

Clairement $h^n = k^m = ([0]_n, [0]_m)$. L'inverse de k dans G est $k^{-1} = ([0]_n, [m-1]_m)$. Il en résulte que

$$\begin{aligned} hk^{-1} &= ([1]_n, [0]_m)([0]_n, [m-1]_m) \\ &= ([1]_n + \tau([0]_m)([0]_n), [m-1]_m) \\ &= ([1]_n, [m-1]_m) \end{aligned}$$

et donc que

$$\begin{aligned} khk^{-1} &= ([0]_n, [1]_m)([1]_n, [m-1]_m) \\ &= ([0]_n + \tau([1]_m)([1]_n), [0]_m) \\ &= ([i]_n, [0]_m) \end{aligned}$$

En particulier $khk^{-1} = h^i$.

Le groupe G est engendré par $a = h$ et $b = k^{-1}$ qui vérifient $a^n = b^b a^i$. Une présentation de G est la suivante

$$\mathrm{G} = \langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i \rangle.$$

1.19. Représentations linéaires des groupes finis

Exercice 667

Montrer que tout groupe fini G admet une représentation fidèle sur tout corps $\Bbbk$.

Éléments de réponse 667

Première réponse possible : la représentation régulière de G sur $\Bbbk$ répond à la question.

Deuxième réponse possible : le théorème de Cauchy assure que G se plonge dans le groupe des permutations de G et ce dernier groupe se plonge dans un groupe linéaire via les matrices de permutations.

Exercice 668

Montrer que si G est un groupe d'ordre fini n, si ρ est une représentation de G sur $\mathbb{C}$, alors pour tout g dans G $\rho(g)$ est diagonalisable et son spectre est inclus dans μ_n.

Éléments de réponse 668

Soit G un groupe d'ordre fini n. Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie, une représentation de G.

Soit g un élément de G. L'ordre de g divise n ; en particulier g est d'ordre fini. L'automorphisme $\rho(g)$ est d'ordre fini puisque g l'est, *i.e.* il existe un entier k tel que $\rho(g)^k = \mathrm{Id}_V$. Alors :

$$X^k - 1 = \prod_{j=0}^{k-1} (X - \zeta^j) \in \mathbb{C}[X]$$

où ζ est une racine primitive $k$ième de l'unité, est un polynôme annulateur de $\rho(g)$ scindé à facteurs simples ; $\rho(g)$ est donc diagonalisable et ses valeurs propres sont les racines $k$ième de l'unité.

Exercice 669

Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrer que $\rho \circ \pi$ est une représentation de G.

b) Montrer que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

Éléments de réponse 669

Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrons que $\rho \circ \pi$ est une représentation de G.

La composée de deux morphismes de groupes étant un morphisme de groupes, $\rho \circ \pi$ est une représentation de G.

b) Montrons que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

- Commençons par montrer que si $\rho \circ \pi$ est irréductible alors ρ l'est.

  Plus généralement si $f\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes et si ρ est une représentation de G′, on a l'implication suivante

  si $\rho \circ f$ est irréductible (comme représentation) de G, alors ρ est irréductible.

  En effet tout sous-espace stable par G′ est stable par G puisque l'action de G se factorise par G′.

- Montrons que si ρ est irréductible, alors $\rho \circ \pi$ est irréductible.

  Soit W un sous-espace strict stable par G. Pour tout $\overline{x} \in {}^{\mathrm{G}}\!/_{\mathrm{H}}$ il existe $g \in \mathrm{G}$ tel que $\pi(g) = \overline{x}$ (ρ est surjective, si elle ne l'était pas l'implication serait fausse). Comme W est stable par g, il est stable par $\overline{x}$. Ainsi W est stable par tout élément de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. La représentation ρ étant irréductible $W = 0$ et $\rho \circ \pi$ est irréductible.

Exercice 670

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}(n, \mathbb{C})$ est le groupe des homothéties. Soit ρ l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$.

a) Montrer que la représentation ρ est irréductible.

b) Montrer que tout élément du centre de $\mathrm{GL}(n, \mathbb{C})$ est un morphisme de la représentation ρ.

c) Conclure en utilisant le Lemme de Schur.

Éléments de réponse 670

Puisque ρ est l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}(n, \mathbb{C})$ dans $\mathrm{GL}(n, \mathbb{C})$.

a) Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}(n, \mathbb{C})$, alors il est évident que $V = \{0\}$ ou $V = \mathbb{C}^n$, c'est-à-dire que ρ est irréductible.

b) Soit h un élément du centre de $\mathrm{GL}(n, \mathbb{C})$. Donc pour tout $M \in \mathrm{GL}(n, \mathbb{C})$ on a $\rho(M) \circ h = Mh = hM = h \circ \rho(M)$, donc h est bien un morphisme de la représentation ρ.

c) Comme ρ est irréductible, d'après le Lemme de Schur, on a $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, c'est-à-dire que h est une homothétie.

Exercice 671

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Soit G un groupe abélien.

a) Si $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ est une représentation de G, montrer que tout élément g de G définit un G-morphisme $V \to V$.

b) En déduire que toute représentation irréductible de G est de dimension 1.

c) Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 671

Comme souvent on note $g \cdot x$ pour $\rho(g)(x)$.

a) Pour tous g, h, $x \in \mathrm{G}$, nous avons

$$g \cdot (h \cdot x) = (gh) \cdot x = (hg) \cdot x = h \cdot (g \cdot x)$$

c'est-à-dire l'application $\rho(g)\colon x \mapsto g \cdot x$ est un G-morphisme pour tout $g \in \mathrm{G}$.

b) On suppose que V est une représentation irréductible de G. Si $g \in \mathrm{G}$, alors d'après la question précédente et le Lemme de Schur, $\rho(g) = \lambda \mathrm{id}$. De plus, comme $\rho(g) \in \mathrm{GL}(V)$, on a $\lambda \neq 0$. Donc tout sous-espace vectoriel de V est stable par G, et est donc une sous-représentation de G. Comme V est irréductible, on a nécessairement $\dim(V) = 1$.

c) D'après la question précédente, une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes $\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*$. Comme tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n, l'élément $\rho(k)$ sera aussi d'ordre divisant n, c'est-à-dire $\rho(k)^n = 1$. Réciproquement, pour toute racine $n$ème de l'unité ω, l'application

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$

est une représentation de $\mathbb{Z}/n\mathbb{Z}$, donc on les obtient toutes ainsi. On voit ainsi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 672

Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V,ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrer que (V,ρ) est isomorphe à la représentation régulière de G.

Éléments de réponse 672

Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V,ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrons que (V,ρ) est isomorphe à la représentation régulière de G.

Soit W un espace vectoriel de base $\{e_j\}_{g\in\mathrm{G}}$; prendre par exemple $W = \mathbb{C}^G$ et $e_g =$ indicatrice de g. Rappelons que la représentation régulière ρ_R de G opère sur W par

$$\rho_R(h)(e_g) = e_{hg}$$

Considérons l'application linéaire ϕ définie sur la base (e_g) oar

$$\phi\colon W \to V, \qquad e_g \mapsto \rho(g)v$$

Puisque par hypothèse $(\rho(g)(v))_{g\in\mathrm{G}}$ est une base de V ϕ est un isomorphisme de $\mathbb{C}$-espaces vectoriels. Par définition ϕ est G-équivariante, *i.e.* $\phi \circ \rho_R(g) = \rho(g) \circ \phi$. En effet d'une part

$$(\phi \circ \rho_R(g))(e_h) = \phi(e_{gh}) = \rho(gh)(v)$$

et d'autre part

$$(\rho(g) \circ \phi)(e_h) = \rho(g)(\phi(e_h)) = \rho(g)(\rho(h)(v)) = \rho(gh)(v)$$

Ainsi ϕ est un isomorphisme entre ρ et ρ_R.

Exercice 673

Soit $\mathrm{G} = \mathfrak{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrer que T est une représentation de G.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad\qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrer que W est une sous-G-représentation de V. W est-il irréductible ?

c) Déterminer la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Éléments de réponse 673

Soit $\mathrm{G} = \mathfrak{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrons que T est une représentation de G.

T est un morphisme de G dans $\mathrm{GL}(V)$: soient g et g' dans G on a d'une part

$$T(gg')(e_\tau) = e_{(gg')\tau(gg')^{-1}} = e_{gg'\tau g'^{-1}g^{-1}}$$

et d'autre part

$$T(g) \circ T(g')(e_\tau) = T(g)(e_{g'\tau g'^{-1}}) = e_{gg'\tau g'^{-1}g^{-1}}$$

d'où $T(gg') = T(g) \circ T(g')$.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad\qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrons que W est une sous-G-représentation de V.

Le groupe $\mathfrak{S}_3$ est engendré par (1 2) et (1 2 3). Il suffit donc de montrer que l'espace engendré par α et β est stable par $T((1\ 2))$ et $T((1\ 2\ 3))$. Un calcul montre que

$$T((1\ 2))(\alpha) = \beta, \qquad T((1\ 2\ 3))(\alpha) = j\alpha, \qquad T((1\ 2))(\beta) = \alpha, \qquad T((1\ 2\ 3))(\beta) = j^2\beta$$

W est-il irréductible ?

Un calcul montre qu'aucun sous-module de W de dimension 1 n'est stable par $\mathfrak{S}_3$ donc W est irréductible.

c) Déterminons la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Remarquons que si C est une classe de conjugaison dans $\mathfrak{S}_3$, alors $\sum_{g\in C} e_g$ est stable par T (c'est par définition même de T). On trouve ainsi trois sous-espaces stables sous $\mathfrak{S}_3$ qui sont les droites

$$W_1 = \mathbb{C}\mathrm{id}, \qquad W_2 = \mathbb{C}(e_{(1\ 2)} + e_{(1\ 3)} + e_{(2\ 3)}), \qquad W_3 = \mathbb{C}(e_{(1\ 2\ 3)} + e_{(1\ 3\ 2)})$$

Enfin si on note sgn la signature on obtient

$$T(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) = \mathrm{sgn}(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$$

En effet d'une part

$$\begin{aligned} T((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2)(1\ 2\ 3)(1\ 2)} - e_{(1\ 2)(1\ 3\ 2)(1\ 2)} \\ &= e_{(1\ 3\ 2)} - e_{(1\ 2\ 3)} \\ &= -(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

d'autre part

$$\begin{aligned} T((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3)^{-1}} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)^{-1}} \\ &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 3\ 2)} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 3\ 2)} \\ &= (e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

L'espace $W_4 = \mathbb{C}(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$ est donc stable par $\mathfrak{S}_3$.

On a finalement $V = W_1 \oplus W_2 \oplus W_3 \oplus W_4 \oplus W$ où W désigne l'unique représentation irréductible de dimension 2.

Exercice 674

Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrer que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Éléments de réponse 674

Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrons que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Le groupe G admet un sous-groupe distingué H d'indice p. Par conséquent ${}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Le corps $\Bbbk$ est algébriquement clos de caractéristique $\neq p$. Par suite le polynôme $X^p - 1$ est scindé à racines simples. Ainsi les racines p-ième de l'unité dans $\Bbbk^*$ forment un sous-groupe cyclique d'ordre p isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ d'où une injection de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\Bbbk^*$. Le morphisme

$$\mathrm{G} \longrightarrow {}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \longrightarrow \Bbbk^*$$

est donc une représentation non triviale de dimension 1 de G sur $\Bbbk$.

Exercice 675

Soit G un groupe fini et soit χ le caractère d'une représentation ρ de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrer que χ est un multiple entier du caractère de la représentation régulière de G.

Éléments de réponse 675

Soit G un groupe fini et soit χ le caractère d'une représentation ρ de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrons que χ est un multiple entier du caractère de la représentation régulière de G.

Rappel : le caractère de la représentation régulière est donné par

$$\chi_{\rho_R}(g) = \begin{cases} |\mathrm{G}| \text{ si } g = e \\ 0 \text{ sinon} \end{cases}$$

Il suffit de montrer que $|\mathrm{G}|$ divise $\chi(e)$. Notons χ_{triv} le caractère de la représentation triviale de G. On a

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi(g) \overline{\chi_{\mathrm{triv}}(g)}$$

Comme $\chi(g) = 0$ pour tout $g \neq e$ on a $\displaystyle\sum_{g \in \mathrm{G}} \chi(g)\overline{\chi_{\mathrm{triv}}(g)} = \chi(e)\overline{\chi_{\mathrm{triv}}(e)} = \chi(e)$ autrement dit

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|}\chi(e)$$

et

$$|\mathrm{G}|\langle \chi, \chi_{\mathrm{triv}} \rangle = \chi(e).$$

Remarquons

- ◇ d'une part que $\chi(e)$ est un entier : pour toute représentation ρ nous avons $\chi_\rho(e) = \mathrm{tr}(\rho(e)) = \mathrm{tr}(\mathrm{id}_{\mathrm{GL}(V)}) = \dim V$;
- ◇ d'autre part que $\langle \chi, \chi_{\mathrm{triv}} \rangle$ est un entier : la représentation ρ s'écrit $\rho = \oplus \rho_i^{n_i}$ où les ρ_i désignent les représentations irréductibles de G et les n_i des entiers naturels uniquement déterminés par ρ. Quitte à réindicer les ρ_i on peut supposer $\rho_1 = \rho_{\mathrm{triv}}$, *i.e.* $\rho = \rho_{\mathrm{triv}}^{n_1} \oplus \Big(\bigoplus_i \rho_i^{n_i}\Big)$. Ainsi $\langle \chi, \chi_{\mathrm{triv}} \rangle = n_1 \in \mathbb{N}$.

Il en résulte que χ est un multiple entier du caractère de la représentation régulière de G.

Exercice 676

Décrire les représentations irréductibles du groupe $\mathrm{GL}(3, \mathbb{F}_2)$ et écrire sa table de caractères.

Éléments de réponse 676

Exercice 677

a) Décrire les représentations irréductibles du groupe diédral D_{2n} et écrire sa table de caractères.

b) Déterminer les sous-groupes distingués de D_8 à l'aide de sa table de caractères.

Éléments de réponse 677

Exercice 678

Soit $\mathbb{H}_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions. Ecrire la table de caractères de $\mathbb{H}_8$ et décrire les représentations irréductibles.

Indication : On rappelle que $\mathbb{H}_8$ s'identifie à un sous-groupe de $\mathrm{SU}(2,\mathbb{C})$ en posant : $I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ et $K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Éléments de réponse 678

On peut vérifier que $\mathbb{H}_8$ admet cinq classes de conjugaison qui sont

$$\{1\}, \quad \{-1\}, \quad \{\pm i\}, \quad \{\pm j\}, \quad \{\pm k\}$$

Le groupe dérivé $D(\mathbb{H}_8)$ de $\mathbb{H}_8$ est donné par : $D(\mathbb{H}_8) = \{\pm 1\}$. Par conséquent a

$$\mathbb{H}_8/D(\mathbb{H}_8) = \langle \bar{i}, \bar{j} \,|\, \bar{i}^2 = \bar{j}^2 = 1, \bar{i}\bar{j} = \bar{j}\bar{i} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ainsi $\mathbb{H}_8$ admet quatre représentations de dimension 1 correspondant aux quatre morphismes de groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^*$. Il s'en suit que la cinquième représentation irréductible de $\mathbb{H}_8$ est de dimension 2. Son caractère se déduit des caractères praécédents par orthogonalité.

La table des caractères de $\mathbb{H}_8$ est

$\mathbb{H}_8$	1	1	2	2	2
	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_3 = \chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

Notons que les tables de $\mathbb{H}_8$ et D_8 sont les mêmes. La table de caractères ne détermine donc pas la classe d'isomorphisme d'un groupe fini.

Exercice 679

Décrire les représentations irréductibles du groupe symétrique $\mathfrak{S}_3$ et écrire sa table de caractères.

Éléments de réponse 679

Les classes de conjugaison de $\mathfrak{S}_3$ sont (Proposition **??**)

$$C_1 = \{\mathrm{id}\}, \qquad C_2 = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}, \qquad C_3 = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Ainsi $\mathfrak{S}_3$ a trois représentations irréductibles à équivalence près. Il y a la représentation triviale ρ_{triv} qui est irréductible. On a aussi la représentation signature

$$\mathrm{sgn}\colon \mathfrak{S}_3 \to \mathrm{GL}(1,\mathbb{C}) \simeq \mathbb{C}^*, \qquad \sigma \mapsto \mathrm{sgn}(\sigma)$$

qui est de degré 1 ; elle est irréductible car

$$\langle \chi_{\mathrm{sgn}}, \chi_{\mathrm{sgn}} \rangle = \frac{1}{6}\Big(\underbrace{1}_{\#C_1} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((\mathrm{id}))} \times \overline{1} + \underbrace{3}_{\#C_2} \times \underbrace{(-1)}_{\chi_{\mathrm{sgn}}((1\ 2))} \times \overline{(-1)} + \underbrace{2}_{\#C_3} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((1\ 2\ 3))} \times \overline{1} \Big) = 1$$

Enfin on a la représentation décrite dans l'Exemple **??** dite représentation standard et notée ρ_S. Notons que

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = 1^2 + 1^2 + 2^2 = 6$$

autrement dit $(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = |\mathfrak{S}_3|$.

Ainsi la table de caractères de $\mathfrak{S}_3$ est

	C_1	C_2	C_3
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1
sgn	1	-1	1
χ_{ρ_S}	2	0	-1

A noter que les colonnes sont bien orthogonales.

Exercice 680 [Table de caractères du groupe symétrique $\mathfrak{S}_4$]

a) Décrire les représentations irréductibles de $\mathfrak{S}_4$ et dresser sa table des caractères.

b) Déterminer les sous-groupes distingués de $\mathfrak{S}_4$ à partir de sa table des caractères.

c) On rappelle que $\mathfrak{S}_4$ s'identifie au groupe des isométries directes d'un cube (ou d'un octaèdre) et également au groupe des isométries (directes et indirectes) d'un tétraèdre. Que pensez-vous des représentations de dimension 3 associées ?

Éléments de réponse 680

Le groupe symétrique $\mathfrak{S}_4$ possède cinq classes de conjugaison (Proposition **??**) :

$$\begin{aligned}
C_1 &= \{\mathrm{id}\},\\
C_2 &= \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\},\\
C_3 &= \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},\\
C_4 &= \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\},\\
C_5 &= \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}.
\end{aligned}$$

Il y a donc cinq représetntations irréductibles à équivalence près. On peut déjà donner deux représentations de degré 1

- ◇ la représentation triviale ρ_{triv} ;
- ◇ la représentation signature sgn.

Intéressons-nous à la représentation par permutations. Notons $\mathcal{B} = (e_1, e_2, e_3, e_4)$ la base canonique de $\mathbb{C}^4$. On définit la représentation par permutations par

$$\rho_P \colon \mathfrak{S}_4 \to \mathrm{GL}(\mathbb{C}^4) \qquad\qquad \sigma \mapsto (e_i \mapsto e_{\sigma(i)}).$$

Cette représentation laisse stable $\mathrm{Vect}(1,1,1,1)$ dont

$$H = \{x = (x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$$

est un supplémentaitre stable. Elle induit une représentation ρ_S appelée représentation standard sur H. Comme ρ_P induit la représentation triviale sur $\mathrm{Vect}(1,1,1,1)$ nous avons la relation $\chi_{\rho_P} = \chi_{\rho_{\mathrm{triv}}} + \chi_{\rho_S}$. Reste à savoir si χ_{ρ_S} est irréductible, *i.e.* si $\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle = 1$. Mais $\chi_{\rho_P}(\sigma)$ est le nombre de 1 sur la diagonale de la matrice de permutations σ, c'est-à-dire le nombre de points fixes de σ (Exemple **??**). Ainsi

$$\chi_{\rho_P}(\mathrm{id}) = 4, \quad \chi_{\rho_P}((1\ 2)) = 2, \quad \chi_{\rho_P}((1\ 2)(3\ 4)) = 0, \quad \chi_{\rho_P}((1\ 2\ 3)) = 1, \quad \chi_{\rho_P}((1\ 2\ 3\ 4)) = 0$$

(en effet $\mathrm{Fix}(\mathrm{id}) = \{1, 2, 3, 4\}$, $\mathrm{Fix}((1\ 2)) = \{3, 4\}$, $\mathrm{Fix}((1\ 2)(3\ 4)) = \emptyset$, $\mathrm{Fix}((1\ 2\ 3)) = \{4\}$ et $\mathrm{Fix}((1\ 2\ 3\ 4)) = \emptyset$) d'où (puisque $\chi_{\rho_S}(g) = \chi_{\rho_P}(g) - \chi_{\rho_{\mathrm{triv}}}(g) = \chi_{\rho_P}(g) - 1$)

$$\chi_{\rho_S}(\mathrm{id}) = 3, \quad \chi_{\rho_S}((1\ 2)) = 1, \quad \chi_{\rho_S}((1\ 2)(3\ 4)) = -1, \quad \chi_{\rho_S}((1\ 2\ 3)) = 0, \quad \chi_{\rho_S}((1\ 2\ 3\ 4)) = -1.$$

Il en résulte que

$$\begin{aligned}
\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle &= \frac{1}{|\mathfrak{S}_4|}\Big(1 \times 3 \times \overline{3} + 6 \times 1 \times \overline{1} + 3 \times (-1) \times \overline{(-1)} + 8 \times 0 \times \overline{0} + 6 \times (-1) \times \overline{(-1)}\Big)\\
&= \frac{1}{24}(9 + 6 + 3 + 6)
\end{aligned}$$

Nous en déduisons que ρ_S est une représentation irréductible de degré 3. Nous la notons ρ_4.

Déterminons les deux autres représentations irréductibles de $\mathcal{A}_4$ notées ρ_3 et ρ_5. Commençons par déterminer leurs degrés : l'identité

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_3^2)^2 + (\deg \rho_4^2)^2 + (\deg \rho_5^2)^2 = |\mathfrak{S}_4|$$

conduit à

$$24 - (\deg \rho_{\mathrm{triv}})^2 - (\deg \mathrm{sgn})^2 - (\deg \rho_4)^2 = (\deg \rho_3)^2 + (\deg \rho_5)^2$$

soit $13 = (\deg \rho_3)^2 + (\deg \rho_5)^2$. Nous en déduisons que $\{\deg \rho_3, \deg \rho_5\} = \{2, 3\}$.

Considérons la représentation

$$\rho_5 \colon \mathfrak{S}_4 \to \mathrm{GL}(H), \qquad \sigma \mapsto \mathrm{sgn}(\sigma)\rho_4(\sigma).$$

Alors $\chi_{\rho_5} = \mathrm{sgn}\chi_{\rho_4}$ d'où

$$\begin{aligned} &\chi_{\rho_S}(\mathrm{id}) = 1 \times 3 = 3, && \chi_{\rho_S}((1\ 2)) = (-1) \times 1 = -1,\\ &\chi_{\rho_S}((1\ 2)(3\ 4)) = 1 \times (-1) = -1, && \chi_{\rho_S}((1\ 2\ 3)) = 1 \times 0 = 0,\\ &\chi_{\rho_S}((1\ 2\ 3\ 4)) = (-1) \times (-1) = 1. \end{aligned}$$

En particulier

$$\langle \chi_{\rho_5}, \chi_{\rho_5} \rangle = \frac{1}{24}\Big(1{\times}3{\times}3{+}6{\times}(-1){\times}(-1){+}3{\times}(-1){\times}(-1){+}8{\times}0{\times}0{+}6{\times}1{\times}1\Big) = \frac{1}{24}\Big(9{+}6{+}3{+}6\Big) = 1.$$

Il s'ensuit que ρ_5 est irréductible. De plus $\deg \rho_5 = \dim H = 3$.

Remarque — On peut donner une interprétation géométrique de ρ_5 : c'est la représentation de $\mathfrak{S}_4$ comme $\mathrm{Isom}^+(C_6)$ (Proposition **??**).

Commençons à écrire la table de caractères de $\mathfrak{S}_4$:

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	?	?	?	?
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

où $C(g)$ désigne la classe de conjugaison de $g \in \mathfrak{S}_4$.

En utilisant que les colonnes de la table de $\mathfrak{S}_4$ sont orthogonales nous obtenons

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	0	2	-1	0
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

Rappelons que les sous-groupes distingués de $\mathfrak{S}_4$ sont les intersections $\bigcap_{i\in I}\ker\chi_{\rho_i}$ où $I\subset$ [triv, sgn, 3, 4, 5]. La table des caractères de $\mathfrak{S}_4$ assure que

$$\begin{aligned}
&\ker\chi_{\rho_{\text{triv}}}=\mathfrak{S}_4\\
&\ker\chi_{\rho_{\text{sgn}}}=\{\text{id},\,C((1\ 2)(3\ 4)),\,C(1\ 2\ 3)\}=\mathcal{A}_4\\
&\ker\chi_{\rho_3}=\{\text{id},\,C((1\ 2)(3\ 4))\}\simeq\mathcal{K}\\
&\ker\chi_{\rho_4}=\{\text{id}\}\\
&\ker\chi_{\rho_5}=\{\text{id}\}
\end{aligned}$$

Par suite les sous-groupes distingués de $\mathfrak{S}_4$ sont

$$\mathfrak{S}_4,\qquad \{\text{id}\},\qquad \mathcal{A}_4,\qquad \{\text{id},\,(1\ 2)(3\ 4),\,(1\ 3)(2\ 4),\,(1\ 4)(2\ 3)\}\simeq\mathcal{K}$$

(on rappelle que $\mathcal{K}$ désigne le groupe de Klein).

Explicitons ρ_3. Nous avons la décomposition en produit semi-direct

$$\mathfrak{S}_4\simeq\mathcal{K}\rtimes\mathfrak{S}_3.$$

À cette décomposition correspond un morphisme surjectif de groupes

$$\pi\colon\mathfrak{S}_4\to{}^{\mathfrak{S}_4}\!/_{\mathcal{K}}\simeq\mathfrak{S}_3$$

d'où par composition avec la représentation standard $\widetilde{\rho_S}$ de $\mathfrak{S}_3$ une représentation de degré 2

$$\rho_3\colon\mathfrak{S}_4\xrightarrow{\pi}\mathfrak{S}_3\xrightarrow{\widetilde{\rho_S}}\mathrm{GL}(\widetilde{H})$$

où $\widetilde{H}$ désigne l'hyperplan de $\mathbb{C}^3$ d'équation $x_1+x_2+x_3=0$, $\mathcal{B}=(e_1,e_2,e_3)$ la base canonique de $\mathbb{C}^3$ et $\widetilde{\rho_S}\colon\mathfrak{S}_3\to\mathrm{GL}(\widetilde{H})$ la représentation standard de $\mathfrak{S}_3$ induite par la représentation par permutation

$$\widetilde{\rho_P}\colon\mathfrak{S}_3\to\mathrm{GL}(\mathbb{C}^3),\qquad\qquad \sigma\mapsto(e_i\mapsto e_{\sigma(i)}).$$

Pour tout σ dans $\mathfrak{S}_4$ nous avons

$$\chi_{\rho_3}(\sigma)=\chi_{\widetilde{\rho_S}}(\pi(\sigma))$$

soit

$$\begin{aligned}
&\chi_{\rho_3}(\text{id})=2\\
&\chi_{\rho_3}((1\ 2))=0\\
&\chi_{\rho_3}((1\ 2)(3\ 4))=2\\
&\chi_{\rho_3}((1\ 2\ 3))=-1\\
&\chi_{\rho_3}((1\ 2\ 3\ 4))=\chi_{\rho_3}((1\ 4)(1\ 2\ 3))=0
\end{aligned}$$

De plus

$$\langle\chi_{\rho_3},\,\chi_{\rho_3}\rangle=\frac{1}{24}\Big(1\times2\times2+6\times0\times0+3\times2\times2+8\times(-1)\times(-1)+6\times0\times0\Big)=\frac{1}{24}\Big(4+12+8\Big)=1$$

autrement dit χ_{ρ_3} est irréductible.

Exercice 681

Déterminer, à isomorphisme près, le groupe dont la table des caractères est :

	e	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Éléments de réponse 681

Exercice 682

Décrire les représentations irréductibles du groupe $\mathcal{A}_4$ et écrire sa table de caractères.

Éléments de réponse 682

Nous allons établir la table des caractères de $\mathcal{A}_4$. Il y a plusieurs façons d'arriver au résultat. La manière la plus systématique consiste à déterminer les classes de conjugaison de $\mathcal{A}_4$, construire toutes les représentations irréductibles de $\mathcal{A}_4$ et calculer la valeur de leurs caractères sur les classes de conjugaison. C'est ce que nous allons faire avant de montrer que certains des résultats démontrés précédemment permettent quelques raccourcis.

a) Désignons par t le 3-cycle (1 2 3). Notons que $t^2 = (1\ 3\ 2)$ et que comme t est d'ordre 3, le sous-groupe $\mathrm{T} = \langle t \rangle = \{\mathrm{id}, t, t^2\}$ de $\mathcal{A}_4$ engendré par t est d'ordre 3.

b) Le sous-groupe $\mathrm{H} = \{\mathrm{id}, s_2, s_3, s_4\}$ de $\mathcal{A}_4$ est abélien et distingué dans $\mathcal{A}_4$. En effet un 2-Sylow de $\mathcal{A}_4$ est d'ordre 4 et comme H est d'ordre 4 et contient tous les éléments de $\mathcal{A}_4$ d'ordre divisant 4 cela montre qu'il n'y a qu'un seul 2-Sylow qui est par conséquent distingué dans $\mathcal{A}_4$ et que ce 2-Sylow est H.

De plus tous les éléments de H sont d'ordre divisant 2 donc H est abélien [33].

c) Tout élément de $\mathcal{A}_4$ peut s'écrire de manière unique sous la forme $t^\ell h$ avec $\ell \in \{0, 1, 2\}$ et $h \in \mathrm{H}$.

Considérons

$$\varphi\colon \mathrm{T} \times \mathrm{H} \to \mathcal{A}_4, \qquad (c, h) \mapsto ch.$$

33. En effet soit G un groupe dont tous les éléments sont d'ordre divisant 2 ; si g et h sont deux éléments de G, alors d'une part $(gh)^2 = e$ et d'autre part $g^2h^2 = e$ d'où $(gh)^2 = g^2h^2$ soit $ghgh = gghh$ et $gh = gh$.

C'est une injection de $\mathrm{T}\times\mathrm{H}$ dans $\mathcal{A}_4$. En effet soient (c_1,h_1) et (c_2,h_2) dans $\mathrm{T}\times\mathrm{H}$ tels que $c_1h_1=c_2h_2$. Alors $c_2^{-1}c_1=h_2h_1^{-1}$; en particulier puisque $c_2^{-1}c_1$ appartient à T et $h_2h_1^{-1}$ appartient à H, les éléments $c_2c_1^{-1}$ et $h_2h_1^{-1}$ appartiennent à $\mathrm{T}\cap\mathrm{H}$. Or $\mathrm{T}\cap\mathrm{H}=\{\mathrm{id}\}$ donc $(c_1,h_1)=(c_2,h_2)$. Remarquons que $|\mathrm{T}\times\mathrm{H}|=|\mathcal{A}_4|$; il en résulte que φ est une bijection ce qui permet de conclure.

d) On peut vérifier que les 3-cycles t et t^2 ne commutent à aucun élément de $\mathrm{H}\smallsetminus\{\mathrm{id}\}$ par un calcul direct.

e) Montrons que les classes de conjugaison de $\mathcal{A}_4$ sont

$$C_1=\{\mathrm{id}\},\qquad C_2=\mathrm{H}\smallsetminus\{\mathrm{id}\},\qquad C_3=t\mathrm{H},\qquad C_4=t^2\mathrm{H}.$$

Comme dans tout groupe la classe de conjugaison de l'élément neutre a un seul élément C_1 appartient à l'ensemble $\mathrm{conj}(\mathcal{A}_4)$ des classes de conjugaison de $\mathcal{A}_4$.

Si s appartient à C_2 et si t^ah, avec $a\in\{0,\,1,\,2\}$ et $h\in\mathrm{H}$, commute à s, alors $t^ahs=st^ah$ donc $t^ahsh=st^ah^2$. Comme H est abélien et $h^2=\mathrm{id}$ nous obtenons $t^as=st^a$ ce qui entraîne $a=0$. Le centralisateur de s est donc G et le cardinal de la classe de conjugaison de s est égal à $\frac{|\mathcal{A}_4|}{|\mathrm{H}|}=3$. Puisqu'un conjugué de s est d'ordre 2, cette classe de conjugaison est incluse dans C_2 et lui est égale pour des raisons de cardinal.

Enfin le centralisateur de t et t^2 est T ; en effet si $t^aht=tt^ah$ alors $ht=th$ et donc $h=\mathrm{id}$. Il s'ensuit que la classe de conjugaison de t est de cardinal $\frac{|\mathcal{A}_4|}{|\mathrm{T}|}=4$. Or

$$(t^ah)t(t^ah)^{-1}=t^ahth^{-1}t^{-a}=t(t^{a-1}ht^{1-a})(t^ah^{-1}t^{-a})\in t\mathrm{H}$$

car H est distingué dans $\mathcal{A}_4$. Donc $t^{a-1}ht^{1-a}$ et $t^ah^{-1}t^{-a}$ appartiennent à H. La classe de conjugaison de t est donc contenue dans C_3 et lui est égale pour des raisons de cardinalité. On obtient de la même façon que la classe de conjugaison de t^2 est C_4.

f) Soit $\zeta=\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ une racine primitive 3ième de l'unité. Rappelons que μ_n désigne l'ensemble des racines $n$ième de l'unité. Pour $0\leq j\leq 2$ on définit $\eta^j:\mathcal{A}_4\to\mu_3$ par $\eta^j(t^ah)=\zeta^{ja}$ si $0\leq a\leq 2$ et $h\in\mathrm{H}$. Alors $\eta^0=\mathrm{id}$, η et η^2 sont des caractères linéaires distincts de $\mathcal{A}_4$.

En effet si $0\leq a,\,b\leq 2$ et si h, g appartiennent à H, alors $t^aht^bg=t^{a+b}(t^{-b}ht^b)g$. Puisque H est distingué dans $\mathcal{A}_4$, on a $t^{-b}ht^b$ appartient à H et donc $(t^{-b}ht^b)g$ appartient à H. De plus $\eta^j(t^aht^bg)=\zeta^{j(a+b)}=\zeta^{ja}\zeta^{jb}=\eta^j(t^ah)\eta^j(t^bg)$.

g) Soit V la représentation de permutation associée à l'action naturelle de $\mathcal{A}_4$ sur $\{1,\,2,\,3,\,4\}$. Rappelons que cette représentation est $\mathbb{C}^4$ muni de l'action de $\mathcal{A}_4$ définie dans la base canonique $(e_1,\,e_2,\,e_3,\,e_4)$ par $g(e_i)=e_{g(i)}$. L'hyperplan W d'équation $x_1+x_2+x_3+x_4=0$ est stable par $\mathcal{A}_4$ et la représentation obtenue est irréductible de caractère :

$$\chi_W(\mathrm{id})=3,\qquad \chi_W(g)=-1\text{ si }g\in\mathrm{H}\smallsetminus\{\mathrm{id}\},\qquad \chi_W(g)=0\text{ si }g\notin\mathrm{H}.$$

En effet la représentation V se décompose sous la forme $V'\oplus W$ où V' est la droite engendrée par $e_1+e_2+e_3+e_4$. Puisque V est une repésentation de permutation $\chi_V(g)$

est le nombre de points fixes de g agissant sur $\{1, 2, 3, 4\}$. Nous avons donc

$$\chi_V(\mathrm{id}) = 4, \qquad \chi_V(g) = 0 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_V(g) = 1 \text{ si } g \notin \mathrm{H}.$$

Nous en déduisons le caractère de W car $\chi_V = \chi_{V'} + \chi_W$ et $\chi_{V'}(g) = 1$ pour tout $g \in \mathcal{A}_4$ (en effet $e_1 + e_2 + e_3 + e_4$ est fixe par $\mathcal{A}_4$ donc $\chi_{V'} \simeq \chi_{\rho_{\mathrm{triv}}}$). Par suite

$$\chi_W(\mathrm{id}) = 3, \qquad \chi_W(g) = -1 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_W(g) = 0 \text{ si } g \notin \mathrm{H}.$$

Montrons que W est irréductible. Commençons par constater que si g appartient à $\mathcal{A}_4$ et si $v = (x_1, x_2, x_3, x_4)$ appartient à $\mathbb{C}^4$, alors

$$g \cdot v = x_1 e_{g(1)} + x_2 e_{g(2)} + x_3 e_{g(3)} + x_4 e_{g(4)} = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}, x_{g^{-1}(4)}).$$

Supposons que v appartienne à $W \smallsetminus \{0\}$; soit W' le sous-espace de W engendré par les $g \cdot v$ pour $g \in \mathcal{A}_4$. Montrons que $W = W'$ quel que soit v. Il existe donc $i \neq j$ tel que $x_i \neq x_j$; sans perdre de généralité on peut supposer que $x_1 \neq x_2$. L'image de v par le 3-cycle t est alors (x_3, x_1, x_2, x_4) ; il s'ensuit que W' qui contient $t \cdot v$ et v contient $w = t \cdot v - v = (x_3 - x_1, x_1 - x_2, x_2 - x_3, 0)$. Le sous-espace W' contient aussi $w + g \cdot w$ si $g = (1\ 3)(2\ 4)$, et comme

$$w + g \cdot w = (x_1 - x_2)(e_2 + e_4 - e_1 - e_3)$$

et $x_1 - x_2 \neq 0$ il contient le vecteur $f_1 = e_1 - e_2 + e_3 - e_4$. Il contient donc aussi les images $f_2 = e_1 + e_2 - e_3 - e_4$ et $f_3 = e_1 - e_2 - e_3 + e_4$ de f_1 par les 3-cycles $(2\ 4\ 3)$ et $(2\ 3\ 4)$. Puisque f_1, f_2 et f_3 forment une base de W nous avons l'égalité recherchée $W = W'$.

h) Le groupe $\mathcal{A}_4$ compte quatre classes de conjugaison, il a donc quatre représentations irréductibles à isomorphismes près qui sont les trois caractères linéaires ρ_{triv}, η et η^2 et la représentation W de dimension 3. Les valeurs des caractères de ces représentations ont été calculées ci-dessus d'où la table des caractères de $\mathcal{A}_4$:

	C_1	C_2	C_3	C_4
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1
χ_η	1	1	ζ	ζ^2
χ_{η^2}	1	1	ζ^2	ζ
χ_W	3	-1	0	0

Exercice 683

a) Soit G un groupe fini abélien et soit χ un caractère de G sur $\mathbb{C}$.

Montrer que

$$\sum_{a \in \mathrm{G}} |\chi(a)|^2 \geq |\mathrm{G}| \cdot \chi(1).$$

b) Soit G un groupe fini et soit H un sous-groupe abélien de G d'indice $n \geq 1$.

Montrer que si χ est un caractère irréductible de G, on a $\chi(1) \leq n$. Que peut-on dire si $\chi(1) = n$?

Éléments de réponse 683

Exercice 684

Soit G un groupe fini. Soient ϕ et ψ des caractères de G dans $\mathbb{C}$.

a) Montrer que si ψ est de degré 1, alors $\phi\psi$ est irréductible si et seulement si ϕ est irréductible.

b) Montrer que si ψ est de degré strictement supérieur à 1, alors le caractère $\psi\overline{\psi}$ n'est pas irréductible.

c) Soit ϕ un caractère irréductible de G. On suppose que ϕ est le seul caractère irréductible de son degré. Montrer que s'il existe un caractère ψ de degré 1 et $g \in \mathrm{G}$ tel que $\psi(g) \neq 1$, alors $\phi(g) = 0$.

Éléments de réponse 684

Exercice 685

Soit p un nombre premier. Soit $n \geq 1$ un entier. On pose $q = p^n$. Soit G le groupe donné par

$$\mathrm{G} = \{x \mapsto ax + b \,|\, a \in \mathbb{F}_q^x,\, b \in \mathbb{F}_q\}.$$

a) Déterminer la table des caractères de G sur $\mathbb{C}$.

b) Déterminer les représentations irréductibles de G sur $\mathbb{C}$.

Éléments de réponse 685

Exercice 686

Soient p un nombre premier, G un p-groupe fini et $\Bbbk$ un corps de caractéristique p.

a) Montrer que toute représentation linéaire de G sur un $\Bbbk$-espace vectoriel non nul admet des vecteurs fixes non nuls.

b) Montrer que toute représentation irréductible de G à coefficients dans $\Bbbk$ est isomorphe à la représentation triviale.

Éléments de réponse 686

Exercice 687

a) Soient G un groupe abélien (éventuellement infini) et (V, ρ) une représentation complexe irréductible de G (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle de dimension 1 ? Est-ce toujours le cas ?

b) Soient $\Bbbk$ un corps de caractéristique nulle, G un groupe (éventuellement infini) et (V, ρ) une représentation de G sur $\Bbbk$ (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle somme directe de sous-représentations irréductibles ? Est-ce toujours le cas ?

Éléments de réponse 687

Exercice 688

Montrer que deux représentations de degré 1 d'un groupe G sont équivalentes si et seulement si elles coïncident.

Éléments de réponse 688

Exercice 689

Soit G un groupe.

a) Soient ρ_1 et ρ_n des représentations complexes de G de degré respectivement 1 et n. Montrer que

$$\rho_1 \cdot \rho_n \colon \mathrm{G} \longrightarrow \mathrm{GL}(n, \mathbb{C}), \qquad g \longmapsto \rho_1(g) \cdot \rho_n(g)$$

est une représentation de G.

b) Si ρ_n est irréductible, montrer que $\rho_1 \cdot \rho_n$ l'est aussi.

Éléments de réponse 689

Exercice 690

Soient G un groupe fini et H un sous-groupe distingué de G. Montrer que l'ensemble des représentations du groupe quotient G/H s'identifie naturellement aux représentations de G dont la restriction à H est triviale.
En déduire une injection de l'ensemble des représentations irréductibles de G/H dans l'ensemble des représentations irréductibles de G.

Éléments de réponse 690

Exercice 691

Soit $\rho \colon \mathrm{G} \longrightarrow \mathrm{GL}(V)$ une représentation irréductible d'un groupe abélien fini G dans un $\mathbb{C}$-espace vectoriel de dimension finie.

a) Utiliser le lemme de Schur pour montrer que $\rho(g)$ est une homothétie, pour tout $g \in \mathrm{G}$.

b) En déduire que chaque sous-espace vectoriel de V est ρ-invariant.

c) Conclure que le degré de ρ est égal à 1.

Éléments de réponse 691

Exercice 692

Soit ρ la représentation du groupe symétrique $\mathfrak{S}_n$ dans $V = \mathbb{C}^n$ agissant par permutations des coordonnées (*i.e.* $\sigma \cdot (x_1, \ldots, x_n) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$). Montrer que l'hyperplan H d'équation $\sum_{1 \leq i \leq n} x_i = 0$ est stable pour cette action et que la représentation associée est irréductible.

Éléments de réponse 692

Exercice 693

Montrer que tout groupe fini est isomorphe (par exemple via la représentation régulière) à un sous-groupe de $\mathrm{GL}(V)$ où V désigne un espace vectoriel approprié de dimension finie.

Éléments de réponse 693

Exercice 694

Soient G un groupe fini et $\rho\colon \mathrm{G} \to \mathrm{GL}(n, \mathbb{C})$ une représentation de G dans $\mathbb{C}^n$. Construire un produit scalaire hermitien $< \cdot, \cdot >_G$ sur $\mathbb{C}^n$ invariant par G, i.e.

$$\langle \rho(g)(x), \rho(g)(y) \rangle_{\mathrm{G}} = \langle x, y \rangle_{\mathrm{G}}, \qquad \forall\, x, y \in \mathbb{C}^n, \forall\, g \in \mathrm{G}.$$

Retrouver le lemme de Maschke : toute sous-représentation de ρ admet un supplémentaire stable par G.

Éléments de réponse 694

Exercice 695

Soient X un ensemble fini et G un groupe fini opérant sur X. Notons V la représentation de permutation de G sur $\mathbb{C}^X$ et χ_V son caractère.
Soit c le nombre d'orbites de l'action de G sur X. Montrer que c est égal au nombre de fois que V contient la représentation triviale 1. En déduire la formule de Burnside :

$$c = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|.$$

Éléments de réponse 695

Exercice 696

Soit G un groupe fini. Soit H un sous-groupe de G. Soit π une représentation de G de caractère χ.

a) Montrer que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$.

b) Si π est irréductible, est-ce que $\chi_{|\mathrm{H}}$ est un caractère irréductible ?

Éléments de réponse 696

a) Montrons que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$. Pour tout $h \in H$ on a

$$\chi_{\pi_{|\mathrm{H}}}(h) = \mathrm{tr}(\pi_{|\mathrm{H}}(h)) = \mathrm{tr}(\pi(h)) = \chi(h) = \chi_{|\mathrm{H}}(h).$$

b) Si π est irréductible, $\chi_{|\mathrm{H}}$ n'est pas nécessairement un caractère irréductible. En effet soit G un groupe fini non abélien. Soit $H = \{e_{\mathrm{G}}\}$ le sous-groupe trivial de G et soit π une représentation complexe irréductible de G de dimension ≥ 2 (une telle représentation existe). Alors toute droite de π est un sous-espace strict non nul de π stable par H donc $\chi_{|\mathrm{H}}$ n'est pas irréductible.

Exercice 697

Soit G un groupe fini. Soit H un sous-groupe de G. Soit (π, V) une représentation de H. On pose

$$W = \{f\colon \mathrm{G} \to V \mid \forall\, x \in \mathrm{G}\, \forall\, h \in H \quad f(hx) = \pi(h)f(x)\}$$

avec une action de G donnée par $g(f)\colon x \mapsto f(xg)$.

a) Montrer que W est une représentation de G. Quelle est sa dimension ?

b) Si π est irréductible, W est-elle une représentation irréductible de G ?

Éléments de réponse 697

a) Montrons que W est une représentation de G. On peut vérifier que

- W est un sous-espace vectoriel de V^{G} ;
- la formule $(g, f) \mapsto g(f)$ définit une action de groupes linéaire de G sur W ;
- pour tout $g \in \mathrm{G}$ et pour tout $f \in W$, on a $f(g)$ appartient à W. En effet, pour tout $h \in H$ et pour tout $x \in \mathrm{G}$ on a

$$g(f)(hx) = f(h(xg)) = \pi(h)f(xg) = \pi(h)g(f)(x).$$

Ces trois points assurent que W est naturellement une représentation de G.

Précisons la dimension de W.

Si $R \subset G$ désigne l'ensemble des représentants de G modulo H l'application

$$W \to V^R \qquad\qquad f \mapsto f_{|R}$$

est une application linéaire. C'est un isomorphisme par définition de W : un élément de W est entièrement déterminé par l'image des éléments de R. Par suite $\dim W = |R| \dim V$, *i.e.* $\dim W = [\mathrm{G} : \mathrm{H}] \dim V$.

b) Si π est irréductible, W n'est pas nécessairement une représentation irréductible de G. Considérons un groupe G non trivial et $H = \{e_G\}$ le sous-groupe trivial. La représentation triviale de H, notée triv, est irréductible. On peut vérifier que $W(\text{triv}) \simeq K[G]$ où $K[G]$ désigne la représentation régulière de G. Or cette dernière est irréductible si et seulement si $|G| = 1$ ce que l'on a exclu.

Exercice 698 [Représentations et sous-groupes distingués, Peyre, l'algèbre discrète de la transformée de Fourier, pages 231-232]

Soit G un groupe fini dont e_G est l'élément neutre. Soient ρ_1, ρ_2, …, ρ_r un ensemble de représentants des classes d'isomorphies de représentations irréductibles. Soient χ_1, χ_2, …, χ_r les caractères irréductibles associés. Posons

$$K_{\chi_i} = \{g \in G \,|\, \chi_i(g) = \chi_i(e_G)\}$$

a) Soit $\rho\colon G \to GL(V)$ une représentation de caractère χ_V sur un $\mathbb{C}$-espace V de dimension d. Soit g un élément d'ordre k de G. Alors

(i) $\rho(g)$ est diagonalisable ;

(ii) χ_V est somme de $\chi_V(1) = \dim V = d$ racines $k$ième de l'unité ;

(iii) $|\chi_V(g)| \leq \chi_V(e_G) = d$;

(iv) $K_{\chi_V} = \{x \in G, \,|\, \chi_V(x) = \chi_V(e_G)\}$ est un sous-groupe distingué de G. On l'appelle noyau de la représentation.

b) Soit $N \lhd G$ un sous-groupe distingué de G. Soit ρ_U une représentation de G/N sur un espace vectoriel U.

Il existe une représentation canonique de G sur U telle que les sous-représentations de U sous l'action de G/N soient exactement celles de U sous l'action de G.

c) Soit V un espace vectoriel de dimension égale à l'ordre de G. Soit $(b_t)_{t\in G}$ une base de V. La représentation régulière de G est la représentation

$$\begin{array}{rcl} \rho_{\text{reg}}\colon G & \to & GL(V) \\ g & \mapsto & \rho_{\text{reg}}(g)\colon V \to V \\ & & \qquad b_t \mapsto b_{gt} \end{array}$$

Soit $\rho\colon G \to GL(V)$ une représentation de G. La représentation est fidèle si ρ est injectif.

Montrer que la représentation régulière est fidèle.

d) Montrer que les sous-groupes distingués de G sont les

$$\bigcap_{i\in I} K_{\chi_i}$$

où $I \subset \{1, 2, 3, \ldots, r\}$.

e) Montrer que G est simple si et seulement si

$$\forall\, i \neq 1,\, \forall\, g \in \mathrm{G} \qquad \chi_i(g) \neq \chi_i(e_{\mathrm{G}}).$$

Éléments de réponse 698

a) (i) Puisque $g^k = 1$, on a $\rho(g)^k = \mathrm{id}$. Le polynôme minimal de $\rho(g)$ divise donc $X^k - 1$ qui est scindé à racines simples.

(ii) Soient λ_1, λ_2, …, λ_d les valeurs propres de $\rho(g)$ qui sont des racines $k$ièmes de l'unité. On a $\chi_V(g) = \lambda_1 + \lambda_2 + \ldots + \lambda_d$.

(iii) On a $|\chi_V(g)| \leq |\lambda_1| + |\lambda_2| + \ldots + |\lambda_d| = d$.

(iv) Si $|\chi_V(g)| = d$, alors d'après (iii) les nombres complexes λ_i sont positivement liés sur $\mathbb{R}$; comme ils sont de module 1, ils sont tous égaux. Si $\chi_V(g) = d$, alors nécessairement $\lambda_i = 1$ donc $\rho(g) = \mathrm{id}$. Ainsi $K_{\chi_V} = \ker\rho$ est bien un sous-groupe distingué.

b) Désignons par $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{N}}$ la projection canonique. La représentation $\widetilde{\rho}_U$ définie par

$$\forall\, g \in \mathrm{G} \qquad \widetilde{\rho}_U(g) = \rho_U \circ \pi(g)$$

convient.

c) Direct.

d) Soit $\mathrm{N} \lhd \mathrm{G}$ un sous-groupe distingué de G. Désignons par ρ_U la représentation régulière de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. Autrement dit U est un espace vectoriel de dimension égale à $|{}^{\mathrm{G}}\!/_{\mathrm{N}}| = \frac{|\mathrm{G}|}{|\mathrm{N}|}$ de base $(e_g)_{g\in{}^{\mathrm{G}}\!/_{\mathrm{N}}}$ et $\rho_U(h)(e_{\mathrm{G}}) = e_{hg}$. La représentation régulière est fidèle (c)) donc ρ_U est injective. Le b) permet d'étendre cette représentation en une représentation $\widetilde{\rho}_U\colon \mathrm{G} \to U$. Notons χ le caractère de la représentation $\widetilde{\rho}_U$. On a $\ker\widetilde{\rho}_U = \ker(\rho_U \circ \pi) = \mathrm{N}$ D'où $\mathrm{N} = K_\chi$. Ecrivons la décomposition de la représentation $\widetilde{\rho}_U$ en fonction des représentations irréductibles

$$\chi = a_1\chi_1 + a_2\chi_2 + \ldots + a_r\chi_r$$

D'après la troisième assertion de a) on a

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}}).$$

On a donc l'égalité $\chi(g) = \chi(e_{\mathrm{G}})$, *i.e.* $g \in K_\chi$, si et seulement si

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| = \sum_{i=1}^{r} a_i|\chi_i(g)| = \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}})$$

autrement dit si et seulement si

$$\forall\, i \qquad a_i\chi_i(g) = a_i\chi_i(e_{\mathrm{G}}).$$

Ceci est finalement équivalent à

$$\forall\, i \qquad a_i > 0 \Rightarrow g \in K_{\chi_i}.$$

On obtient donc le résultat voulu avec $I = \{i \,|\, a_i > 0\}$.

Réciproquement comme les K_{χ_i} sont distingués tout sous-groupe du type $\bigcap_{i\in I} K_{\chi_i}$ l'est aussi.

e) Supposons qu'il existe un élément de $\mathrm{G} \smallsetminus \{e_\mathrm{G}\}$ tel que $\chi_i(g) = \chi_i(e_\mathrm{G})$; alors $K_{\chi_i} \subset \mathrm{G}$ est un sous-groupe distingué non trivial et G n'est pas simple.

Réciproquement si G n'est pas simple, il existe $g \neq e_\mathrm{G}$ dans un certain sous-groupe distingué $\mathrm{N} \triangleleft \mathrm{G}$ non trivial. Le d) assure que $\mathrm{N} = \bigcap_{i\in I} K_{\chi_i}$ donc g appartient à K_{χ_i} pour $i \in I \subset \{2, 3, \ldots, r\}$. Ceci signifie bien que $\chi_i(g) = \chi_i(e_\mathrm{G})$.

Exercice 699

Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}(n, \mathbb{C})$ est le groupe des homothéties.

Une représentation ρ du groupe $\mathrm{GL}(n, \mathbb{C})$ est donnée par son action naturelle sur $\mathbb{C}^n$.

1. Montrer que la représentation ρ est irréductible.
2. Montrer que tout élément du centre de $\mathrm{GL}(n, \mathbb{C})$ est un morphisme de la représentation ρ, *i.e.* montrer que pour tout élément h du centre et pour tout élément M de $\mathrm{GL}(n, \mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M).$$
3. Conclure en utilisant le Lemme de Schur.

Éléments de réponse 699

Puisque ρ est l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}(n, \mathbb{C})$ dans $\mathrm{GL}(n, \mathbb{C})$.

1. Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}(n, \mathbb{C})$, alors $V = \{0\}$ ou $V = \mathbb{C}^n$, *i.e.* ρ est irréductible.
2. Soit h un élément du centre de $\mathrm{GL}(n, \mathbb{C})$. Pour tout M dans $\mathrm{GL}(n, \mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M)$$
ainsi h est bien un morphisme de la représentation ρ.
3. Comme ρ est irréductible, le Lemme de Schur assure que $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, *i.e.* h est une homothétie.

Exercice 700

Soit G un groupe fini. Soit E un ensemble fini sur lequel G agit et soit ρ la représentation de permutation correspondante. Notons χ le caractère de ρ. Montrer que $\chi(g)$ est le nombre d'éléments de E fixé par g.

Éléments de réponse 700

Dans la représentation de permutation la matrice $\rho(g)$ est une matrice de permutation avec

- ◇ un 1 à la position (i,i) si i est fixé par g,
- ◇ un 0 à la position (i,i) sinon.

Puisque $\chi(g) = \mathrm{tr}\rho(g)$, $\chi(g)$ coïncide avec le nombre d'éléments de E fixé par g.

Exercice 701

Soit G un groupe fini. Soit ρ une représentation linéaire de G. Notons χ le caractère de ρ. Montrons que le nombre de fois où ρ_{triv} apparaît dans ρ est égal à $\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)$.

Éléments de réponse 701

Décomposons ρ en somme de représentations irréductibles : $\rho = \bigoplus_{i=1}^{k}\rho_i^{n_i}$. Quitte à réindicer les ρ_i on peut supposer que $\rho_1 = \rho_{\mathrm{triv}}$.

De plus

$$\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)\cdot 1 = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi(g)\cdot\chi_{\rho_{\mathrm{triv}}}(g^{-1}) = \langle\chi,\chi_{\rho_{\mathrm{triv}}}\rangle = n_1$$

Exercice 702

Soit G un groupe abélien.

1. Si $\rho\colon \mathrm{G}\to\mathrm{GL}(V)$ est une représentation de G, montrer que tout élément G de G définit un G-morphisme $V\to V$.
2. En déduire que toute représentation irréductible de G est de dimension 1.
3. Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 702

1. Pour tous g, h et x dans G on a
$$g\cdot(h\cdot x) = (gh)\cdot x = (hg)\cdot x = h\cdot(g\cdot x)$$
c'est-à-dire l'application $\rho(g)\colon x\mapsto g\cdot x$ est un G-morphisme pour tout $g\in\mathrm{G}$.
2. On suppose que V est une représentation irréductible de G. Si $g\in\mathrm{G}$, alors, d'après 1. et le Lemme de Schur, $\rho(g) = \lambda\mathrm{id}$. De plus comme $\rho(g)\in\mathrm{GL}(V)$, λ est non nul. Par conséquent tout sous-espace vectoriel de V est stable par G donc est une sous-représentation de G. Puisque V est irréductible, $\dim V = 1$.

3. D'après 1. une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes
$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*$$
Tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n ; par suite $\rho(k)$ est aussi d'ordre divisant n, *i.e.* $\rho(k)^n = 1$. Réciproquement pour tout racine $n$ième de l'unité ω l'application
$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$
est une représentation de $\mathbb{Z}/n\mathbb{Z}$. On les obtient donc toutes ainsi.

Notons aussi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 703

Soit G un groupe fini. Soit H un sous-groupe abélien de G.

Montrer que toute représentation irréductible de G est de dimension au plus [G : H].

Indication : si V est une représentation irréductible de G*, c'est aussi une représentation de* H*. On pourra considérer la représentation de* G *engendrée par une sous-représentation de* H*.*

Éléments de réponse 703

Soit V une représentation irréductible de G. C'est aussi par restriction une représentation irréductible de H. Puisque H est abélien, V vu comme représentation de H se décompose en somme directe de représentations de H de degré 1. Soit v un vecteur directeur d'une de ces représentations et soit V' le sous-espace vectoriel de V engendré par les vecteurs de la forme $g \cdot v$ où g parcourt G. Il est clair que $V' \neq \{0\}$ est une sous-représentation de V du groupe G ; ainsi $V' = V$. Or si $g' = gh$ avec h dans H, alors par définition de v, $g' \cdot v$ et $g \cdot v$ sont colinéaires. Par conséquent V' est engendré par [G : H] vecteurs, et est donc de dimension au plus [G : H].

Exercice 704

Montrer que tout groupe non abélien admet une représentation irréductible de dimension > 1.

Éléments de réponse 704

Soit G un groupe dont toutes les représentations irréductibles sont de degré 1. La somme des carrés des dimensions des représentations irréductibles de G est égale au cardinal de G ; par suite les classes de conjugaisons de G sont toutes réduites à un élément. Autrement dit G est abélien.

Exercice 705

Montrer que si V est une représentation d'un groupe fini vérifiant $\langle \chi_V, \chi_V \rangle = 2$, alors V est somme de deux représentations irréductibles.

Éléments de réponse 705

Si $V = \oplus V_i^{a_i}$, alors $\langle \chi_V, \chi_V \rangle = 2$ si et seulement si deux a_i distincts sont non nuls et égaux à 1.

Exercice 706

Soit $\mathfrak{S}_3$ le groupe des permutations de $\{1, 2, 3\}$.

Notons e, s et t les trois classes de conjugaison de $\mathfrak{S}_3$ où e est la classe de conjugaison de l'identité, s celle des transpositions et t celle des 3-cycles.

1. Montrer (sans les construire) que $\mathfrak{S}_3$ a deux représentations irréductibles de dimension 1 et une de dimension 2.
2. Notons χ_1 le caractère de la représentation triviale, χ_2 celui de la signature sgn qui est l'autre représentation de dimension 1 et θ celui de la représentation W de dimension 2. De quelle représentation $\psi = \chi_1 + \chi_2 + 2\theta$ est-il le caractère ? Compléter la table

	e	s	t
χ_1			
χ_2			
$\chi_1 + \chi_2 + 2\theta$			
θ			

3. Faisons agir $\mathfrak{S}_3$ sur lui-même par conjugaison intérieure ($g \cdot x = gxg^{-1}$). Notons V la représentation de permutation associée et χ son caractère. Calculer χ. En déduire les multiplicités de la représentation triviale, de la représentation sgn et de la représentation W dans la décomposition de V.

Éléments de réponse 706

1. Puisque le groupe $\mathfrak{S}_3$ a trois classes de conjugaison, il a trois représentations irréductibles ; nous les notons W_1, W_2 et W_3. Comme $(\dim W_1)^2 + (\dim W_2)^2 + (\dim W_3)^2 = 6$ la seule possibilité est que deux des dimensions valent 1 et la troisième 2.
2. La première colonne des première, deuxième et quatrième lignes correspond aux dimensions des W_i.

   Les seconde et troisième colonnes des deux premières lignes s'obtiennent directement.

   Les seconde et troisième colonnes de la troisième ligne s'obtient par orthogonalité des colonnes (si on note a (resp. b) le coefficient de la seconde (resp. troisième) colonne, on a $1 \times 1 + 1 \times (-1) + 2 \times a = 0$ soit $a = 0$ et $1 \times 1 + 1 \times 1 + 2 \times b = 0$ soit $b = -1$).

   La troisième ligne s'obtient à partir des première, seconde et quatrième lignes.

   Finalement on a

	e	s	t
χ_1	1	1	1
χ_2	1	-1	1
$\chi_1+\chi_2+2\theta$	6	0	0
θ	2	0	-1

Enfin $\chi_1+\chi_2+2\theta$ est le caractère de la représentation régulière [34].

3. Comme V est une représentation de permutation, $\chi(g)$ est le nombre de points fixes de g, *i.e.* le nombre d'éléments h de $\mathfrak{S}_3$ tels que $ghg^{-1}=h$, ou encore le nombre d'éléments de $\mathfrak{S}_3$ qui commutent avec g. Nous avons donc $\chi(g)=|Z_g|=|\mathfrak{S}_3|\cdot|C_g|^{-1}$ où Z_g désigne l'ensemble des éléments de $\mathfrak{S}_3$ qui commutent à g et C_g la classe de conjugaison de g. Nous en déduisons que $\chi(e)=6$, $\chi(s)=2$ et $\chi(t)=3$.

   Si W' est une représentation irréductible, alors la multiplicité de W' dans V est $\langle\chi_{W'},\chi\rangle$. Comme

$$\langle\chi_1,\chi\rangle=\frac{1}{6}\Big(6+3\times(1\times 2)+2\times(1\times 3)\Big)=3$$
$$\langle\chi_2,\chi\rangle=\frac{1}{6}\Big(6+2\times(-1\times 2)+2\times(1\times 3)\Big)=1$$
$$\langle\theta,\chi\rangle=\frac{1}{6}\Big(2\times 6+3\times(0\times 2)+2\times(-1\times 3)\Big)=1$$

   nous avons $V=3\rho_{\text{triv}}\oplus\text{sgn}\oplus W$.

Exercice 707

On se propose d'établir la table des caractères du groupe $\mathfrak{S}_4$ des permutations de $\{1, 2, 3, 4\}$. Les partitions de 4 sont

$$4 \qquad 3+1 \qquad 2+2 \qquad 2+1+1 \qquad 1+1+1+1;$$

il en résulte que le groupe $\mathfrak{S}_4$ a 5 classes de conjugaison : la classe C_1 de l'élément neutre (1 élément), celle C_2 des transpositions (6 éléments), celle $C_{2,2}$ des produits de deux transpositions de supports disjoints (3 éléments), celle C_3 des 3-cycles (8 éléments), celle C_4 des 4-cycles (6 éléments) ;

34. Rappelons que si G est fini, si $E=\text{G}$ et si l'action de G est donnée par la multiplication à gauche, alors la représentation régulière est donnée par : $\chi(1)=|\text{G}|$ et $\chi(g)=0$ si $g\in\text{G}\smallsetminus\{e\}$.

	1	6	3	8	6
	C_1	C_2	$C_{2,2}$	C_3	C_4
$\chi_{\rho_{\text{triv}}}$	1	1	1	1	1
sgn	1	-1	1	1	-1
θ	2	0	2	-1	0
χ_1	3	1	-1	0	-1
χ_2	3	-1	-1	0	1

1. Soit V la représentation de permutation associée à l'action de $\mathfrak{S}_4$ sur $\{1, 2, 3, 4\}$.
   a) Calculer χ_V et $\langle \chi_V, \chi_V \rangle$. En déduire que V est la somme directe $V_1 \oplus V_2$ de deux représentations irréductibles V_1, V_2 non isomorphes.
   b) Déterminer les sous-espaces V_1 et V_2 de V et montrer, en revenant à la définition, que ce sont des représentations irréductibles de $\mathfrak{S}_4$.
   c) Calculer les caractères de V_1 et V_2. Quelles lignes de la table cela permet-il de remplir ?
2. Quelle est la seconde représentation de dimension 1 ? Comment peut-on obtenir la seconde de dimension 3 (pourquoi est-elle irréductible et différente de celle déjà construite ?) ?
3. Comment peut-on compléter la table des caractères de $\mathfrak{S}_4$?

Éléments de réponse 707

1. a) Puisque V est une représentation de permutation, $\chi_V(\sigma)$ est le nombre de points fixes de σ agissant sur $\{1, 2, 3, 4\}$. Par conséquent nous avons

$$\chi_V(C_1) = 4, \qquad \chi_V(C_2) = 2, \qquad \chi_V(C_{2,2}) = 0, \qquad \chi_V(C_3) = 1, \qquad \chi_V(C_4) = 0.$$

   Par suite

$$\langle \chi_V, \chi_V \rangle = \frac{1}{24}\Big(4^2 + 6 \times 2^2 + 3 \times 0^2 + 8 \times 1^2 + 6 \times 0^2\Big) = 2.$$

   Si $V = \bigoplus_{W \in \mathrm{Irr}(\mathfrak{S}_4)} m_W W$, $\langle \chi_V, \chi_V \rangle$ est aussi égal à $\sum_{W \in \mathrm{Irr}(\mathfrak{S}_4)} m_W^2$ puisque les χ_W forment une famille orthonormale. Étant donné que la seule écriture de 2 comme somme de deux carrés est $1^2 + 1^2$ nous en déduisons que $m_W = 1$ pour exactement deux représentations irréductibles W de $\mathfrak{S}_4$ et $m_W = 0$ pour les autres ce qui permet de conclure.

   b) La droite V_1 engendrée par $e_1 + e_2 + e_3 + e_4$ et l'hyperplan V_2 d'équation $x_1 + x_2 + x_3 + x_4 = 0$ sont stables par $\mathfrak{S}_4$.

   Puisque V_1 est de dimension 1 elle est automatiquement irréductible.

Soit $x = (x_1, x_2, x_3, x_4) \in V_2$ non nul. Il s'agit de démontrer que le sous-espace vectoriel U_x de V_2 engendré par les $\sigma \cdot x$, pour $\sigma \in \mathfrak{S}_4$, est égal à V_2. Il existe $i \neq j$ tels que $x_i \neq x_j$. Soit τ la transposition $(i\ j)$. Alors $x - \tau \cdot x$ est un multiple non nul de $e_i - e_j$. Il en résulte que $e_i - e_j$ appartient à U_x et donc que $\sigma \cdot (e_i - e_j) = e_{\sigma(i)} - e_{\sigma(j)}$ appartient à U_x pour tout $\sigma \in \mathfrak{S}_4$. Mais $(\sigma(i), \sigma(j))$ décrit les couples d'éléments distincts de $\{1, 2, 3, 4\}$ quand σ décrit $\mathfrak{S}_4$; ainsi U_x contient $e_1 - e_2$, $e_1 - e_3$ et $e_1 - e_4$. Ces vecteurs engendrant V_2 cela permet de conclure.

c) La représentation V_1 est la représentation triviale ; par conséquent $\chi_{V_1}(C) = 1$ pour toute classe de conjugaison C de $\mathfrak{S}_4$. Nous pouvons donc remplir la première ligne de la table.

Par ailleurs $\chi_V = \chi_{V_1} + \chi_{V_2}$, cela permet donc de déterminer χ_{V_2}. Nous pouvons donc remplir la quatrième ligne de la table.

2. La seconde représentation de dimension 1 est la signature sgn. Ses valeurs sont bien celles reportées dans la seconde ligne. La seconde représentation de dimension 3 est $V_1 \otimes \mathrm{sgn}$. Si elle pouvait se décomposer sous la forme $V_1 \otimes \mathrm{sgn} = W_1 \oplus W_2$, alors $V_1 = (V_1 \otimes \mathrm{sgn}) \otimes \mathrm{sgn}$ pourrait se décompose sous la forme $(W_1 \otimes \mathrm{sgn}) \oplus (W_2 \otimes \mathrm{sgn})$ ce qui est absurde. Nous avons $\chi_{V_1 \otimes \mathrm{sgn}}(g) = \chi_{V_1}(g)\mathrm{sgn}(g)$; ainsi $\chi_{V_1 \otimes \mathrm{sgn}}(C_2) = -1$ est différent de $\chi_{V_1}(C_2) = 1$. Les représentations $V_1 \otimes \mathrm{sgn}$ et V_1 ne sont donc pas isomorphes (leurs caractères sont distincts).

3. Le groupe $\mathfrak{S}_4$ ayant cinq classes de conjugaison, il y a cinq représentations irréductibles. Soient d la dimension de la représentation manquante et θ son caractère. La formule de Burnside assure que
$$24 = 1^2 + 1^2 + 3^2 + 3^2 + d^2$$
d'où $d = 2$.

Pour remplier la dernière ligne on utilise le fait que $\chi_{\rho_{\mathrm{triv}}} + \mathrm{sgn} + 2\theta + 3\chi_1 + 3\chi_2$ est le caractère de la représentation régulière qui est connu [35].

Exercice 708

Soit $\Bbbk$ un corps. Soit $\mathrm{G} \subset \mathrm{GL}(2, \Bbbk)$ le sous-groupe des $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ avec $a \in \Bbbk^*$ et $b \in \Bbbk$. Faisons agir G sur $\Bbbk$ par
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot x = ax + b.$$

1. Calculer
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1}.$$

35. Rappelons que si G est fini, si $E = \mathrm{G}$ et si l'action de G est donnée par la multiplication à gauche, alors la représentation régulière est donnée par : $\chi(1) = |\mathrm{G}|$ et $\chi(g) = 0$ si $g \in \mathrm{G} \smallsetminus \{e\}$.

En déduire que les classes de conjugaison de G sont

$$C_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \qquad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \smallsetminus \{0\} \right\}$$

et les

$$D_a = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \right\}$$

pour $a \in \Bbbk^* \smallsetminus \{1\}$.

2. Supposons désormais que $\Bbbk$ est fini, de cardinal q et donc que $|\mathrm{G}| = q(q-1)$ et G compte q classes de conjugaison. Désignons par V la représentation de permutation de G associée à l'action de G sur $\Bbbk$ et W l'hyperplan de V défini par

$$W = \Big\{ \sum_{x \in \Bbbk} \lambda_x e_x, \sum_{x \in \Bbbk} \lambda_x = 0 \Big\}$$

Montrer que W est une sous-représentation de V.

3. Calculer χ_W ; en déduire que W est irréductible.

4. Quelles sont les dimensions des autres représentations irréductibles de G ?

5. Comment peut-on construire un caractère linéaire de G à partir d'un caractère linéaire de $\Bbbk^*$?

En déduire que si $\Bbbk = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, alors la table des caractères de G est la suivante

	C_1	N	D_2	D_4	D_3
χ_{triv}	1	1	1	1	1
η	1	1	-1	1	-1
η^2	1	1	1	-1	-1
η^3	1	1	-1	-1	1
χ_W	2	-2	0	0	0

6. Supposons que $q = 4$. Établir la table des caracères de G. Cette table vous rappelle-t-elle quelque chose ? Pouvez-vous expliquer cette coïncidence ?

Éléments de réponse 708

1. Nous avons

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c & ad + (1-c)b \\ 0 & 1 \end{pmatrix}$$

Par suite un conjugué de $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ est de la forme $\begin{pmatrix} c & d' \\ 0 & 1 \end{pmatrix}$ et tout élément de cette forme est un conjugué de $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ si $c \neq 1$.

Les D_a, pour $a \in \Bbbk^* \smallsetminus \{1\}$ forment donc des classes de conjugaison.

Par ailleurs C_1 est la classe de conjugaison de l'élément neutre et N est la classe de conjugaison de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ car pour $a \neq 0$

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

2. Nous avons
$$g \cdot \Big(\sum_{x \in \Bbbk} \lambda_x e_x \Big) = \sum_{x \in \Bbbk} \lambda_x e_{g \cdot x} = \sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} e_x.$$
Or $x \mapsto g^{-1} \cdot x$ est une bijection de $\Bbbk$ donc $\sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} = \sum_{x \in \Bbbk} \lambda_x$ ce qui montre que $g \cdot v = \sum_{x \in \Bbbk} \lambda_{g^{-1} \cdot x} e_x$ appartient à W si $v = \sum_{x \in \Bbbk} \lambda_x e_x \in W$.

3. V est une représentation de permutation ; par conséquent $\chi_V(g)$ est le nombre de points fixes de g agissant sur $\Bbbk$. Nous sommes donc ramenés à calculer le nombre de solutions de l'équation $ax + b = x$ dans $\Bbbk$ ce qui conduit à
$$\chi_V(C_1) = q, \qquad \chi_V(N) = 0, \qquad \chi_V(D_a) = 1 \text{ si } a \in \Bbbk^* \smallsetminus \{1\}.$$
Maintenant V est la somme directe de W et de la droite engendrée par $\sum_{x \in \Bbbk} e_x$ sur laquelle G agit trivialement. Nous en déduisons $\chi_V(g) = \chi_W(g) + 1$ ce qui conduit à
$$\chi_W(C_1) = q - 1, \qquad \chi_W(N) = -1, \qquad \chi_W(D_a) = 0 \text{ si } a \in \Bbbk^* \smallsetminus \{1\}.$$
Alors
$$\langle \chi_W, \chi_W \rangle = \frac{1}{q(q-1)} \Big((q-1)^2 + |N| \times 1^2 + \sum_{a \in \Bbbk^* \smallsetminus \{1\}} |D_a| \times 0^2 \Big) = \frac{1}{q(q-1)} \Big((q-1)^2 + (q-1) \Big) = 1$$
ce qui assure l'irréductibilité de W [36].

4. Puisque
   - ◇ le nombre de classes de conjugaison de G coïncide avec le nombre de représentations irréductibles de G
   - ◇ G compte q classes de conjugaison

36. Nous utilisons ici le critère d'irréductibilité suivant : une représentation V de G est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.

il y a $q-1$ autres représentaitons irréductibles. Notons d_1, d_2, …, d_{q-1} leurs dimensions. La formule de Burnside assure que

$$q(q-1) = |\mathrm{G}| = (\dim W)^2 + \sum_{i=1}^{q-1} d_i^2;$$

comme $\dim W = q-1$ nous obtenons

$$\sum_{i=1}^{q-1} d_i^2 = q(q-1) - (q-1)^2 = q-1.$$

Une somme de $q-1$ entiers ≥ 1 ne pouvant être égale à $q-1$ que si tous les entiers sont égaux à 1 nous obtenons que les $q-1$ autres représentations de G sont de dimension 1 (*i.e.* sont des caractères linéaires).

5. Si χ est un caractère linéaire de $\Bbbk^*$, alors $\chi \circ \det$ est un caractère linéaire de G. Le groupe $\mathbb{F}_5^*$ est cyclique d'ordre 4 engendré par 2 (en effet $2^2 = 4$, $2^3 = 8 = 3$ et $2^3 = 16 = 1$). Un caractère de $\mathbb{F}_5^*$ est donc déterminé par sa valeur en 2 qui doit être une racine 4-ième de l'unité, c'est-à-dire 1, -1, $\mathbf{i}$ ou $-\mathbf{i}$. On compte donc quatre tels caractères. Si on note η celui pour lequel $\eta(2) = \mathbf{i}$ les autres sont η^2, η^3 et η^4 qui n'est autre que le caractère trivial. Les quatre caractères de G recherchés sont donc exactement les $\eta^j \circ \det$, pour $0 \leq j \leq 3$, ce qui fournit bien la table annoncée.

6. Le groupe $\Bbbk^*$ est d'ordre 3 ; il est donc cyclique, engendré par n'importe quel $a \neq 1$ (en effet si K est un corps fini, alors K^* est toujours cyclique ; dans le cas présent si $a \in K^* \smallsetminus \{1\}$, alors l'ordre du sous-groupe engendré par a divise $|K^*| = 3$, et donc vaut 3 ce qui fait que ce sous-groupe est K^*). Un caractère linéaire de $\Bbbk^*$ est donc déterminé par sa valeur en a qui est une racine cubique de l'unité. Il y a trois tels caractères. Si on note η celui pour lequel $\eta(a) = \mathbf{j} = \exp\left(\frac{2\mathbf{i}\pi}{3}\right)$ les autres sont η^2 et η^3 qui n'est autre que le caractère trivial. Nous obtenons donc la table

	C_1	N	D_a	D_{a^2}
χ_{triv}	1	1	1	1
η	1	1	j	j^2
η^2	1	1	j^2	j
χ_W	3	-1	0	0

Nous reconnaissons la table des caractères de $\mathcal{A}_4$ ce qui n'est pas étonnant car G est isomorphe à $\mathcal{A}_4$. En effet le choix d'une bijection entre $\Bbbk$ et $\{1, 2, 3, 4\}$ transforme l'action de G sur $\Bbbk$ en une action de G sur $\{1, 2, 3, 4\}$ et fournit donc une injection de G dans $\mathfrak{S}_4$. L'image H de cette injection est donc un sous-groupe de $\mathfrak{S}_4$, isomorphe à G. Un tel groupe est distingué dans $\mathfrak{S}_4$; en effet si g n'appartient pas à H nous avons $g\mathrm{H} = \mathrm{H}g = \mathfrak{S}_4 \smallsetminus \mathrm{H}$ pour des raisons d'ordre ($|\mathrm{H}| = |\mathrm{G}| = 12 = |\mathcal{A}_4|$ et $|\mathfrak{S}_4| = 24 = 2|\mathrm{H}|$) et

donc $gHg^{-1} = Hgg^{-1} = H$. Le quotient G/H est de cardinal 2 et donc isomorphe à $\{\pm\mathrm{id}\}$ ce qui fournit un caractère linéaire $\eta\colon \mathfrak{S}_4 \to \{\pm\mathrm{id}\}$. La restriction de η à $\mathcal{A}_4$ est encore un caractère linéaire mais les caractères de $\mathcal{A}_4$ sont à valeurs dans $\mu_3 = \{z \in \mathbb{C}^* \mid z^3 = 1\}$ ce qui implique $\eta = 1$ sur $\mathcal{A}_4$. Autrement dit $\mathcal{A}_4$ est inclus dans le noyau H de η et lui est donc égal pour des raisons d'ordre. Ainsi $G \simeq \mathcal{A}_4$.

Exercice 709

Soit G un groupe non abélien d'ordre 6.

1. Quels sont les ordres des éléments de G ?
2. Montrer que G a deux caractères irréductibles de degré 1 (notés **1** et η) et un de degré 2 (noté χ).
3. Montrer que G a trois classes de conjugaison. Quelles sont-elles ?
4. Montrer que $\eta(g) = 1$ si g est d'ordre 2 et que $\eta(g) = -1$ si g est d'ordre 2 (on s'intéressera à $\eta(g^2)$). En déduire le cardinal de chaque classe de conjugaison.
5. Dresser la table des caractères de G.

Éléments de réponse 709

Exercice 710

Faisons agir $\mathfrak{S}_n$ sur $\mathbb{C}^n$ par permutation des éléments de la base canonique. Montrer que l'hyperplan $\sum_{i=1}^{n} x_i = 0$ est stable par $\mathfrak{S}_n$ et que la représentation ainsi obtenue est irréductible (considérer $v - \sigma \cdot v$ où σ est une transposition).

En déduire une décomposition de $\mathbb{C}^n$ en somme de représentations irréductibles de $\mathfrak{S}_n$.

Éléments de réponse 710

Exercice 711

Soit G un sous-groupe fini de $\mathrm{GL}(n, \mathbb{C})$. Montrer que $\sum_{M \in G} \operatorname{tr} M$ est un entier. Comment cet entier s'interprète-t-il ?

Éléments de réponse 711

Exercice 712

Soit V une représentation de degré fini d'un groupe G (non nécessairement fini).

1. On suppose qu'il existe une forme hermitienne H sur V invariante par G, c'est-à-dire
$$H(u, v) = H(g \cdot u, g \cdot v) \qquad \forall\, u,\, v \in V \quad \forall\, g \in G.$$
Montrer que toute sous-représentation de V admet une sous-représentation supplémentaire.

2. Montrer que si G est fini, alors il existe toujours une telle forme hermitienne G-invariante.
3. On suppose V irréductible. Montrer que deux formes hermitiennes G-invariantes sont multiples l'une de l'autre (c'est-à-dire $H_1 = \mu H_2$).

Éléments de réponse 712

Cet exercice est une (re)démonstration du théorème de Maschke.

1. Soit W une sous-représentation de V. La forme hermitienne H nous donne un moyen canonique de trouver un supplémentaire de W : on prend son orthogonal. Comme H est invariante par G, on en déduit que $W^\perp$ est une sous-représentation de G par le calcul suivant
$$\forall\, g \in \mathrm{G} \quad \forall\, v \in W \quad \forall w \in W^\perp \quad H(v, g \cdot w) = H(g^{-1} \cdot v, w) = 0.$$
2. Soit H_0 une forme hermitienne sur V. Puisque G est fini, on peut définir une forme hermitienne H G-invariante en « moyennant » H_0 par G :
$$H(v, w) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} H_0(g \cdot v, g \cdot w)$$
Remarque : dans une base adéquate, une représentation d'un groupe fini sur un $\mathbb{C}$-espace vectoriel est donc unitaire. En particulier, tous les automorphismes linéaires sont diagonalisables.
3. Soient H et H' deux formes hermitiennes G-invariantes sur V. Alors H induit une bijection anti-linéaire
$$\varphi_H \colon V \to V^* \qquad\qquad v \mapsto (w \to H(w, v)).$$
De plus, comme H est G-invariante, $\varphi_H(g \cdot v) = g \cdot \varphi_H(v)$. L'application $\varphi_{H'}^{-1} \circ \varphi_H$ est donc un G-automorphisme linéaire de V, donc d'après le Lemme de Schur, $\varphi_{H'}^{-1} \circ \varphi_H = \mu \mathrm{id}$, c'est-à-dire $H = \mu H'$.

Exercice 713

Soient p un nombre premier et G un groupe d'ordre p^3 non abélien. On note $\mathbb{U}_p = \{z \in \mathbb{C} \mid z^p = 1\}$.

1. Montrer que les représentations irréductibles de G ont dimension 1 ou p. Que peut-on dire du nombre des représentations de G dans $\mathbb{C}$?
2. Montrer que le nombre de classes d'isomorphie de représentations irréductibles de dimension p de G est $p - 1$ et donner l'ordre de l'abélianisé de G.

   Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$.
3. Montrer que pour tout $\zeta \in \mathbb{U}_p$ il existe une représentation V de dimension 1 de G telle que $\chi_V(g) = \zeta$.

4. Déduire de ce qui précède et du fait que si G est un groupe fini le produit d'un caractère irréductible de G par un caractère de degré 1 est un caractère irréductible de G de même degré que si V est une représentation irréductible de dimension p de G, alors $\chi_V(g) = 0$.
5. Montrer que si V est une représentation de G de dimension n ($n \in \mathbb{N}^*$) alors l'un des nombres $\chi_V(g)$, $\chi_V(g^2)$, …, $\chi_V(g^n)$ est non nul (on pourra considérer la somme $\sum_\lambda C(\lambda)$, où C désigne le polynôme caractéristique de $v \cdot gv$, et λ parcourt ses n valeurs propres).
6. Déduire des questions 4. et 5. que l'abélianisé de G n'est pas cyclique. à quel groupe est-il isomorphe ?
7. Montrer à l'aide de la question 4. que si $g' \in D(\mathrm{G})$ et si (V, ρ) est une représentation irréductible de G alors $|\chi_V(g')| = \dim V$. Préciser les endomorphismes $\rho(g')$ pour g' parcourant $D(\mathrm{G})$.
8. Décrire le centre de G et donner le cardinal des différentes classes de conjugaison de G.
9. Donner explicitement la table des caractères de G lorsque $p = 3$.

Éléments de réponse 713

Soient p un nombre premier et G un groupe d'ordre p^3 non abélien. On note $\mathbb{U}_p = \{z \in \mathbb{C} \,|\, z^p = 1\}$.

1. La dimension des représentations irréductibles de G divise l'ordre de G, donc p^3 ; par la formule de Burnside, la somme des carrés de ces dimensions vaut l'ordre, p^3. Donc les seules valeurs possibles sont 1 et p. On sait que 1 est la dimension de la représentation triviale, irréductible. Et que G possède une représentation irréductible de dimension > 1, car il est non abélien (cours). Donc $\{1, p\}$ est l'ensemble des dimensions des représentations irréductibles de G. On sait qu'une représentation de G dans $\mathbb{C}$ est donnée précisément par un morphisme de G dans $\mathbb{C}^\times$ (*i.e.* un élément du dual G) et que leur nombre est l'ordre de l'abélianisé G_{ab}. En particulier ce nombre divise $|\mathrm{G}| = p^3$.
2. On écrit la formule de Burnside pour G : si r est le nombre de classes d'isomorphie de représentations irréductibles de dimension p de G, on obtient : $p^3 = |\mathrm{G}_{\mathrm{ab}}| + rp^2$. Par suite p^2 divise G_{ab}, qui divise lui-même p^3. Or G n'est pas abélien, donc l'ordre de G_{ab} n'est pas p^3, et c'est p^2. Il suit de la formule que $r = p - 1$.

   Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$.
3. Toute représentation (V, χ) de dimension 1 de G factorise par G_{ab}, d'ordre p^2. Puisque $g \notin D(\mathrm{G})$ on sait qu'il existe χ un caractère de degré 1 tel que $\chi(g) \neq 1$. On a $\chi(g)^{p^2} = 1$; si $\chi(g)$ est d'ordre p dans $\mathbb{C}^\times$, alors il engendre $\mathbb{U}_p$, donc tout $\zeta \in \mathbb{U}_p$ s'écrit $\zeta = \chi(g)^k = \chi^k(g)$ et la représentation $(\mathbb{C}, \chi^k)$ convient pour V. Sinon, $\chi^p(g)$ est d'ordre p, on remplace χ par le caractère χ^p dans l'argument.
4. Supposons $\chi_V(g) \neq 0$. Alors en multipliant χ_V par les p caractères de degré 1 obtenus en 3), on obtient par I 3. p caractères irréductibles de degré p distincts, car leur valeur en g diffère. Or par 2) G n'admet que $p - 1$ caractères irréductibles de degré p, contradiction.

5. Si on note λ_1, λ_2, …, λ_n les n valeurs propres de $\rho_V(g)$ (diagonalisable), alors celles de $\rho_V(g^k)$ sont λ_1^k, λ_2^k, …, λ_n^k. De plus $\rho_V(g)$ est inversible, donc de déterminant d_g non nul. La somme proposée par l'énoncé $\sum_\lambda C(\lambda)$, qui est nulle par définition, s'écrit donc aussi
$$\sum_{k=1}^{n} a_k \chi_V(g^k) + n a_0,$$
où on note $C(X) = \sum_{k=0}^{n} a_k X^k$ ($a_n = 1$, $a_0 = \pm d_g$). Le fait que na_0 soit non nul entraîne ainsi que l'un des $\chi_V(g^k)$, $1 \leq k \leq n$, l'est également.

6. Si l'abélianisé de G était cyclique, il serait engendré par la classe, d'ordre p^2, d'un certain élément g de $\mathrm{G} \smallsetminus D(\mathrm{G})$. On applique alors 5) à g et V une représentation irréductible de G de dimension p : avec 4) on en déduit que l'un des g^i, $1 \leq i \leq p$ est dans $D(\mathrm{G})$. Mais alors l'ordre de la classe de g dans l'abélianisé serait majorée par $i \leq p$, contradiction. Par suite G_{ab} est un groupe abélien d'ordre p^2, non cyclique. Par le théorème de structure des groupes abéliens finis, on a $\mathrm{G}_{\mathrm{ab}} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

7. Si $\dim V = 1$, alors $\chi_V(g') = 1$ pour tout $g' \in D(\mathrm{G})$ car χ_V est un morphisme dans $\mathbb{C}^\times$ abélien. Sinon, $\dim V = p$ et on écrit que le carré hermitien de χ_V vaut 1 : d'après 4), on trouve $\sum_{g' \in D(\mathrm{G})} |\chi_V(g')|^2 = p^3$. Or pour tout g' on sait que $|\chi_V(g')| \leq p = \dim V$. Puisque $|D(\mathrm{G})| = p$, ceci entraîne l'égalité $|\chi_V(g')| = p$ pour tout g'. Le cours montre que l'égalité $|\chi_V(g')| = \dim V$ a lieu si et seulement si $\rho_V(g')$ est une homothétie. Or si $g' \neq 1$, g' est d'ordre p donc l'ordre de $\rho_V(g')$ est 1 ou p. Si c'était 1, alors g' et donc $D(\mathrm{G})$ seraient dans le noyau de ρ_V ; ainsi ρ_V factoriserait en un morphisme de G_{ab} abélien dans $\mathrm{GL}(V)$, ce qui contredit le fait que V est irréductible de dimension > 1. Donc $\rho_V(g')$ est une homothétie d'ordre p, de rapport une racine primitive $p$ième ζ de 1. Alors on a $D(\mathrm{G}) = \{g'^{\ell} \mid 0 \leq \ell \leq p-1\}$, et chaque $\rho(g'^{\ell})$ est l'homothétie de V de rapport ζ^ℓ.

8. D'après 7., les p éléments de $D(\mathrm{G})$ ont pour carré hermitien de leur colonne associée dans la table de caractères de G la valeur $|\mathrm{G}| = p^3$ obtenue (Burnside) pour la colonne de 1, donc leur centralisateur est G, *i.e.* ils sont dans le centre de G. Soit $g \in \mathrm{G} \smallsetminus D(\mathrm{G})$. Par 4., g n'est pas dans le centre car il n'agit pas comme une homothétie sur V irréductible de dimension p (en effet, on sait que $\rho_V(g)$ est alors un G–morphisme, donc par Schur une homothétie). Or le centralisateur de g contient g et $D(\mathrm{G})$, donc ce sous-groupe a cardinal $> p$, et distinct de p^3, soit exactement p^2 par Lagrange. Le cardinal de la classe de conjugaison de g est donc $\frac{p^3}{p^2} = p$ (toute la classe a même image dans l'abélianisé, par cardinalité elle coïncide donc avec la classe à droite $gD(\mathrm{G})$). On obtient en particulier que le centre de G est égal à $D(\mathrm{G})$.

9. On note x un générateur de $D(\mathrm{G})$ (d'ordre 3), et g_{ij} un élément de $\mathrm{G} \smallsetminus D(\mathrm{G})$ qui s'envoie sur $(\bar{i}, \bar{j})$ dans le quotient G_{ab}, identifié au groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. On a $Z(\mathrm{G}) = D(\mathrm{G})$,

et la classe de conjugaison de g_{ij} dans G est $g_{ij}\langle x\rangle$ (cf. 8.). Ainsi la partie haute de la table privée des colonnes de x et x^2 est la table de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (groupe abélien, donc isomorphe à son groupe dual). Les deux représentations de degré 3, duales l'une de l'autre, correspondent sur $Z(\mathrm{G}) = D(\mathrm{G})$ à une action fidèle par homothéties, et on a $\rho(x^2) = \rho(x)^2$. Leurs caractères sont conjugués.

	1	x	x^2	g_{10}	g_{20}	g_{01}	g_{02}	g_{11}	g_{22}	g_{12}	g_{21}
χ_{00}	1	1	1	1	1	1	1	1	1	1	1
χ_{10}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$
χ_{20}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$
χ_{01}	1	1	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$
χ_{02}	1	1	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$
χ_{11}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$	1	1
χ_{22}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$	1	1
χ_{12}	1	1	1	$\mathbf{j}$	$\mathbf{j}^2$	$\mathbf{j}^2$	$\mathbf{j}$	1	1	$\mathbf{j}^2$	$\mathbf{j}$
χ_{21}	1	1	1	$\mathbf{j}^2$	$\mathbf{j}$	$\mathbf{j}$	$\mathbf{j}^2$	1	1	$\mathbf{j}$	$\mathbf{j}^2$
χ'	3	$3\mathbf{j}$	$3\mathbf{j}^2$	0	0	0	0	0	0	0	0
χ''	3	$3\mathbf{j}^2$	$3\mathbf{j}$	0	0	0	0	0	0	0	0

Exercice 714

1. Soit G un groupe abélien fini. Pour $g \in \mathrm{G}$ notons δ_g l'élément de $\mathbb{C}[\mathrm{G}]$ qui vaut 1 en g et 0 sur $\mathrm{G} \smallsetminus \{g\}$.
   a) Énoncer la formule d'inversion de Fourier et l'appliquer aux éléments δ_g de $\mathbb{C}[\mathrm{G}]$.
   b) En déduire que le morphisme naturel de G dans son bidual $\widehat{\widehat{\mathrm{G}}}$ est injectif.
2. Soit V une représentation d'un groupe fini G qui est somme directe de r représentations irréductibles deux à deux non isomorphes.
   a) Décrire l'algèbre $\mathrm{End}_{\mathrm{G}}(V)$ des G-endomorphismes de V.
   b) Déterminer toutes les sous–représentations de V.
3. Soit G un groupe fini. Montrer que le produit d'un caractère irréductible de G par un caractère de degré 1 est un caractère irréductible de G de même degré.

Éléments de réponse 714

1. Soit G un groupe abélien fini. Pour $g \in \mathrm{G}$ notons δ_g l'élément de $\mathbb{C}[\mathrm{G}]$ qui vaut 1 en g et 0 sur $\mathrm{G} \smallsetminus \{g\}$.

a) Pour toute f dans $\mathbb{C}[\mathrm{G}]$, nous avons

$$f = \frac{1}{|\mathrm{G}|} \sum_{\xi \in \widehat{\mathrm{G}}} \widehat{f}(\chi)\chi^{-1}$$

Et

$$\widehat{\delta_g}(\chi) = \sum_{g'} \delta_g(g')\chi(g') = \chi(g).$$

Ainsi

$$\delta_g = \frac{1}{|\mathrm{G}|} \sum_{\chi \in \widehat{\mathrm{G}}} \chi(g)\chi^{-1}.$$

b) Soit $g \in \mathrm{G}$. Par a), la transformée de Fourier de δ_g est l'application $\chi \mapsto \chi(g)$. Elle s'identifie donc à l'image naturelle de g dans son bidual. Un élément g est dans le noyau de ce morphisme naturel d'évaluation si et seulement si tous les caractères $\chi \in \widehat{\mathrm{G}}$ y valent 1, c'est-à-dire si et seulement si g a même transformée de Fourier que 1. Par la formule d'inversion ceci équivaut à $g = 1$.

2. Soit V une représentation d'un groupe fini G qui est somme directe de r représentations irréductibles deux à deux non isomorphes.

a) Si $V = \bigoplus_{i=1}^{r} V_i$, alors chaque élément de $\mathrm{End}_{\mathrm{G}}(V)$ se « décompose » en une somme directe de G-morphismes de V_i dans V_j, pour (i, j) variant dans $\{1, \ldots, r\} \times \{1, \ldots, r\}$. Par le lemme de Schur, les G-morphismes entre irréductibles non isomorphes sont nuls, et $\mathrm{End}_{\mathrm{G}}(V_i) = \mathbb{C}\mathrm{id}_{V_i}$. Nous en déduisons que l'algèbre $\mathrm{End}_{\mathrm{G}}(V)$ s'identifie au produit des algèbres $\mathbb{C}\mathrm{id}_{V_i}$ (blocs diagonaux d'une homothétie sur chaque V_i).

b) On utilise l'unicité de la décomposition canonique de V : par l'hypothèse, toutes les composantes isotypiques de V sont irréductibles, et les sous-représentations sont toutes les sommes (directes) de certaines de ces composantes. (Attention, si une représentation irréductible apparaissait dans V avec multiplicité > 1, la composante isotypique correspondante, et par suite V, possèderait une infinité de sous-représentations irréductibles, toutes isomorphes !)

3. Soit G un groupe fini.

Le produit des caractères de deux représentations V et (W, ρ) est le caractère de la représentation $\mathrm{Hom}(V^*, W)$, où V^* est la représentation duale de V. Ou encore : si $\dim V = 1$, ce produit est le caractère de la représention $\chi_V \cdot \rho$ de G sur W ($g \cdot w =: \chi_V(g) \cdot \rho(g)(w) \in W$). Le degré de ce caractère produit est sa valeur en 1, donc clairement le degré de χ_W. L'irréductibilité du produit (valable si $\dim V = 1$!) s'obtient facilement en calculant le carré hermitien de $\chi_V\chi_W$, égal à celui de χ_W (car χ_V, morphisme de G dans $\mathbb{C}^\times$, a pour valeurs des racines de l'unité donc de module 1), donc ce carré hermitien vaut 1 par l'irréductibilité de χ_W. On peut aussi remarquer qu'une sous–représentation de $(W, \chi_V \cdot \rho)$,

c'est-à-dire un sous-espace vectoriel stable pour l'action correspondante de G, est une sous–représentation de (W, ρ), donc $\{0\}$ ou W.

Exercice 715

Soit C le cube de l'espace euclidien $\mathbb{R}^3$ dont les huit sommets ont pour coordonnées $(\pm 1, \pm 1, \pm 1)$. Soit G le groupe des isométries de $\mathbb{R}^3$ qui laissent stable le cube, *i.e.* permutent ses huit sommets. Soit T le tétraèdre de sommets $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$.

a) Montrer que C est réunion de T et de τT, où $\tau = -\mathrm{id}$.

b) Soit $S(T)$ le groupe des isométries de T. Montrer que G est produit direct de $S(T) \simeq \mathfrak{S}_4$ et de $\{\mathrm{id}, \tau\}$.

c) Montrer que G a deux fois plus de caractères irréductibles que $\mathfrak{S}_4$.

d) Décrire les caractères irréductibles de G et écrire sa table de caractères.

Éléments de réponse 715

Exercice 716

Soit G un groupe abélien infini. Soit p un nombre premier ; supposons que tout élément x de G vérifie $x^p = 1$.

a) Soit n un entier positif. Montrer que si $\Bbbk$ est un corps de caractéristique différente de p, alors G ne peut pas être un sous-groupe de $\mathrm{GL}(n, \Bbbk)$.

b) Soit $\Bbbk$ un corps quelconque. Montrer que le groupe infini $\mathbb{Z}/2\mathbb{Z}^{\mathbb{N}} \times \mathbb{Z}/3\mathbb{Z}^{\mathbb{N}}$ n'admet pas de représentation linéaire fidèle de dimension finie sur $\Bbbk$.

Éléments de réponse 716

1.20. À classer

Exercice 717 Soit G un groupe fini dont tout sous-groupe propre est cyclique.

1. G est-il nécessairement cyclique, abélien ?
2. Si G est de plus supposé abélien, G est-il cyclique ?

Éléments de réponse 717

1. La réponse est négative. Par exemple le groupe $\mathrm{G} = \mathfrak{S}_3$ n'est pas abélien et ses sous-groupes propres, qui sont d'ordre 2 ou 3, sont cycliques. Autre exemple : le groupe des quaternions est non abélien et ses sous-groupes propres sont $\langle -1 \rangle$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$.
2. La réponse est négative. Ainsi le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ où p est premier a tous ses éléments non nuls d'ordre p et n'est donc pas cyclique. Cependant ses sous-groupes sont d'ordre 1 ou p et sont donc cycliques.

Exercice 718 Soit $n \in \mathbb{N}^*$ un entier. Soit G un groupe d'ordre n. Soit p un diviseur premier de n.

1. Montrer que G a au plus $\frac{n-1}{p-1}$ sous-groupes d'ordre p.
2. Donner un exemple où on a exactement $\frac{n-1}{p-1}$ sous-groupes d'ordre p.

Éléments de réponse 718

1. Soient H et K deux sous-groupes d'ordre p de G. Si $\mathrm{H} \cap \mathrm{K} \neq \{1\}$, alors il existe $x \in \mathrm{H} \cap \mathrm{K}$ tel que $x \neq 1$; en particulier x est d'ordre > 1. D'après le Théorème de Lagrange l'ordre de x divise $|\mathrm{H}| = |\mathrm{K}| = p$. Comme p est premier x est donc nécessairement d'ordre p et $\mathrm{H} = \mathrm{K} = \langle x \rangle$. Ainsi deux sous-groupes d'ordre p de G sont soit égaux, soit ont pour seul élément commun l'élément neutre 1. Notons k le nombre de sous-groupes d'ordre p de G et soient H_1, H_2, …, H_k les k sous-groupes d'ordre p (distincts) de G. Posons $A_i = \mathrm{H}_i \smallsetminus \{e\}$. Nous avons l'inclusion de l'union disjointe suivante dans G :
$$\{1\} \sqcup \bigsqcup_{i=1}^{k} A_i \subset \mathrm{G}$$
d'où
$$|\{1\}| + \sum_{i=1}^{k} |A_i| \leq |\mathrm{G}|.$$
Mais $|\mathrm{G}| = n$, $|A_i| = |\mathrm{H}| - 1 = p - 1$ donc $1 + \sum_{i=1}^{k}(p-1) \leq n$ soit $1 + k(p-1) \leq n$ ou encore $k \leq \frac{n-1}{p-1}$.
2. Considérons le groupe $\mathrm{G} = \mathbb{Z}/p\mathbb{Z}$; alors $n = p$ et $k = 1 = \frac{n-1}{p-1}$.

Exercice 719 Soit $n \in \mathbb{N}^*$.

1. Donner un élément d'ordre n de $\mathfrak{S}_n$.
2. Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$ un sous-groupe distingué de $\mathfrak{S}_n$ contenant une transposition. Montrer que $\mathrm{H} = \mathfrak{S}_n$.

Éléments de réponse 719

1. Soit σ l'élément défini par $\sigma(i) = i + 1$ pour tout $1 \leq i \leq n-1$ et $\sigma(n) = 1$. On vérifie par récurrence que $\sigma^k(1) = k + 1$ pour $1 \leq k \leq n-1$ et que $\sigma^n = \mathrm{id}$. Ainsi $\sigma^k \neq \mathrm{id}$ pour $1 \leq k \leq n-1$ et $\sigma^n = \mathrm{id}$; autrement dit σ est d'ordre n.
2. Si H contient une transposition τ_{ij} et si τ est une autre transposition, alors il existe un élément g dans $\mathfrak{S}_n$ tel que $\tau = g\tau_{ij}g^{-1}$ et H étant distingué dans G, $g\tau_{ij}g^{-1}$ appartient à H, *i.e.* τ appartient à H. Ainsi H contient toutes les transpositions.

   Il en résulte que H contient donc aussi le sous-groupe engendré par toutes les transpositions. Mais les transpositions engendrent $\mathfrak{S}_n$. Par suite $\mathrm{H} = \mathfrak{S}_n$.

Exercice 720 Pour tout entier $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple. Dans l'exercice qui suit nous montrons que parmi les groupes à 60 éléments la simplicité caractérise $\mathcal{A}_5$.

Soit G un groupe simple à 60 éléments. Nous allons montrer que G est isomorphe à $\mathcal{A}_5$.

1. Montrer que le groupe $\mathcal{A}_5$ est simple (Indication : penser à dénombrer).
2. Montrer que G possède exactement six sous-groupes d'ordre 5.
3. Désignons par X l'ensemble des 5-Sylow de G. Construire un morphisme injectif φ de G dans le groupe des permutations de X.
4. Montrer que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$ (où $\mathcal{A}_X$ désigne l'ensemble des permutations de X de signature 1).
5. Notons $E = \mathcal{A}_X/\varphi(\mathrm{G})$ l'ensemble des classes à gauche. On définit un morphisme ψ de $\mathcal{A}_X$ dans $\mathfrak{S}_E$ de la manière suivante

$$\begin{array}{rcl} \psi\colon \mathcal{A}_X & \to & \mathfrak{S}_E \\ x & \mapsto & \psi_x\colon E \to E \\ & & a\varphi(\mathrm{G}) \mapsto xa\varphi(\mathrm{G}) \end{array}$$

Montrer que ψ est injectif. Conclure que G est isomorphe à $\mathcal{A}_5$.

Éléments de réponse 720

1. Cette question se résout par dénombrement. Le groupe $\mathcal{A}_5$ possède
   - ◇ un élément d'ordre 1 (l'élément neutre),
   - ◇ quinze éléments d'ordre 2 (ce sont les produits de deux transpositions à supports disjoints),
   - ◇ vingt éléments d'ordre 3 (les 3-cycles),
   - ◇ vingt-quatre éléments d'ordre 5 (les autres).

   Si σ appartient à $\mathfrak{S}_5$ et si $(a_1\ a_2\ \ldots\ a_k)$ est un cycle, on a alors la formule suivante

$$\sigma(a_1\ a_2\ \ldots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)).$$

   On en déduit que tous éléments d'ordre 2 sont conjugués dans $\mathcal{A}_5$ et qu'il en est de même pour les 3-cycles. Ainsi si G est un sous-groupe distingué dans $\mathcal{A}_5$ et s'il contient un élément d'ordre 2, il les contient tous. Il en est de même pour les éléments d'ordre 3. Finalement s'il contient un élément d'ordre 5, alors il contient le 5-Sylow qu'il engendre. Comme tous les 5-Sylow sont conjugués, il contient tous les éléments d'ordre 5. Pour conclure il suffit maintenant de remarquer qu'aucune somme d'au moins deux entiers distincts pris parmi 1, 15, 20 ou 24 ne divise l'entier 60 (sauf 60). Le groupe $\mathcal{A}_5$ est donc simple.

2. On décompose 60 en facteurs premiers : $60 = 2^2 \times 3 \times 5$. Soit n_5 le nombre de 5-Sylow. D'une part $n_5 \equiv 1 \bmod 5$, d'autre part $n_5 | 60$ (car G agit transitivement sur les 5-Sylow par conjugaison). Comme G est simple, $n_5 \neq 1$ (en effet si n_5 alors G contient un unique 5-Sylow qui est distingué dans G). Il en résulte que $n_5 = 6$.

3. On peut faire agir G sur X par conjugaison ce qui induit un morphisme $\varphi\colon \mathrm{G} \to \mathfrak{S}_X$ défini de la manière suivante :

$$\begin{array}{rcl} \varphi\colon \mathrm{G} & \to & \mathfrak{S}_X \\ g & \mapsto & \varphi_g\colon X \to X \\ & & \qquad S \mapsto \varphi(g)(S) = gSg^{-1} \end{array}$$

   Ce morphisme n'est pas trivial car les 5-Sylow sont conjugués. L'action de G sur X est donc transitive. Comme G est simple, le noyau de φ doit être trivial. Par conséquent φ est bien injectif.

4. Soit H un groupe. Notons $D(\mathrm{H})$ son groupe dérivé. En passant au groupe dérivé l'inclusion $\varphi(\mathrm{G}) \subset \mathfrak{S}_X$ nous obtenons

$$D(\varphi(\mathrm{G})) \subset D(\mathfrak{S}_X) = \mathcal{A}_X.$$

   Comme G est simple il en est de même pour $\varphi(\mathrm{G})$. De plus $\varphi(\mathrm{G})$ possède aussi six 5-Sylow et donc n'est pas abélien. On en déduit alors $D(\varphi(\mathrm{G})) = \varphi(\mathrm{G})$ (le sous-groupe dérivé est toujours distingué). On a bien montré que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$.

5. Si x appartient à $\ker\psi$, alors $x\varphi(\mathrm{G}) = \varphi(\mathrm{G})$; ainsi x appartient à $\varphi(\mathrm{G})$ et $\ker\psi \subset \varphi(\mathrm{G})$. Le morphisme ψ ne peut donc pas être trivial pour des raisons de cardinalité (la partie $\varphi(\mathrm{G})$ est strictement contenue dans $\mathcal{A}_X$ de cardinal 360). Puisque $\mathcal{A}_X \simeq \mathcal{A}_6$ est simple on en déduit que ψ est injectif.

   Comme précédemment, en passant aux sous-groupes dérivés on sait également que $\psi(\varphi(\mathrm{G})) \subset \mathcal{A}_E$. Finalement on remarque que

$$\forall\, x \in \varphi(\mathrm{G}) \qquad \psi(x)(\varphi(\mathrm{G})) = x\varphi(\mathrm{G}) = \varphi(\mathrm{G}).$$

   Ainsi l'image de ψ est incluse dans le groupe des permutations de E qui fixent $\varphi(\mathrm{G}) \in E$. On note A le sous-groupe de $\mathcal{A}_E$ formé de telles permutations. Comme de plus E possède six éléments, $A \simeq \mathcal{A}_5$ et, pour des raisons de cardinalité, ψ est un bien isomorphisme de $\varphi(\mathrm{G})$ sur A. Nous avons donc montré que $\mathrm{G} \simeq \mathcal{A}_5$.

Exercice 721

1. Lemme de Cauchy. Soit G un groupe fini ; notons e son élément neutre. Soit p un nombre premier qui divise $|\mathrm{G}|$. Définissons l'ensemble

$$E = \{(x_1, x_2, \ldots, x_p) \in \mathrm{G}^p \,|\, x_1x_2\ldots x_p = e\}$$

   En faisant agit $\mathbb{Z}/p\mathbb{Z}$ sur E montrer que G possède un élément d'ordre p.

Supposons jusqu'à la fin de l'exercice que Aut(G) agit transitivement sur l'ensemble $\mathrm{G} \setminus \{e\}$.

2. Montrer que G est un p-groupe, c'est-à-dire qu'il existe un entier naturel n tel que $|\mathrm{G}| = p^n$.
3. Montrer que le centre de G est non trivial.
4. Conclure que $\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

Éléments de réponse 721

1. Soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$, *i.e.* $(x_2, x_3, \ldots, x_p, x_1)$ appartient à E. Notons c le cycle $(1\ 2\ \ldots\ p)$ de $\mathfrak{S}_p$. Il s'agit d'un élément d'ordre p qui engendre un sous-groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Nous définissons une opération de K sur l'ensemble G^p par

$$c \cdot (x_1, x_2, \ldots, x_p) = (x_{c(1)}, x_{c(2)}, \ldots, x_{c(p)}) = (x_2, x_3, \ldots, x_p, x_1).$$

La remarque ci-dessus montre que E est stable par cette opération.

Si x appartient à E, nous notons $\mathcal{O}(x)$ l'orbite de x sous l'action de G. Les éléments de E^{K} sont exactement les éléments x de E tels que $\mathcal{O}(x) = \{x\}$. Notons ω_1, ω_2, …, ω_r les orbites de E de cardinal strictement supérieur à 1. Si x_i est un élément de ω_i, alors $|\omega_i| = [\mathrm{G} : \mathrm{G}_{x_i}]$, c'est donc une puissance de p. Il résulte de l'équation aux classes que

$$|E| = |E^{\mathrm{K}}| + \sum_{i=1}^{r} |\omega_i| \equiv |E^{\mathrm{K}}| \mod p$$

Nous avons $|E| \equiv |E^{\mathrm{K}}| \mod p$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, …, x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n, $|E^{\mathrm{K}}|$ est nul modulo p. Or les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Notons que E^{K} contient le p-uplet $(e, e, \ldots, e)$; en particulier E^{K} est non vide et par suite le cardinal de E^{K} est supérieur à p. Il y a donc au moins $(p-1)$ éléments d'ordre p dans G.

2. Soit x un élément d'ordre p (l'existence d'un tel élément est assuré par le Lemme de Cauchy que nous venons de redémontrer). Soit $y \in \mathrm{G} \setminus \{e\}$. Par hypothèse il existe un automorphisme φ de G tel que $\varphi(x) = y$. On en déduit que

$$y^p = \varphi(x)^p = \varphi(x^p) = \varphi(e) = e$$

ce qui prouve que y est d'ordre p. On vient de montrer que p est le seul nombre premier qui divise $|\mathrm{G}|$. En effet si q en est un autre, il existe d'après la question précédente un élément d'ordre q et nécessairement $q = p$. Il existe donc un entier n tel que $|\mathrm{G}| = p^n$.

3. Faisons agir G sur lui-même par conjugaison, *i.e.* considérons l'action donnée par l'application $(g_1, g_2) \mapsto g_1 g_2 g_1^{-1}$. En reprenant les notations utilisées précédemment l'équation aux classes s'écrit
$$p^n = |\mathrm{G}| = |\mathrm{G}^{\mathrm{G}}| + \sum_{x \in A} |\mathcal{O}(x)|$$
où G^{G} est l'ensemble des éléments de G laissés fixes par l'action de G et A est un système de représentants de chaque orbite non trivial. Remarquons que $\mathrm{G}^{\mathrm{G}} = Z(\mathrm{G})$. Autrement dit
$$p^n = |\mathrm{G}| = |Z(\mathrm{G})| + \sum_{x \in A} \frac{|\mathrm{G}|}{|\mathrm{G}_x|} = |Z(\mathrm{G})| + \sum_{x \in A} \frac{|p^n|}{|\mathrm{G}_x|}$$
ou encore
$$|Z(\mathrm{G})| = p^n - \sum_{x \in A} \frac{|p^n|}{|\mathrm{G}_x|}.$$
Ceci entraîne que p divise $|Z(\mathrm{G})|$ et donc $|Z(\mathrm{G})| \neq 1$.

4. Soit g un élément de $Z(\mathrm{G}) \setminus \{e\}$ et soit g' un élément de $\mathrm{G} \setminus \{e\}$. Par hypothèse il existe un automorphisme φ de G tel que $\varphi(g) = g'$. Par suite
$$\forall\, h \in \mathrm{G} \qquad g'h = \varphi(g\varphi^{-1}h) = \varphi(\varphi^{-1}hg) = hg'$$
ce qui prouve que g' appartient au centre de G et donc que G est abélien. Si on note $+$ la loi de groupe de G on vérifie que l'action de $\mathbb{Z}/p\mathbb{Z}$ sur G (bien) définie par
$$\overline{k} \cdot g = \underbrace{g + g + \ldots + g}_{k \text{ termes}}$$
munit alors $(\mathrm{G}, +, \cdot)$ d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Sa dimension est donc nécessairement n et
$$\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n.$$

Exercice 722

Soit G un groupe fini dont tout sous-groupe propre est cyclique.

1. G est-il nécessairement cyclique, abélien ?
2. Si G est de plus supposé abélien, G est-il cyclique ?

Éléments de réponse 722

Exercice 723 Soit $n \in \mathbb{N}^*$ un entier. Soit G un groupe d'ordre n. Soit p un diviseur premier de n.

1. Montrer que G a au plus $\frac{n-1}{p-1}$ sous-groupes d'ordre p.
2. Donner un exemple où on a exactement $\frac{n-1}{p-1}$ sous-groupes d'ordre p.

Éléments de réponse 723

Exercice 724 Soit $n \in \mathbb{N}^*$.

1. Donner un élément d'ordre n de $\mathfrak{S}_n$.
2. Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$ un sous-groupe distingué de $\mathfrak{S}_n$ contenant une transposition. Montrer que $\mathrm{H} = \mathfrak{S}_n$.

Éléments de réponse 724

Exercice 725 Pour tout entier $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple. Dans l'exercice qui suit nous montrons que parmi les groupes à 60 éléments la simplicité caractérise $\mathcal{A}_5$.

Soit G un groupe simple à 60 éléments. Nous allons montrer que G est isomorphe à $\mathcal{A}_5$.

1. Montrer que le groupe $\mathcal{A}_5$ est simple (Indication : penser à dénombrer).
2. Montrer que G possède exactement six sous-groupes d'ordre 5.
3. Désignons par X l'ensemble des 5-Sylow de G. Construire un morphisme injectif φ de G dans le groupe des permutations de X.
4. Montrer que $\varphi(\mathrm{G}) \subset \mathcal{A}_X$ (où $\mathcal{A}_X$ désigne l'ensemble des permutations de X de signature 1).
5. Notons $E = {}^{\mathcal{A}_X}\!/_{\varphi(\mathrm{G})}$ l'ensemble des classes à gauche. On définit un morphisme ψ de $\mathcal{A}_X$ dans $\mathfrak{S}_E$ de la manière suivante

$$\begin{array}{rcl} \psi\colon \mathcal{A}_X & \to & \mathfrak{S}_E \\ x & \mapsto & \psi_x\colon E \to E \\ & & a\varphi(\mathrm{G}) \mapsto xa\varphi(\mathrm{G}) \end{array}$$

Montrer que ψ est injectif. Conclure que G est isomorphe à $\mathcal{A}_5$.

Éléments de réponse 725

Exercice 726

1. Lemme de Cauchy. Soit G un groupe fini ; notons e son élément neutre. Soit p un nombre premier qui divise $|\mathrm{G}|$. Définissons l'ensemble

$$E = \{(x_1, x_2, \ldots, x_p) \in \mathrm{G}^p \mid x_1x_2\ldots x_p = e\}.$$

En faisant agit ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ sur E montrer que G possède un élément d'ordre p.

Supposons jusqu'à la fin de l'exercice que $\mathrm{Aut}(\mathrm{G})$ agit transitivement sur l'ensemble $\mathrm{G} \smallsetminus \{e\}$.

2. Montrer que G est un p-groupe, c'est-à-dire qu'il existe un entier naturel n tel que $|\mathrm{G}| = p^n$.

3. Montrer que le centre de G est non trivial.
4. Conclure que $G \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

Éléments de réponse 726

CHAPITRE 2

EXERCICES, GROUPES ET GÉOMÉTRIE

2.1. Groupes et géométrie

Exercice 727

Montrer que le groupe affine $\mathrm{GA}(\mathcal{E})$ de l'espace affine dont l'espace vectoriel associé est E est isomorphe à un produit semi-direct de E et $\mathrm{GL}(E)$.

Éléments de réponse 727

Fixons un point O de $\mathcal{E}$. Soit $\mathrm{GA}_O(\mathcal{E})$ le sous-groupe de $\mathrm{GA}(\mathcal{E})$ formé des transformations affines qui laissent fixe le point O.

Soit $\mathrm{T}(\mathcal{E})$ le groupe des translations.

Le groupe $\mathrm{T}(\mathcal{E})$ est distingué dans $\mathrm{GA}(\mathcal{E})$. En effet soit $f \in \mathrm{GA}(\mathcal{E})$ une transformation affine ; notons $\overrightarrow{f}$ sa partie linéaire. Pour tout point M de $\mathcal{E}$ nous avons

$$f(M + \overrightarrow{u}) = f(M) + \overrightarrow{f}(\overrightarrow{u})$$

i.e.

$$(f \circ t_{\overrightarrow{u}})(M) = (t_{\overrightarrow{f}(\overrightarrow{u})} \circ f)(M)$$

ou encore

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f}(\overrightarrow{u})}.$$

Notons qu'une translation qui laisse fixe un point est égale à l'identité ; autrement dit $\mathrm{T}(\mathcal{E}) \cap \mathrm{GA}_O(\mathcal{E}) = \{\mathrm{id}\}$.

Enfin toute transformation affine est composée d'une transformation affine laissant fixe le point O et d'une translation, c'est-à-dire $\mathrm{T}(\mathcal{E})\mathrm{GA}_O(\mathcal{E}) = \mathrm{GA}(\mathcal{E})$. En effet une transformation affine $f \in \mathrm{GA}(\mathcal{E})$ s'écrit

$$f = t_{\overrightarrow{Of(O)}} \circ \left(t_{\overrightarrow{f(O)O}} \circ f \right)$$

et $t_{\overrightarrow{f(O)O}} \circ f$ laisse fixe le point O.

Le groupe $\mathrm{GA}(\mathcal{E})$ est donc le produit semi-direct du sous-groupe des translations par le sous-groupe laissant fixe O. [1]

Observons maintenant que l'action du sous-groupe $\mathrm{GA}_O(\mathcal{E})$ sur le sous-groupe distingué $\mathrm{T}(\mathcal{E})$ est donnée par la formule

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f}(\overrightarrow{u})}$$

Comme $\mathrm{T}(\mathcal{E})$ est isomorphe à E et comme $\mathrm{GA}_O(\mathcal{E})$ est isomorphe à $\mathrm{GL}(E)$ via l'application $f \mapsto \overrightarrow{f}$ nous avons

$$\mathrm{GA}(\mathcal{E}) \simeq E \rtimes_\rho \mathrm{GL}(E)$$

où $\rho(f) = \overrightarrow{f}$. Le produit de deux éléments de ce produit semi-direct

$$(\overrightarrow{u}, f)(\overrightarrow{v}, g) = (\overrightarrow{u} + f(\overrightarrow{v}), fg).$$

Exercice 728

Déterminer la composée de deux symétries vectorielles orthogonales planes.

Déterminer l'ordre de cette composée.

Éléments de réponse 728

Le déterminant d'une symétrie orthogonale est -1 ; la composée $r = s's$ de deux telles symétries s et s' est donc une isométrie directe, c'est-à-dire une rotation.

Déterminons l'angle θ de la rotation à partir des axes respectifs $\mathbb{R}\overrightarrow{u}$ et $\mathbb{R}\overrightarrow{u'}$ ($\overrightarrow{u}$ et $\overrightarrow{u'}$ unitaires) des symétries s et s'. Pour cela il suffit de déterminer l'image de $\overrightarrow{u}$ par r, ou plutôt l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$. Puisque $s(\overrightarrow{u}) = \overrightarrow{u}$ nous avons $r(\overrightarrow{u}) = s'(\overrightarrow{u})$ donc l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$ est aussi l'angle $(\overrightarrow{u}, s'(\overrightarrow{u}))$. Comme une symétrie renverse l'orientation nous avons

$$(\overrightarrow{u}, \overrightarrow{u'}) = -(s'(\overrightarrow{u}), s'(\overrightarrow{u'}))$$

d'où

$$(\overrightarrow{u}, \overrightarrow{u'}) = (s'(\overrightarrow{u'}), s'(\overrightarrow{u})).$$

Puisque $\overrightarrow{u'}$ appartient à l'axe de s' nous obtenons

$$(\overrightarrow{u}, \overrightarrow{u'}) = (\overrightarrow{u'}, s'(\overrightarrow{u})).$$

Il en résulte que

$$\theta = (\overrightarrow{u}, s'(\overrightarrow{u})) = (\overrightarrow{u}, \overrightarrow{u'}) + (\overrightarrow{u'}, s'(\overrightarrow{u})) = 2(\overrightarrow{u}, \overrightarrow{u'})$$

Notons que $\overrightarrow{u}$ peut être remplacé par $-\overrightarrow{u}$ ou $\overrightarrow{u'}$ par $-\overrightarrow{u'}$. L'angle $(\overrightarrow{u}, \overrightarrow{u'})$ n'est donc défini qu'à π près à partir de la donnée des deux symétries (ce n'est pas étonnant : la seule donnée

1. Soit G un groupe. Soient N et H deux sous-groupes de G tels que

- $\mathrm{N} \triangleleft \mathrm{G}$,
- $\mathrm{N} \cap \mathrm{H} = \{e\}$,
- $\mathrm{G} = \mathrm{NH}$.

Alors $\mathrm{G} \simeq \mathrm{N} \rtimes \mathrm{H}$.

intrinsèque est l'angle de droites $(\mathbb{R}\overrightarrow{u}, \mathbb{R}\overrightarrow{u'})$). Mais grâce à la multiplication par 2 l'angle θ se trouve être bien défini à 2π près.

Déterminons l'ordre de cette composée. L'ordre d'une rotation est infini si l'angle de la rotation n'est pas égal à $\frac{2k\pi}{n}$ pour n et k entiers. L'ordre de la rotation d'angle $\frac{2k\pi}{n}$ pour n et k premiers entre eux est n.

Exercice 729

Montrer que toute rotation plane se décompose en le produit de deux symétries.

Que pouvons-nous dire pour les rotations de l'espace ?

Éléments de réponse 729

Montrons que toute rotation plane se décompose en le produit de deux symétries.

D'après l'exercice précédent on peut décomposer toute rotation plane d'angle θ en le produit de deux symétries orthogonales : l'axe de la première est choisi au hasard, l'axe de la seconde fait un angle de $\frac{\theta}{2}$ avec la première.

Il y a un résultat analogue pour une rotation de l'espace d'axe $\mathbb{R}u$ et d'angle θ. Elle se décompose en le produit de deux symétries orthogonales par rapport à deux plans vectoriels contenant $\mathbb{R}u$ et qui font un angle égal à $\frac{\theta}{2}$ entre eux : la restriction de la rotation au plan vectoriel orthogonal à $\mathbb{R}u$ est une rotation plane.

Exercice 730 [Le groupe diédral]

Considérons un polygone régulier ayant un sommet P de coordonnées $(1, 0)$ et centré à l'origine du repère.

1. Déterminer le groupe D_6 des isométries du plan qui conservent un triangle équilatéral. Établir la table de D_6.
2. Déterminer le groupe D_8 des isométries du plan qui conservent carré. Déterminer les ordres des éléments de D_8. Établir la table de D_8.
3. Déterminer le groupe D_{2n} des isométries du plan qui conservent un polygone régulier à n côtés.
4. Soit $n \geq 2$ un entier. Considérons le groupe $\mathbb{Z}/n\mathbb{Z}$ et un générateur $[a]$ de ce groupe. Soit $\tau \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par $\tau([c]) = -[c]$.

   Soit $\rho\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par

   $$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

   Montrer que D_{2n} est isomorphe au produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ le long de ρ.

Éléments de réponse 730

Notons O l'origine de $\mathbb{R}^2$. Munissons $\mathbb{R}^2$ de l'orientation géométrique.

1. Commençons par déterminer les isométries (*i.e.* les symétries axiales et les rotations centrées en O) qui fixent un des sommets du triangle équilatéral. En dehors de l'identité il y a la symétrie d'axe la médiane issue du sommet considéré. Comme il y a trois sommets on obtient ainsi trois symétries dans D_6.

   Par ailleurs il y a les deux rotations centrées en O d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$.

   En ajoutant l'identité cela fait déjà 6 éléments dans D_6. Or une isométrie affine qui conserve le triangle équilatéral induit une permutation sur l'ensemble des sommets du triangle équilatéral qui sont au nombre de trois. Par suite D_6 est un sous-groupe de $\mathfrak{S}_3$.

   Il y a $3! = 6$ permutations de ces trois sommets donc $\mathrm{D}_6 \simeq \mathfrak{S}_3$ et nous avons listé tous les éléments de D_6.

   Désignons par A_1, A_2 et A_3 les sommets du triangle équilatéral. Pour $1 \leq i \leq 3$ notons s_i la symétrie qui laisse le point A_i fixe, r_1 la rotation d'angle $\frac{2\pi}{3}$ et $r_2^2 = r_1$ la rotation d'angle $\frac{4\pi}{3}$.

   La table de $\mathrm{D}_6 \simeq \mathfrak{S}_3$ est la suivante

	id	s_1	s_2	s_3	r_1	r_2
id	id	s_1	s_2	s_3	r_1	r_2
s_1	s_1	id	r_1	r_2	s_2	s_3
s_2	s_2	r_2	id	r_1	s_1	s_3
s_3	s_3	r_1	r_2	id	s_2	s_1
r_1	r_1	s_3	s_1	s_2	r_2	id
r_2	r_2	s_2	s_3	s_1	id	r_1

2. Notons qu'une isométrie qui préserve un carré envoie chaque sommet sur un sommet, chaque côté sur un côté et chaque diagonale sur une diagonale.

   Déterminons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui laissent fixe le point A_1. De telles isométries laissent donc fixe la diagonale $[A_1, A_3]$ et donc le point A_3. Il n'y en a donc qu'une non triviale : la symétrie par rapport à cette diagonale.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_2. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$. Il en résulte que A_3 a pour image A_4. Il y a deux telles isométries

   - ◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_2]$ et $[A_3, A_4]$ qui envoie A_4 sur A_3 et A_2 sur A_1 ;
   - ◇ la rotation d'angle $\frac{3\pi}{2}$ qui envoie A_4 sur A_1 et A_2 sur A_3.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_4. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$; le point A_3 a donc pour image le point A_2. Il y en a donc deux :

   - ◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_4]$ et $[A_2, A_3]$ qui envoie A_4 sur A_1 et A_2 sur A_3 ;

◇ la rotation d'angle $\frac{\pi}{2}$ qui envoie A_4 sur A_3 et A_2 sur A_1.

Restent les isométries qui envoient A_1 sur A_3 en conservant le carré. La diagonale $[A_2, A_4]$ est alors préservée. Il y en a deux :

◇ la symétrie par rapport à la diagonale $[A_2, A_4]$;

◇ la rotation d'angle π.

Notations :

◇ r_1 la rotation d'angle $\frac{\pi}{2}$;

◇ r_2 la rotation d'angle π ;

◇ r_3 la rotation d'angle $\frac{3\pi}{2}$;

◇ s_{12} la symétrie d'axe la médiatrice de $[A_1, A_2]$;

◇ s_{23} la symétrie d'axe la médiatrice de $[A_2, A_3]$;

◇ s_{13} la symétrie d'axe la médiatrice de $[A_1, A_3]$;

◇ s_{24} la symétrie d'axe la médiatrice de $[A_2, A_4]$.

Chacune des symétries est d'ordre 2 ; r_1 et r_3 sont d'ordre 4 et r_2 est d'ordre 2.

La table de D_8 est

	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
id	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
r_1	r_1	r_2	r_3	id	s_{13}	s_{24}	s_{23}	s_{12}
r_2	r_2	r_3	id	r_1	s_{23}	s_{12}	s_{24}	s_{13}
r_3	r_3	id	r_1	r_2	s_{24}	s_{13}	s_{12}	s_{23}
s_{12}	s_{12}	s_{24}	s_{23}	s_{13}	id	r_2	r_3	r_1
s_{23}	s_{23}	s_{13}	s_{12}	s_{24}	r_2	id	r_1	r_3
s_{13}	s_{13}	s_{12}	s_{24}	s_{23}	r_1	r_3	id	r_2
s_{24}	s_{24}	s_{23}	s_{13}	s_{12}	r_3	r_1	r_2	id

3. Soit P un polygone régulier à n côtés. Numérotons les sommets de P_n dans le sens trigonométrique, il s'écrit $[A_1, A_2, \ldots, A_n]$.

Pour une isométrie conservant le polygone chaque sommet va sur un sommet, chaque côté va sur un côté donc si A_1 a pour image A_k alors A_2 a pour image soit A_{k-1} soit A_{k+1}. Dans le premier cas l'isométrie est une symétrie (car ce n'est pas un élément de $\mathrm{SO}(2, \mathbb{R})$), dans le second cas l'isométrie est une rotation d'angle $\frac{2k\pi}{n}$. Les axes de symétrie possibles sont

◇ si n est pair les droites déterminées par un sommet quelconque et le centre (il y en a $\frac{n}{2}$) et les droites déterminées par les médiatrices des côté (il y en a $\frac{n}{2}$) ;

◇ si n est impair, les droites déterminées par un sommet quelconque et le centre qui sont les droites déterminées par les médiatrices des côtés (il y en a n).

Soit r la rotation d'angle $\frac{2\pi}{n}$ et soit s l'une des symétries de D_{2n}. Le groupe D_{2n} est engendré par s et r.

4. Le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ est d'ordre $2n$. Si $\beta = ([0],[1])$ et $\alpha = ([1],[0])$, alors
   - ◇ $\beta^2 = ([0],[0])$ où $([0],[0])$ est l'élément neutre du produit semi-direct, *i.e.* β est d'ordre 2 ;
   - ◇ $\alpha^n = ([0],[0])$, *i.e.* α est d'ordre n ;
   - ◇ et

   $$\beta\alpha\beta^{-1} = ([0],[1])([1],[0])([0],[1]) = ([0],[1])([1],[1]) = ([n-1],[0]) = \alpha^{n-1}.$$

   En effet, rappel : soient N et H deux groupes. Soit Aut(N) le groupe des automorphismes de groupe de N. Soit $\varphi\colon \mathrm{H} \to \mathrm{Aut(N)}$ un morphisme qui définit une opération de H sur N par la formule $h \cdot n = \varphi(h)(n)$.

   On définit sur l'ensemble produit $\mathrm{N} \times \mathrm{H}$ une loi par

   $$(n,h)(n',h') = \big(n(h \cdot n'), hh'\big).$$

   Alors $\mathrm{N} \times \mathrm{H}$, muni de cette loi, est un groupe appelé *produit semi-direct* de N par H relativement à φ et noté $\mathrm{N} \rtimes_\varphi \mathrm{H}$ ou plus simplement $\mathrm{N} \rtimes \mathrm{H}$.

   Ici $\mathrm{H} = \mathbb{Z}/2\mathbb{Z}$, $\mathrm{N} = \mathbb{Z}/n\mathbb{Z}$ et $\varphi = \rho$. Par suite

   $$(n,h)(n',h') = \big(n + \rho(h)(n'), h + h'\big).$$

   et

   $$\begin{aligned}
   ([0],[1])([1],[0])([0],[1]) &= ([0],[1])([1] + \rho([0])([0]), [0]+[1]) \\
   &= ([0],[1])([1],[1]) \\
   &= ([0] + \rho([1])([1]), [1]+[1]) \\
   &= (\rho([1])([1]), [2]) \\
   &= ([0] + (-[1]), [0]) \\
   &= ([n-1],[0])
   \end{aligned}$$

   Nous avons

   $$\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} = \{e,\, \alpha,\, \ldots,\, \alpha^{n-1},\, \beta,\, \beta\alpha,\, \beta\alpha^2,\, \ldots,\, \beta\alpha^{n-1}\}.$$

   Rappelons que

   $$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id}\rangle.$$

   Soit φ le morphisme défini par

   $$\mathrm{D}_{2n} \to \mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \qquad \begin{cases} s \mapsto \beta \\ r \mapsto \alpha \end{cases}$$

   Par construction c'est un isomorphisme.

Exercice 731

Soit $\tau \in \mathrm{Aut}\Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big)$ défini par $\tau([a],[b]) = ([b],[a])$.

Soit $\rho\colon \mathbb{Z}\!\diagup_{2\mathbb{Z}} \to \mathrm{Aut}\Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big)$ défini par

$$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

Montrer que D_8 est isomorphe au produit semi-direct de $\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}$ et $\mathbb{Z}\!\diagup_{2\mathbb{Z}}$ le long de ρ.

Éléments de réponse 731

Décrivons le produit semi-direct

$$\mathrm{G} = \Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big) \rtimes_\rho \mathbb{Z}\!\diagup_{2\mathbb{Z}}$$

Le groupe G est engendré par $\beta = ([0],[0],[1])$ qui est d'ordre 2, $\alpha_1 = ([1],[0],[0])$ et $\alpha_2 = ([0],[1],[0])$. Nous avons $\beta\alpha_1 = \alpha_2\beta$, $\beta\alpha_2 = \alpha_1\beta$. En effet vérifions la première relation : d'une part

$$\begin{aligned}
\beta\alpha_1 &= ([0],[0],[1])([1],[0],[0]) \\
&= (([0],[0]) + \tau([1])([1],[0]),[1]+[0]) \\
&= (([0],[0]) + ([0],[1]),[1]+[0]) \\
&= ([0],[1],[1])
\end{aligned}$$

et d'autre part

$$\begin{aligned}
\alpha_2\beta &= ([0],[1],[0])([0],[0],[1]) \\
&= (([0],[1]) + \tau([0])([0],[0]),[0]+[1]) \\
&= (([0],[1]) + ([0],[0]),[0]+[1]) \\
&= ([0],[1],[1])
\end{aligned}$$

Le groupe G est d'ordre 8 et

$$\mathrm{G} = \{e,\ \alpha_1,\ \alpha_2,\ \alpha_1\alpha_2,\ \beta,\ \beta\alpha_1,\ \beta\alpha_2,\ \beta\alpha_1\alpha_2\}.$$

Isomorphisme entre D_8 et G : l'image d'un élément d'ordre 2 est d'ordre 2, l'image d'un élément d'ordre 4 est d'ordre 4. Les éléments d'ordre 4 de G sont $\beta\alpha_1$ et $\beta\alpha_2$. Soit φ le morphisme entre ces deux groupes qui envoie r sur $\beta\alpha_1$. Alors $\varphi(r^3) = \beta\alpha_2$ et $\varphi(r^2) = \alpha_1\alpha_2$. Prenons $\varphi(s) = \beta$. Nous pouvons vérifier qu'on a bien un isomorphisme.

Exercice 732

Déterminer le groupe des isométries du plan qui conservent un rectangle non carré.

Établir la table de ce groupe.

Éléments de réponse 732

Considérons un rectangle $ABCD$ tel que « A est le coin en haut à gauche, B le coin en haut à droite, C le coin en bas à droite, D le coin en bas à gauche, $[AB]$ et $[CD]$ sont les longueurs et $[BC]$ et $[AD]$ les largeurs ». Prenons pour origine du repère le centre du rectangle.

Une isométrie qui conserve le rectangle laisse fixe le centre du rectangle donc le groupe recherché est isomorphe à un sous-groupe du groupe des isométries vectorielles. Par ailleurs une isométrie qui conserve le rectangle envoie chaque diagonale sur une diagonale.

Une isométrie qui conserve le rectangle et laisse fixe le sommet A laisse fixe la diagonale $[AC]$ et donc le sommet C et tous les autres sommets. Ainsi la seule isométrie qui conserve le rectangle et laisse fixe le sommet A est l'identité. Il en est de même lorsque l'on remplace A par B (respectivement C, respectivement D). Une isométrie qui conserve le rectangle et qui n'est pas l'identité ne fixe donc aucun sommet.

- ◇ ou bien A a pour image B alors C a pour image D et cette isométrie est la symétrie s_1 d'axe la médiatrice de $[AB]$;
- ◇ ou bien A a pour image D, alors B a pour image C et cette isométrie est la symétrie s_2 d'axe la médiatrice de $[AD]$;
- ◇ ou bien A et C sont échangés et cette isométrie est la rotation r d'angle π.

On a donc un groupe d'ordre 4, abélien, dont la table est :

	id	s_1	s_2	r
id	id	s_1	s_2	r
s_1	s_1	id	r	s_2
s_2	s_2	r	id	s_1
r	r	s_2	s_1	id

Exercice 733

Quel est le centre de $\mathfrak{S}_3$? de D_8 ? de D_{12} ? de D_{4n} ?

Éléments de réponse 733

Rappelons que $\mathfrak{S}_3 \simeq \mathrm{D}_6$. Le centre de $\mathfrak{S}_3$ est trivial.

Considérons le groupe D_{4n}. Le centre de D_{4n} ne contient pas les rotations r_k d'angle $\frac{2k\pi}{2n} = \frac{k\pi}{n}$, pour $k \neq n$, car elles ne commutent pas avec les symétries.

Par contre le retournement r_0 donné par $k = n$ (*i.e.* la rotation d'angle π) commute avec tous les éléments de D_{4n} :

- avec les rotations de D_{4n} car l'ensemble des rotations est un sous-groupe cyclique de D_{4n} ;
- avec les symétries orthogonales car ce retournement est la composée de deux symétries orthogonales par rapport à des axes orthogonaux (r_0 s'écrit ss' avec s symétrie orthogonale de D_{4n} et s' la symétrie orthogonale d'axe orthogonal à celui de s ; d'une part $r_0 s = s'ss = s'$ et $sr_0 s = sss' = s'$).

Le centre de D_{4n} est donc $\{\mathrm{id}, r_0\}$.

Exercice 734

Soit $n \geq 3$; le sous-ensemble $\{g \in \mathrm{D}_{2n} \,|\, g^2 = \mathrm{id}\}$ de D_{2n} est-il un sous-groupe de D_{2n} ?

Éléments de réponse 734

La composée de deux symétries orthogonales éléments de D_{2n} est une rotation d'angle deux fois l'angle formé par les deux axes. Par suite dès que $n \geq 3$ l'un de ces produits au moins est d'ordre différent de 2. Ainsi l'ensemble des éléments d'ordre 2 de D_{2n} n'est pas un sous-groupe de D_{2n}.

Exercice 735

Quelle est la matrice de la rotation de $\mathbb{R}^3$ d'angle θ autour de l'axe $\mathbb{R}e_2$?

Éléments de réponse 735

Le vecteur e_2 est vecteur propre pour la valeur propre 1 de la matrice, *i.e.* c'est un vecteur fixe pour la rotation considérée.

L'image de e_1 est dans le plan (e_1, e_3) et est égale à $\cos\theta e_1 - \sin\theta e_3$.

L'image de e_3 est dans le plan (e_1, e_3) et est égale à $\sin\theta e_1 + \cos\theta e_3$.

La matrice cherchée est donc

$$\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$$

Exercice 736

Soit $M \in \mathrm{O}(3, \mathbb{R})$ de déterminant -1.

Montrer que -1 est valeur propre de M.

Éléments de réponse 736

Puisque une isométrie vectorielle conserve les normes, ses valeurs propres sont de module 1. Ceci est donc vrai pour une matrice M de $\mathrm{O}(3, \mathbb{R})$ qui est la matrice d'une isométrie vectorielle. Si de plus $\det M = -1$, alors le produit des racines du polynôme caractéristique de M est -1. Par suite

- ou bien toutes les racines du polynôme caractéristique de M sont réelles et dans ce cas l'une ou trois d'entre elles sont égales à -1 ;
- ou bien deux d'entre elles sont complexes conjuguées, leur produit étant égal à 1 la dernière est -1.

Exercice 737

Soit M une matrice orthogonale 2×2 et de déterminant -1.

Montrer que M est la matrice d'une symétrie orthogonale.

Éléments de réponse 737

Les racines du polynôme caractéristique de M sont de module 1. Si elles sont complexes conjuguées mais dans ce cas le déterminant de M est 1 : contradiction. Elles sont donc toutes les deux réelles, l'une valant 1 et l'autre -1.

Il s'en suit que M est la matrice de la symétrie orthogonale d'axe la droite vectorielle propre associée à la valeur propre 1.

Exercice 738

Soit $M \in \mathrm{SO}(3,\mathbb{R})$ la rotation d'angle θ. Montrer que

$$\cos\theta = \frac{1}{2}\Big(\mathrm{Tr}\, M - 1\Big).$$

Éléments de réponse 738

Si M est la matrice d'une rotation d'angle θ, alors M est semblable à la matrice

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Par suite $\mathrm{Tr}\, M = 2\cos\theta - 1$ et $\cos\theta = \frac{1}{2}\Big(\mathrm{Tr}\, M - 1\Big)$.

Exercice 739

Soit s une symétrie plane d'axe $\mathcal{D}$.

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrer que la composée $t \circ s$ (respectivement $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.
2. Soit r une rotation de centre C. Montrer que la composée $r \circ s$ (respectivement $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.
3. Soient s' et s'' deux symétries axiales. Montrer que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

Éléments de réponse 739

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrons que la composée $t \circ s$ (respectivement $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.

   Supposons $\overrightarrow{v}$ normal à $\mathcal{D}$. Soit $t'(\mathcal{D}') = \mathcal{D}'$ où t' est la translation de vecteur $\overrightarrow{v}/2$. La droite $\mathcal{D}'$ est une droite de points fixes par ts qui est donc la symétrie orthogonale d'axe $\mathcal{D}'$.

   Soit t'' la translation de vecteur $-\overrightarrow{v}/2$. Posons $\mathcal{D}'' = t''(\mathcal{D})$. La droite $\mathcal{D}''$ est une droite de points fixes par st qui est donc la symétrie orthogonale d'axe $\mathcal{D}''$.

   Si ts est une symétrie orthogonale s' et si A est un point de l'axe de symétrie, nous avons $ts(A) = A$ donc $\overrightarrow{s(A)A} = \overrightarrow{v}$. Par suite $\overrightarrow{v}$ est normal à la droite $\mathcal{D}$ et d'après ce qui précède st est une symétrie orthogonale.

Si st est une symétrie, nous arrivons à la même conclusion.

2. Soit r une rotation de centre C. Montrons que la composée $r \circ s$ (respectivement $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que C appartienne à $\mathcal{D}$. Soit θ l'angle de la rotation r. Considérons la rotation r' de centre C et d'angle $-\frac{\theta}{2}$. Alors $\mathcal{D}' = r'(\mathcal{D})$ est une droite de points fixes de $s \circ r$ qui est une symétrie d'axe $\mathcal{D}'$.

   Soit r'' la rotation de centre C et d'angle $\frac{\theta}{2}$. Alors $\mathcal{D}'' = r''(\mathcal{D})$ est une droite de points fixes de $r \circ s$ qui est une symétrie d'axe $\mathcal{D}''$.

   Réciproquement supposons que $r \circ s$ soit une symétrie orthogonale d'axe $\mathcal{D}'$. Soit C' l'intersection de $\mathcal{D}$ et $\mathcal{D}'$. Nous avons $rs(C') = C'$ ainsi que $s(C') = C'$. Par conséquent $C' = r(C')$ et C' est le centre de la rotation r, c'est-à-dire C qui est donc sur $\mathcal{D}$. Dans ce cas $s \circ r$ est aussi une symétrie orthogonale.

   La conclusion est identique en supposant a priori que $s \circ r$ est une symétrie.

3. Soient s' et s'' deux symétries axiales. Montrons que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient sécants en un point C. Alors $s' \circ s''$ est une rotation de centre C et d'après 2. $ss's''$ est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient parallèles alors $s' \circ s''$ est une translation de vecteur orthogonal à la direction commune et d'après 1. $ss's''$ est une symétrie si et seulement si cette direction commune est celle de $\mathcal{D}$.

Exercice 740

Montrer que pour une translation t de vecteur $\overrightarrow{u}$ et une symétrie s d'axe $\mathcal{D}$ nous avons $t \circ s = s \circ t$ si et seulement si $\overrightarrow{u}$ est dans la direction de $\mathcal{D}$.

Éléments de réponse 740

Si $st = ts$, alors pour tout point M de $\mathcal{D}$ nous avons $st(M) = ts(M) = t(M)$ donc $t(M)$ appartient à $\mathcal{D}$ et $\overrightarrow{u} = \overrightarrow{Mt(M)}$ est parallèle à $\mathcal{D}$.

Réciproquement supposons que $\overrightarrow{u}$ soit parallèle à $\mathcal{D}$. Posons $M' = ts(M)$ et $M'' = st(M)$. Nous avons $\overrightarrow{Ms(M)} = \overrightarrow{t(M)s(t(M))} = \overrightarrow{t(M)M''}$. Par conséquent $\overrightarrow{s(M)M''} = \overrightarrow{Mt(M)} = \overrightarrow{u}$ et donc $\overrightarrow{s(M)M''} = \overrightarrow{s(M)t(s(M))} = \overrightarrow{s(M)M'}$ $M'' = M'$. Il s'en suit que $st = ts$.

Exercice 741

Soit $\mathcal{R}$ le réseau plan des points à coordonnées entières dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$.

Quelles sont les isométries affines qui conservent $\mathcal{R}$?

Quelles sont les centres des rotations affines qui conservent $\mathcal{R}$?

Éléments de réponse 741

Si une isométrie affine qui conserve le réseau $\mathcal{R}$ a exactement un point fixe, c'est une rotation autour de l'un des points du réseau d'angle $\frac{k\pi}{2}$, ou une rotation d'angle $\frac{k\pi}{2}$ autour de l'un des centres des carrés du type $[O, A, B, C]$ où O est le centre du repère, A a pour coordonnées $(1, 0)$, B a pour coordonnées $(1, 1)$, C a pour coordonnées $(0, 1)$. Enfin il y a aussi les symétries centrales autour des milieux des segments du type OA, AB, BC et CO.

Si une isométrie affine qui conserve le réseau $\mathcal{R}$ a une droite de points fixes, alors c'est une symétrie orthogonale par rapport aux droites du type OA, AB, BC et CO (côtés des carrés du type $[O, A, B, C]$) ainsi que AC et OC (diagonales des carrés du type $[O, A, B, C]$) et des médiatrices des segments OA et AB.

Si une isométrie affine qui conserve le réseau $\mathcal{R}$ n'a pas de point fixe, alors soit c'est une translation de vecteur $\in \mathbb{Z}e_1 + \mathbb{Z}e_2$ (où (e_1, e_2) est la base canonique de $\mathbb{R}^2$), soit c'est un produit d'une translation de ce type avec les autres isométries affines déjà trouvées.

Exercice 742

Soit $\mathfrak{S}$ la représentation graphique dans un repère orthonormal de la fonction sinus.

Quelles sont les isométries affines qui conservent la figure $\mathfrak{S}$?

Éléments de réponse 742

La figure $\mathfrak{S}$ est conservée par la rotation de centre l'origine du repère et d'angle π, par les translations de vecteurs $2k\pi e_1$ pour $k \in \mathbb{Z}$ et par les composées de telles applications.

Exercice 743

Déterminer les isométries affines qui conservent l'ensemble $\mathfrak{F}$ des points de coordonnées $(n, 0)$, $n \in \mathbb{Z}$, dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$ du plan affine euclidien.

Éléments de réponse 743

La figure $\mathfrak{F}$ est l'ensemble des points à coordonnées entières de l'axe des abscisses. Elle est conservée par

- les rotations de centre les points de $\mathfrak{F}$ ou les milieux des segments joignant deux points de $\mathfrak{G}$ et d'angle π,
- la symétrie orthogonale par rapport à l'axe des x,
- la symétrie orthogonale par rapport à n'importe quelle droite verticale qui passe par des points de $\mathfrak{F}$ ou par le milieu du segment joignant deux points de $\mathfrak{F}$,
- toutes les translations de vecteur $\in \mathbb{Z}e_1$,
- les composées de telles applications.

Exercice 744

Notons $\mathrm{OA}(2, \mathbb{R})$ le groupe des déplacements de $\mathbb{R}^2$. Soit G un sous-groupe de $\mathrm{OA}(2, \mathbb{R})$ qui contient les rotations centrées en deux points distincts.

Montrer que G contient une translation.

Éléments de réponse 744

Toute rotation se décompose en une composée de deux symétries orthogonales. Soient A et B les deux points qui sont centres des rotations que G contient. Soit s la symétrie orthogonale d'axe (AB). Soit s_1 la symétrie orthogonale d'axe une droite quelconque $\mathcal{D}_1$ passant par A différente de (AB). Soit s_2 la symétrie orthogonale d'axe la droite $\mathcal{D}_2$ passant par B parallèle à $\mathcal{D}_1$.

Les rotations $s_1 s$ et $s s_2$ appartiennent à G ; par suite $(s_1 s)(s s_2)$ appartient à G, *i.e.* $s_1 s_2$ est dans G. Or la composée $s_1 s_2$ est une translation donc G contient une translation.

Exercice 745

Les actions considérées ci-après sont les actions naturelles.

1. Montrer que l'action de $\mathrm{GL}(n, \mathbb{R})$ sur $\mathbb{R}^n$ n'est pas transitive mais qu'elle définit sur l'ensemble des bases de $\mathbb{R}^n$ une action transitive.
2. Montrer que $\mathrm{SO}(2, \mathbb{R})$ agit transitivement sur le cercle unité de $\mathbb{R}^2$.
3. Montrer que $\mathrm{SO}(3, \mathbb{R})$ agit transitivement sur la sphère unitée de $\mathbb{R}^3$.

Éléments de réponse 745

1. Deux vecteurs quelconques de $\mathbb{R}^n$ sont dans la même orbite pour l'action de $\mathrm{GL}(n, \mathbb{R})$ sur $\mathbb{R}^n$ à condition qu'aucun des deux ne soit nul : l'orbite du vecteur nul est réduite à ce vecteur nul. L'action considérée n'est donc pas transitive.

   Par contre deux bases quelconques de $\mathbb{R}^n$ sont images l'une de l'autre par une unique application linéaire bijective. L'action de $\mathrm{GL}(n, \mathbb{R})$ sur l'ensemble des bases de $\mathbb{R}^n$ est donc transitive.
2. Deux vecteurs quelconques de $\mathbb{R}^2$ sont dans la même orbite pour l'action de $\mathrm{SO}(2, \mathbb{R})$ sur $\mathbb{R}^2$ à condition qu'ils aient même norme ; les éléments du cercle unité ont norme 1, par suite l'action de $\mathrm{SO}(2, \mathbb{R})$ est transitive sur le cercle unité.
3. Même chose qu'à la question précédente.

Exercice 746

Soit $n \geq 3$ un entier. Considérons les matrices suivantes de $\mathrm{GL}(2, \mathbb{R})$

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \tau = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

Notons G le sous-groupe de $\mathrm{GL}(2, \mathbb{R})$ engendré par σ et τ ; désignons par H le sous-groupe de G engendré par σ et K le sous-groupe de G engendré par τ :

$$\mathrm{G} = \langle \sigma, \tau \rangle, \qquad \mathrm{H} = \langle \sigma \rangle, \qquad \mathrm{K} = \langle \tau \rangle.$$

Posons $\mathrm{K}' = \{g \in \mathrm{G} \mid \det g = 1\}$ et définissons les vecteurs v_0 et Y_0 de $\mathbb{R}^2$ par

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad Y_0 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

1. Donner l'ordre de σ.
2. Donner une interprétation géométrique pour τ et donner son ordre.
3. Si G est d'ordre fini, que peut-on dire sur son ordre ?
4. Montrer que $\sigma\tau = \tau^{n-1}\sigma$.
5. Donner tous les éléments de H, K et G.
6. Combien y a-t-il de classes à gauche de G modulo H ?
7. Décrire G/H.
8. A-t-on $\mathrm{H} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient G/H.
9. A-t-on $\mathrm{K} \triangleleft \mathrm{G}$? Si oui décrire le groupe quotient G/K.
10. Le sous-ensemble K' de G est-il un sous-groupe de G ? Si oui, a-t-on $\mathrm{K}' \triangleleft \mathrm{G}$?
11. Comparer K et K'.
12. Existe-t-il un sous-groupe de G isomorphe à G/K ?
13. Calculer $D(\mathrm{G})$. À quel groupe est isomorphe $\mathrm{G}/D(\mathrm{G})$?
14. Montrer que la multiplication des matrices définit une action
$$\mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX$$
15. L'action est-elle transitive ?
16. L'action est-elle fidèle ?
17. Quels sont les points fixes de l'action ?
18. Quel est le stabilisateur G_{v_0} du vecteur v_0 ?
19. Décrire l'orbite du vecteur v_0.
20. Quel est le stabilisateur G_S du segment $S = [v_0, Y_0]$?

Éléments de réponse 746

1. Donnons l'ordre de σ.

   Nous avons $\sigma \neq \mathrm{id}$ mais $\sigma^2 = \mathrm{id}$ donc σ est d'ordre 2.

2. Donnons une interprétation géométrique pour τ et donnons son ordre.

   On voit que τ est la rotation de centre $O = (0, 0)$ et d'angle $\frac{2\pi}{n}$. En particulier τ est d'ordre n. On peut de plus déterminer τ^k :
$$\tau^k = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$

3. Si G est d'ordre fini, alors son ordre est divisible d'une part par 2 et d'autre part par n, donc par $\text{ppcm}(2, n)$.

4. Montrons que $\sigma\tau = \tau^{n-1}\sigma$. Un calcul direct assure que $\sigma\tau\sigma^{-1} = \tau^{-1}$:

$$\sigma\tau\sigma^{-1} = \sigma\tau\sigma = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(-\frac{2\pi}{n}\right) & -\sin\left(-\frac{2\pi}{n}\right) \\ \sin\left(-\frac{2\pi}{n}\right) & \cos\left(-\frac{2\pi}{n}\right) \end{pmatrix} = \tau^{-1}$$

   On en déduit, puisque τ est d'ordre n, que $\sigma\tau\sigma^{-1} = \tau^{n-1}$ puis que $\sigma\tau = \tau^{n-1}\sigma$.

5. Donnons tous les éléments de G, H et K.

   Puisque σ est d'ordre 2, nous avons $\text{H} = \{\text{id}, \sigma\}$.

   Comme τ est d'ordre n, nous avons $\text{K} = \{\text{id}, \tau, \tau^2, \ldots, \tau^{n-1}\}$.

   Nous avons $\text{G} = \{\text{id}, \tau, \tau^2, \ldots, \tau^{n-1}, \sigma, \tau\sigma, \tau^2\sigma, \ldots, \tau^{n-1}\sigma\}$. En effet remarquons que d'une part un élément de G s'écrit

$$(\sigma)\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}(\sigma)$$

   d'autre part $\sigma\tau\sigma^{-1} = \tau^{n-1}$ implique $\sigma\tau^{\ell}\sigma^{-1} = \tau^{\ell(n-1)}$ et $\sigma\tau^{\ell} = \tau^{\ell(n-1)}\sigma$. Montrons par exemple par récurrence qu'un élément de la forme $(\sigma)\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}(\sigma)$ avec k pair est de la forme τ^{ℓ} ou $\tau^{\ell}\sigma$:

   a) commençons par considérer un élément de la forme $\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair. Montrons par récurrence sur k qu'il s'écrit aussi τ^{κ} pour un certain κ. C'est vrai pour $k = 2$, en effet

$$\underbrace{\sigma\tau^{i_1}}_{\tau^{i_1(n-1)}\sigma}\sigma\tau^{i_2} = \tau^{i_1(n-1)}\sigma\sigma\tau^{i_2} = \tau^{i_1(n-1)}\tau^{i_2} = \tau^{i_1(n-1)+i_2}$$

   Soit k un entier pair. Supposons que la propriété soit vraie pour tout $j \leq k$ pair et montrons qu'alors elle est vraie pour $k + 2$

$$\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa_1}}\underbrace{\sigma\tau^{i_{k+1}}\sigma\tau^{i_{k+2}}}_{\tau^{\kappa_2}} = \tau^{\kappa_1}\tau^{\kappa_2} = \tau^{\kappa_1+\kappa_2}.$$

   La propriété est donc vraie pour tout k pair.

   b) considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}$ avec k pair, alors d'après a) il s'écrit $\tau^{\ell}\sigma$ pour un certain ℓ

$$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k} = \underbrace{\sigma\sigma}_{\text{id}}\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k} = \sigma\underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa}} = \sigma\tau^{\kappa} = \tau^{\kappa(n-1)}\sigma.$$

   c) considérons un élément de la forme $\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma$ avec k pair ; d'après b) il s'écrit $\tau^{\kappa}\sigma$ pour un certain κ :

$$\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}\sigma = \underbrace{\tau^{i_1}\sigma\tau^{i_2}\sigma\ldots\sigma\tau^{i_k}}_{\tau^{\kappa}\sigma}\sigma = \tau^{\kappa}\sigma\sigma = \tau^{\kappa}\underbrace{\sigma\sigma}_{\text{id}} = \tau^{\kappa}.$$

d) finalement considérons un élément de la forme $\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\dots\sigma\tau^{i_k}\sigma$ avec k pair ; d'après a) il s'écrit $\tau^\kappa\sigma$ pour un certain κ :

$$\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\dots\sigma\tau^{i_k}\sigma = \underbrace{\sigma\tau^{i_1}\sigma\tau^{i_2}\sigma\dots\sigma\tau^{i_k}}_{\tau^\kappa}\sigma = \tau^\kappa\sigma$$

Un raisonnement analogue permet de conclure lorsque k est impair.

6. Déterminons le nombre de classes à gauche de G modulo H.

   L'ensemble des classes à gauche de G modulo H est l'ensemble ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Son cardinal est $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| = [\mathrm{G} : \mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|}$. D'après la question précédente nous avons $|\mathrm{G}| = 2n$, $|\mathrm{H}| = 2$ et donc $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| = \frac{|\mathrm{G}|}{|\mathrm{H}|} = n$.

7. Décrivons ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

   Les descriptions de G et H nous permettent d'affirmer que

$$ {}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\overline{\mathrm{id}}, \overline{\tau}, \dots, \overline{\tau^{n-1}}\}.$$

8. Commençons par rappeler :

> Rappel : soient G un groupe et H un sous-groupe de G. Le groupe H est distingué dans G s'il est invariant par automorphisme intérieur, c'est-à-dire si
> $$\forall\, a \in \mathrm{G} \quad \forall\, h \in \mathrm{H} \quad aha^{-1} \in \mathrm{H}$$
> Si H est distingué dans G, nous notons $\mathrm{H} \triangleleft \mathrm{G}$.
> La condition ci-dessus équivaut à dire que pour tout $a \in \mathrm{G}$ nous avons $a\mathrm{H} = \mathrm{H}a$, *i.e.* l'égalité des classes à droite et des classes à gauche modulo H.

   Le sous-groupe H de G n'est pas distingué dans G ; en effet

$$\tau^{-1}\sigma\tau = \tau^{-1}\tau^{n-1}\sigma = \tau^{n-2}\sigma \notin \mathrm{H} \text{ (car par hypothèse } n \geq 3).$$

9. Commençons par rappeler

Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Alors H est un sous-groupe distingué de G.
Première méthode :
En effet, si g appartient à H, alors $g\mathrm{H} = \mathrm{H}g = \mathrm{H}$ (l'hypothèse indice 2 est inutile ici). Si g n'appartient pas à H, alors puisque H est d'indice 2 nous avons

$$\mathrm{G} = \mathrm{H} \cup g\mathrm{H} = \mathrm{H} \cup \mathrm{H}g.$$

On voit que $g\mathrm{H} = \mathrm{H}g = \mathrm{G} \setminus \mathrm{H}$; en particulier $g\mathrm{H} = \mathrm{H}g$, autrement dit H est distingué dans G.

Deuxième méthode :
Nous avons donc ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\mathrm{H},\, x\mathrm{H}\}$ où $x \notin \mathrm{H}$ et $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $\mathrm{H} \cap x\mathrm{H} = \emptyset$.
Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons

$$ghg^{-1} = xh_0hh_0^{-1}x^{-1} = xh'x^{-1}$$

où $h' = h_0hh_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à $x\mathrm{H}$, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

Nous avons $[\mathrm{G} : \mathrm{K}] = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{2n}{2} = 2$. Ainsi K est un sous-groupe d'indice 2 de G ; il est donc distingué dans G et ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ a une structure de groupe.

Le groupe quotient ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ est d'ordre 2 donc isomorphe à ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Nous avons ${}^{\mathrm{G}}\!/_{\mathrm{K}} = \{\overline{\mathrm{id}},\, \overline{\sigma}\}$.

10. Commençons par rappeler

Rappel : soient G et G′ deux groupes. Soit $f : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Alors le noyau $\ker f$ de f est un sous-groupe distingué de G.

L'application $\det : \mathrm{G} \to \mathbb{R}^*$ est un morphisme de groupes et K′ est son noyau. Ainsi K′ est un sous-groupe distingué de G.

11. Comparons K et K′.

Remarquons que $\det \tau^\ell = \cos^2\left(\frac{2\pi\ell}{n}\right) + \sin^2\left(\frac{2\pi\ell}{n}\right) = 1$ donc τ^ℓ appartient à K′. Ainsi $\mathrm{K} = \langle\tau\rangle \subset \mathrm{K}'$.

Soit $g \in \mathrm{G} \setminus \mathrm{K}$, alors g s'écrit $\tau^\ell\sigma$ avec $0 \leq \ell \leq n-1$ (cf 5.) d'où $\det g = \det(\tau^\ell\sigma) = \det(\tau^\ell)\det\sigma = 1 \times (-1) = -1$. Par suite g n'appartient pas à K′. Nous venons de montrer que si g n'appartient pas à K, alors g n'appartient pas à K′, autrement dit que si g appartient à K′, alors g appartient à K, *i.e.* $\mathrm{K}' \subset \mathrm{K}$.

12. Les groupes H et ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ sont d'ordre 2, donc sont isomorphes. Il en résulte qu'il existe un sous-groupe de G (le sous-groupe H) isomorphe à ${}^{\mathrm{G}}\!/_{\mathrm{K}}$.

13. Calculons $D(\mathrm{G})$.

> Rappel : le groupe dérivé de G, noté $D(\mathrm{G})$, est le sous-groupe engendré par les éléments de la forme $xyx^{-1}y^{-1}$ avec x, y dans G.
> Remarque : $D(\mathrm{G})$ est un sous-groupe distingué de G.
> Remarque : ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$. Autrement dit on peut définir le groupe dérivé $D(\mathrm{G})$ de G de la façon suivante : $D(\mathrm{G})$ est le sous-groupe de G tel que ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ soit le plus grand (au sens de l'inclusion) quotient abélien de G.

Le groupe G n'est pas abélien : $\sigma\tau = \tau^{n-1}\sigma \neq \tau\sigma$ car $n \neq 2$. Par conséquent $D(\mathrm{G}) \neq \{\mathrm{id}\}$.

De plus ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ est abélien (en effet d'après 9. le groupe ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ est isomorphe au groupe abélien ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$) ; ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ étant le plus grand quotient abélien $D(\mathrm{G}) \subset \mathrm{K}$.

Calculons $[\sigma, \tau]$:

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \tau^{-1}\tau^{-1} = \tau^{-2}$$

ainsi τ^{-2} appartient à $D(\mathrm{G})$ et τ^2 appartient à $D(\mathrm{G})$. Finalement $\langle\tau^2\rangle \subset D(\mathrm{G})$. Nous avons donc les inclusions

$$\langle\tau^2\rangle \subset D(\mathrm{G}) \subset \mathrm{K}.$$

Si n est impair, alors n est premier avec 2 et l'ordre de τ^2 est $\frac{n}{\mathrm{pgcd}(2,n)} = n$ donc $\langle\tau^2\rangle = \langle\tau\rangle$ et $\mathrm{K} = \langle\tau\rangle \subset D(\mathrm{G})$. Finalement $D(\mathrm{G}) = \mathrm{K} = \langle\tau\rangle = \langle\tau^2\rangle$. Dans ce cas nous avons ${}^{\mathrm{G}}\!/_{D(\mathrm{G})} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Si $n = 2m$ est pair, montrons que

$$D(\mathrm{G}) = \langle\tau^2\rangle = \{\mathrm{id}, \tau^2, \tau^4, \ldots, \tau^{n-2}\} = \{\mathrm{id}, \tau^2, \tau^4, \ldots, \tau^{2(m-1)}\}.$$

Nous avons vu que $\langle\tau^2\rangle \subset D(\mathrm{G})$. Montrons que $\langle\tau^2\rangle \triangleleft \mathrm{G}$. Soit $y = \tau^{2a} \in \langle\tau^2\rangle$ et $x \in \mathrm{G}$; nous avons $x = \tau^k$ ou $x = \tau^k\sigma$. Dans le premier cas nous obtenons

$$xyx^{-1} = \tau^k\tau^{2a}\tau^{-k} = \tau^{k+2a-k} = \tau^{2a} = y \in \langle\tau^2\rangle.$$

Dans le second cas nous obtenons

$$\begin{aligned} xyx^{-1} &= \tau^k\sigma\tau^{2a}(\tau^k\sigma)^{-1} = \tau^k \underbrace{\sigma\tau^{2a}}_{\tau^{2a(n-1)}\sigma} \sigma^{-1}\tau^{-k} \\ &= \tau^k\tau^{2a(n-1)}\sigma\sigma^{-1}\tau^{-k} = \tau^k\tau^{2a(n-1)}\tau^{-k} \\ &= \tau^{k+2a(n-1)-k} = \tau^{2a(n-1)} \in \langle\tau^2\rangle \end{aligned}$$

Ainsi $\langle\tau^2\rangle \triangleleft \mathrm{G}$.

De plus τ^2 est d'ordre $\frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{2} = m$ donc $|\langle\tau^2\rangle| = m$. Ainsi le quotient ${}^{\mathrm{G}}\!/_{\langle\tau^2\rangle}$ est d'ordre $\frac{2n}{m} = 4$. Mais un groupe d'ordre 4

— ou bien a un élément d'ordre 4 et est alors isomorphe à $\mathbb{Z}/4\mathbb{Z}$,

— ou bien n'a que des éléments d'ordre 2 et est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

En particulier un groupe d'ordre 4 est abélien donc $\mathrm{G}/\langle\tau^2\rangle$ est abélien. Comme $\mathrm{G}/D(\mathrm{G})$ est le plus grand quotient abélien de G nous avons l'inclusion $\mathrm{G}/\langle\tau^2\rangle \subset \mathrm{G}/D(\mathrm{G})$ et l'inclusion $D(\mathrm{G}) \subset \langle\tau^2\rangle$. À partir de $\langle\tau^2\rangle \subset D(\mathrm{G})$ et $D(\mathrm{G}) \subset \langle\tau^2\rangle$ on obtient $D(\mathrm{G}) = \langle\tau^2\rangle$.

Il reste à déterminer $\mathrm{G}/D(\mathrm{G}) = \mathrm{G}/\langle\tau^2\rangle$ qui est d'ordre 4. On peut décrire $\mathrm{G}/D(\mathrm{G})$:

$$\mathrm{G}/D(\mathrm{G}) = \{\overline{\mathrm{id}}, \overline{\sigma}, \overline{\tau}, \overline{\tau\sigma}\}.$$

Mais $\overline{\tau}^2 = \overline{\tau^2} = \mathrm{id}$ (car on quotiente par τ^2), $\overline{\sigma}^2 = \overline{\sigma^2} = \overline{\mathrm{id}}$ (car σ est d'ordre 2) et $\overline{\tau\sigma}^2 = \overline{\tau}^2\overline{\sigma}^2 = \overline{\mathrm{id}}$ (car le groupe est abélien). Ainsi tous les éléments de $\mathrm{G}/D(\mathrm{G})$ sont d'ordre 2 et $\mathrm{G}/D(\mathrm{G}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe de Klein.

14. Commençons par rappeler :

> Soit G un groupe. Soit X un ensemble. On dit que G opère sur X si on s'est donné une application
> $$\mathrm{G} \times X \to X, \qquad (g, x) \mapsto g \cdot x$$
> vérifiant les axiomes suivants :
> 1) $\forall\, g,\, g' \in \mathrm{G},\, \forall\, x \in X,\, g \cdot (g' \cdot x) = (gg') \cdot x$
> 2) $\forall\, x \in X,\, 1 \cdot x = x$.
> Remarque : il revient au même de se donner un morphisme de groupes $\varphi\colon \mathrm{G} \to \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ désigne le groupe des bijections de X, on pose alors : $g \cdot x = \varphi(g)(x)$.

Montrons que la multiplication des matrices définit une action

$$\mathrm{G} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, X) \mapsto M \cdot X = MX$$

D'une part $\mathrm{id} \cdot X = X$; d'autre part pour M, M' dans G nous avons

$$(MM') \cdot X = MM'X = M \cdot (M' \cdot X)$$

par l'associativité du produit matriciel. Nous avons donc bien une action de G sur $\mathbb{R}^2$.

15. Commençons par rappeler :

> Soit G un groupe opérant sur un ensemble X. On dit que G opère transitivement sur X si
> $$\forall\, x \in X, \quad \forall\, y \in X, \quad \exists\, g \in \mathrm{G}, \quad g \cdot x = y$$

L'action n'est pas transitive. En effet, d'une part l'orbite d'un vecteur $X \in \mathbb{R}^2$ est l'ensemble

$$\mathcal{O}_X = \{g \cdot X \,|\, g \in \mathrm{G}\} = \{gX \,|\, g \in \mathrm{G}\};$$

d'autre part $|\mathrm{G}| = 2n$. En particulier $\mathcal{O}_X$ compte au plus $2n$ éléments alors que $\mathbb{R}^2$ est infini. Il s'en suit qu'aucune orbite ne peut être égale à $\mathbb{R}^2$ tout entier.

16. Commençons par rappeler :

> Soit G un groupe opérant sur un ensemble X. On dit que G opère fidèlement si $\varphi\colon \mathrm{G} \to \mathfrak{S}(X)$ est injectif, c'est-à-dire si $g \cdot x = x$ pour tout $x \in X$ implique $g = 1$.
> Remparque : $\mathrm{G}/\ker\varphi$ opère fidèlement sur X.

L'action est fidèle : soit $g \in \mathrm{G}$ tel que $g \cdot X = X$ pour tout $X \in \mathbb{R}^2$, *i.e.* tel que $gX = X$ pour tout $X \in \mathbb{R}^2$, alors $g = \mathrm{Id}$.

17. Commençons par rappeler :

> Soit G un groupe opérant sur un ensemble X. L'ensemble des points fixes de l'action de G sur X est
> $$\{x \in X \,|\, g \cdot x = x \quad \forall\, g \in \mathrm{G}\}$$

Déterminons les points fixes de l'action, *i.e.* déterminons

$$\{X \in \mathbb{R}^2 \,|\, g \cdot X = X \quad \forall\, g \in \mathrm{G}\}.$$

Autrement dit nous cherchons les $X \in \mathbb{R}^2$ tels que $g \cdot X = X$ pour tout $g \in \mathrm{G}$. Remarquons que $X = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ est un point fixe. Montrons que c'est le seul. En effet si $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est un point fixe, alors en particulier $\sigma \cdot X = X$, c'est-à-dire $(x, -y) = (x, y)$ d'où $y = 0$. De plus nous avons $\tau \cdot X = X$ soit $\tau \cdot \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$ qui se réécrit $\begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) x \\ \sin\left(\frac{2\pi}{n}\right) x \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$. En particulier $\sin\left(\frac{2\pi}{n}\right) x = 0$; mais pour $n \geq 3$, nous avons $\sin\left(\frac{2\pi}{n}\right) \neq 0$ donc $x = 0$ et $X = (0, 0)$. Finalement $(0, 0)$ est l'unique point fixe de l'action.

18. Commençons par rappeler :

> Soit G un groupe opérant sur un ensemble X. Si x appartient à X, nous définissons
> $$\mathrm{H}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$
> C'est un sous-groupe de G (non distingué en général) appelé le stabilisateur de x.

Déterminons le stabilisateur

$$\mathrm{G}_{v_0} = \{g \in \mathrm{G} \,|\, g \cdot v_0 = v_0\} = \{g \in \mathrm{G} \,|\, g v_0 = v_0\}$$

du vecteur $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Remarquons que $\sigma \cdot v_0 = \sigma v_0 = v_0$, *i.e.* σ appartient à G_{v_0}.

Par ailleurs, soit $1 \leq k \leq n-1$, alors $\tau^k \cdot v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$; ainsi $\tau^k \cdot v_0 = v_0$ si et seulement si $\cos\left(\frac{2k\pi}{n}\right) = 1$ et $\sin\left(\frac{2k\pi}{n}\right) = 0$, c'est-à-dire si et seulement si $\frac{2k\pi}{n} \equiv 0 \pmod{2\pi}$, *i.e.* si et seulement si k est un multiple de n : contradiction avec $1 \leq k \leq n-1$. Ainsi aucun τ^k, $1 \leq k \leq n-1$, ne fixe v_0.

De même nous avons $\tau^k\sigma \cdot v_0 = v_0$ si et seulement si $\tau^k \cdot v_0 = v_0$ si et seulement si $\tau^k = \mathrm{id}$; ainsi aucun $\tau^k\sigma$, $1 \leq k \leq n-1$, fixe v_0.

Il en résulte que $\mathrm{G}_{v_0} = \{\mathrm{id}, \sigma\} = \mathrm{H}$.

19. Commençons par rappeler :

> Soit G un groupe opérant sur un ensemble X. L'orbite d'un élément $x \in X$ sous l'action de G est
> $$\mathcal{O}_x = \{g \cdot x \,|\, g \in \mathrm{G}\}.$$

Décrivons l'orbite du vecteur v_0.

Puisque $\mathcal{O}_{v_0}$ et ${}^{\mathrm{G}}\!/_{\mathrm{G}_{v_0}}$ sont en bijection nous avons

$$|\mathcal{O}_{v_0}| = \left|{}^{\mathrm{G}}\!/_{\mathrm{G}_{v_0}}\right|.$$

Or

$$\left|{}^{\mathrm{G}}\!/_{\mathrm{G}_{v_0}}\right| = [\mathrm{G} : \mathrm{G}_{v_0}] = [\mathrm{G} : \mathrm{H}] = \frac{|\mathrm{G}|}{|\mathrm{H}|} = \frac{2n}{2} = n.$$

Ainsi l'orbite du vecteur v_0 compte n éléments.

Les éléments $\tau^k \cdot v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$, $0 \leq k \leq n-1$, sont 2 à 2 distincts. Ils forment donc l'orbite de v_0.

20. Quel est le stabilisateur G_S du segment $S = [v_0, Y_0]$?

Comme $Y_0 = -v_0$ nous voyons que

$$\sigma \cdot Y_0 = \sigma \cdot (-v_0) = \sigma(-v_0) = -\sigma(v_0) = -v_0 = Y_0$$

donc $\sigma[v_0, Y_0] = [v_0, Y_0]$ et σ appartient à G_S.

Si g appartient à G_S, alors comme g est linéaire, g doit envoyer v_0 sur un élément de la droite $\langle v_0 \rangle = (v_0, Y_0)$. Cherchons de tels $g \in \mathrm{G}$. On a ou bien $g = \tau^k$, ou bien $g = \tau^k\sigma$ avec dans les deux cas $0 \leq k \leq n-1$. Dans les deux éventualités

$$g \cdot v_0 = \tau^k v_0 = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$$

Mais $\langle v_0 \rangle = \{(x, y) \in \mathbb{R}^2 \,|\, y = 0\}$ donc on veut que $\sin\left(\frac{2k\pi}{n}\right) \equiv 0 \pmod{\pi}$ c'est-à-dire $\frac{2k\pi}{n} \equiv 0 \pmod{\pi}$.

Si n est impair, alors la seule possibilité est $k = 0$ et $\mathrm{G}_S = \{\mathrm{id}, \sigma\} = \mathrm{H}$.

Si $n = 2m$ est pair, alors nous avons deux possibilités : $k = 0$ et $k = m$. Pour $k = m$ nous avons

$$\tau^m = \begin{pmatrix} \cos\left(\frac{2m\pi}{n}\right) & -\sin\left(\frac{2m\pi}{n}\right) \\ \sin\left(\frac{2m\pi}{n}\right) & \cos\left(\frac{2m\pi}{n}\right) \end{pmatrix}$$

Ainsi $\tau^m \cdot v_0 = Y_0$ et $\tau^m \cdot Y_0 = v_0$. Par suite $\tau^m \cdot S = S$. Finalement $\mathrm{G}_S = \{\mathrm{id}, \sigma, \tau^m, \tau^m\sigma\}$.

Exercice 747

Rappelons que $\mathrm{SL}(2,\mathbb{R})$ désigne le groupe des applications linéaires de déterminant 1 de $\mathbb{R}^2$ dans lui-même.

Rappelons aussi que $\mathrm{SO}(2,\mathbb{R})$ désigne le groupe des applications linéaires orthogonales directes de $\mathbb{R}^2$ dans lui-même.

Notons $x \cdot y$ le produit scalaire usuel sur $\mathbb{R}^2$.

1. Soit G un sous-groupe fini de $\mathrm{SL}(2,\mathbb{R})$. Soit $g \in \mathrm{G}$. Soit $\varphi_g \colon \mathbb{R}^2 \to \mathbb{R}$ l'application définie par
$$\varphi_g(x,y) = g(x) \cdot g(y).$$
Montrer que $\psi = \sum_{g\in\mathrm{G}} \varphi_g$ est une forme bilinéaire symétrique définie positive sur $\mathbb{R}^2$.
2. Montrer que pour $g \in \mathrm{G}$ nous avons $\psi(g(x), g(y)) = \psi(x,y)$.

   Montrer que la matrice d'un élément de G dans la base $\{e_1, e_2\}$ orthonormée pour ψ est de la forme
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
En déduire que G est un sous-groupe fini de $\mathrm{SO}(2,\mathbb{R})$.
3. Quel est l'ordre d'un élément g de G ? En déduire que g est une rotation d'angle $\frac{2k\pi}{n}$ avec k et n convenables.
4. Montrer que G est cyclique.

Éléments de réponse 747

1. Remarquons que pour tout $g \in \mathrm{G}$ nous avons $\varphi_g(x,y) = \varphi_g(y,x)$. De plus
$$\begin{aligned} \varphi_g(x+x',y) &= g(x+x')g(y) \\ &= (g(x)+g(x'))g(y) \\ &= g(x)g(y) + g(x')g(y) \\ &= \varphi_g(x,y) + \varphi_g(x',y') \end{aligned}$$
et
$$\varphi_g(\lambda x, y) = g(\lambda x)g(y) = (\lambda g(x))g(y) = \lambda g(x)g(y) = \lambda\varphi_g(x,y).$$
Il en résulte que ψ est une forme bilinéaire symétrique.

Si $\psi(x,x)=0$, alors
$$\sum_{g\in \mathrm{G}} \varphi_g(x,x) = \sum_{g\in \mathrm{G}} g(x)^2 = 0.$$
Or dans $\mathbb{R}^2$ une somme de carrés ne peut être nulle que si chacun des carrés est nul donc $g(x)=0$ pour tout $g\in \mathrm{G}$. Toutes les applications linéaires $g\in \mathrm{G}$ sont de déterminant 1 donc inversibles ; il s'en suit que $x=0$ et ψ est définie. C'est une forme définie positive puisque pour tout x, $\psi(x,x)$ est une somme de carrés.

2. Nous avons
$$\psi(g(x),g(y)) = \sum_{h\in \mathrm{G}} h(g(x))h(g(y)).$$
Puisque G est un groupe le morphisme $h\mapsto hg$ de G dans lui-même est injectif donc un isomorphisme car G est fini. Il s'en suit que
$$\sum_{h\in \mathrm{G}} h(g(x))h(g(y)) = \sum_{h\in \mathrm{G}} h'(x)h'(y)$$
autrement dit $\psi(g(x),g(y))=\psi(x,y)$.

Les éléments de G préservent le produit scalaire associé à ψ donc G est un sous-groupe (fini) du groupe orthogonal associé à ce produit scalaire (qui est le groupe orthogonal classique) et la matrice d'un élément $g\in \mathrm{G}$ est donc de la forme
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

3. L'ordre d'un élément de G est fini et divise l'ordre de G. Le groupe G est fini d'ordre n donc si $g\in \mathrm{G}$ est d'ordre k_0, alors g est la rotation d'angle $\frac{2k\pi}{n}$ avec $kk_0=n$.
4. Tout élément de $\langle g\rangle \subset \mathrm{G}$, où g est la rotation d'angle $\frac{2k\pi}{n}$ s'écrit g_0^k où g_0 est la rotation d'angle $\frac{2\pi}{n}$. Par suite $\mathrm{G}\subset\langle g_0\rangle$; or $|\mathrm{G}|=|\langle g_0\rangle|$ donc $\mathrm{G}=\langle g_0\rangle$ et le groupe G est cyclique.

Exercice 748

Désignons par $\mathrm{SL}(2,\mathbb{R})$ le groupe des matrices carrées de taille 2×2 à coefficients réels et de déterminant 1.

Pour $u=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ notons $t_u=a+d$.

1. Quel est le polynôme caractéristique P_u de u ? Quelles sont ses valeurs propres ?
2. Montrer que $P_u(u)=0$.
3. Si P_u admet une racine double, montrer qu'alors
   — ou bien $u=\mathrm{Id}$, ou bien $u=-\mathrm{Id}$;
   — ou bien il existe $v\in \mathrm{SL}(2,\mathbb{R})$ tel que
   $$vuv^{-1}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{ou} \qquad vuv^{-1}=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

— ou bien il existe $w \in \mathrm{SL}(2,\mathbb{R})$ tel que

$$wuw^{-1} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \qquad \text{ou} \qquad wuw^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$

4. Si P_u admet deux racines distinctes réelles, montrer qu'il existe $v \in \mathrm{SL}(2,\mathbb{R})$ et $a \in \mathbb{R}^*$ tels que $vuv^{-1} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Y a-t-il une réciproque ?
5. Si P_u admet deux racines complexes non réelles distinctes montrer qu'il existe $v \in \mathrm{SL}(2,\mathbb{R})$ et a, $b \in \mathbb{R}$, $b \neq 0$, tels que $a^2 + b^2 = 1$ et $vuv^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
6. En déduire pour tout $u \in \mathrm{SL}(2,\mathbb{R})$ l'équivalence, si $n \notin \{1, 2\}$, entre les deux assertions suivantes :

   — u est d'ordre n ;

   — il existe $k \in \mathbb{N}$ premier avec n tel que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$.

7. Soit $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ formé des matrices à coefficients dans $\mathbb{Z}$. Montrer que dans $\mathrm{SL}(2,\mathbb{Z})$ il y a :

   — un élément d'ordre 2 ;

   — une infinité d'éléments d'ordre 4, explicitez-les ;

   — une infinité d'éléments d'ordre 3, explicitez-les ;

   — une infinité d'éléments d'ordre 6, explicitez-les ;

   — aucun élément d'ordre n si $n \notin \{1, 2, 3, 4, 6\}$.

Éléments de réponse 748

1. Soit P_u le polynôme caractéristique de u. Le produit des racines de P_u est égal à $\det u$ qui vaut 1 (puisque $u \in \mathrm{SL}(2,\mathbb{R})$). La somme des racines de P_u est égale à $\mathrm{trace}(u) = t_u = a + d$. Par conséquent $P_u = X^2 - t_u X + 1$.
2. L'endomorphisme associé à u annule son polynôme caractéristique (théorème de Cayley-Hamilton) donc $P_u(u) = 0$.
3. Supposons que P_u admette une racine double. Alors $t_u^2 = 4$ et ou bien $P_u = (X-1)^2$, ou bien $P_u = (X+1)^2$. Nous avons l'alternative suivante :
   - ◇ ou bien u est diagonalisable et u est semblable à id ou $-$id, *i.e.* u est égal à id ou $-$id ;
   - ◇ ou bien u n'est pas diagonalisable et est semblable à sa forme de Jordan ; nous allons distinguer le cas $P_u = (X-1)^2$ du cas $P_u = (X+1)^2$.

i) si $P_u = (X-1)^2$, alors u est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par suite il existe $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0$.

Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et $u = v^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$.

Si $\det v_0 < 0$, $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0 = v_0^{-1}\sigma\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\sigma v_0 = v_0'^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v_0'$$

Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. D'une part $v \in \mathrm{SL}(2,\mathbb{R})$ d'autre part

$$u = v^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$$

ii) Supposons que $P_u = (X+1)^2$ alors u est semblable à $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0$. Soit $v = \lambda v_0$. Nous avons $\det v = \lambda^2 \det v_0$.

Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$ alors v appartient à $\mathrm{SL}(2,\mathbb{R})$ et $u = v^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$.

Si $\det v_0 < 0$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0 = v_0^{-1}\sigma\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}\sigma v_0 = v_0'^{-1}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v_0'$$

Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. Ainsi v appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v.$$

4. Supposons que P_u admette deux racines réelles distinctes. Leur produit étant 1, elles sont inverses l'une de l'autre. La matrice u est donc semblable à une matrice de la forme $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v_0$.

Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$ alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$$

Si $\det v_0 < 0$ et si $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda\sigma v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} v.$$

La réciproque est vraie pour $\alpha \neq \pm 1$.

5. Supposons que P_u admette deux racines complexes distinctes. Elles sont conjuguées et de module 1. Comme $u \in \mathrm{SL}(2,\mathbb{R})$ est de déterminant 1, c'est la matrice, dans la base canonique de $\mathbb{R}^2$, d'une application orthogonale directe g, donc ici (puisque g n'a pas de valeur propre réelle) la matrice d'une rotation d'angle ϑ. Par conséquent u est semblable à $\begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$. Ainsi u est semblable à une matrice du type $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ où $\alpha^2+\beta^2 = 1$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1} \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v_0$.

   Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v.$$

   Si $\det v_0 < 0$ et si λ est tel que $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} v_0$ et

$$u = v^{-1} \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} v.$$

6. Supposons que $n > 2$.
   - ◇ Si $u = \pm\mathrm{id}$, alors l'ordre de u est 1 ou 2.
   - ◇ Si $u = v^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$, alors l'ordre de u est infini.
   - ◇ Reste le cas où $u = v^{-1} \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v$ avec $\alpha^2+\beta^2 = 1$, alors u est la matrice d'une rotation d'angle φ.

   Ainsi $u \in \mathrm{SL}(2,\mathbb{R})$ est d'ordre n si et seulement si u est la matrice d'une rotation d'angle φ et d'ordre n. Une rotation r d'angle φ est d'ordre n si et seulement si $\varphi = \frac{2k\pi}{n}$ avec k et n premiers entre eux (sinon r serait d'ordre strictement inférieur à n). La trace

de l'endomorphisme r est égale à $2\cos\left(\frac{2k\pi}{n}\right)$ et à t_u. Par suite $u \in \mathrm{SL}(2,\mathbb{R})$ est d'ordre n si et seulement si $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux.

7. Les éléments d'ordre n de $\mathrm{SL}(2,\mathbb{Z})$ sont des éléments d'ordre n de $\mathrm{SL}(2,\mathbb{R})$. D'après les questions qui précèdent
   - ◇ il y a un seul élément d'ordre 2 dans $\mathrm{SL}(2,\mathbb{Z})$, c'est $-\mathrm{id}$;
   - ◇ il y a une infinité d'éléments d'ordre 4 : ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = 0$;
   - ◇ il y a une infinité d'éléments d'ordre 3 ; ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = -1$;
   - ◇ il y a une infinité d'éléments d'ordre 6 ; ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = 1$;
   - ◇ pour qu'un élément u de $\mathrm{SL}(2,\mathbb{Z})$ soit d'ordre $n > 2$ il faut et il suffit que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux et que t_u appartienne à $\mathbb{Z}$. Or $2\cos\left(\frac{2k\pi}{n}\right)$ est entier seulement lorsque $n = 3$, 4 et 6. Il s'en suit qu'il n'y a pas d'éléments d'ordre $n \neq 1$, 2, 3, 4, 6 dans $\mathrm{SL}(2,\mathbb{Z})$.

Exercice 749

Soit D_{2n} le groupe diédral d'ordre $2n$ engendré par r d'ordre n et s d'ordre 2 tels que $rs = sr^{-1}$. Autrement dit

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id}\rangle.$$

Exprimer $r^2sr^{-1}s^{-1}r^3s^3$ sous la forme r^is.

Éléments de réponse 749

Nous avons

$$r^2sr^{-1}s^{-1}r^3s^3 = r^2(sr^{-1})s^{-1}r^3(s^2s) = r^2(rs)s^{-1}r^3s = r^2r(ss^{-1})r^3s = r^6s.$$

Exercice 750

Faire la liste de tous les sous-groupes de D_8.

Éléments de réponse 750

Rappelons que

$$\mathrm{D}_8 = \langle r,\, s \,|\, r^4 = s^2 = \mathrm{id},\, rs = sr^{-1}\rangle = \{\mathrm{id},\, r,\, r^2,\, r^3,\, s,\, rs,\, r^2s,\, r^3s\}.$$

Bien entendu $\{\mathrm{id}\}$ et D_8 sont des sous-groupes de D_8.

Le groupe D_8 ne possède que deux éléments d'ordre 4, à savoir r et r^3 Chacun d'eux engendre le groupe $\langle r\rangle$ qui est cyclique d'ordre 4.

Le groupe D_8 possède cinq éléments d'ordre 2 qui sont r^2 et $r^i s$ avec $0 \leq i \leq 3$. Il y a donc cinq sous-groupes cycliques d'ordre 2 :

$$\langle r^2 \rangle, \qquad \langle s \rangle \qquad \langle rs \rangle \qquad \langle r^2 s \rangle \qquad \langle r^{-1} s \rangle.$$

Le groupe D_8 possède un sous-groupe d'ordre 4 non cyclique : $\langle r^2,\, s \rangle$ qui est abélien et isomorphe à $\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}}$ via

$$\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}} \to \langle r^2,\, s \rangle \qquad\qquad (i,j) \mapsto r^{2i} s^j.$$

En effet les groupes $\mathrm{G}_1 = \langle r^2 \rangle$ et $\mathrm{G}_2 = \langle s \rangle$ satisfont les propriétés suivantes :

- $\mathrm{G}_1 \cap \mathrm{G}_2 = \{\mathrm{id}\}$;
- G_1 et G_2 commutent ;
- $\mathrm{G}_1\mathrm{G}_2 = \langle r^2,\, s \rangle$

donc $\langle r,\, s^2 \rangle$ est isomorphe au produit direct de G_1 et G_2, et G_1 et G_2 sont cycliques d'ordre 2.

Le groupe D_8 ne contient pas d'autre sous-groupe ; en effet rappelons que si G est un sous-groupe de D_8, alors $|\mathrm{G}|$ divise $|\mathrm{D}_8| = 8$, *i.e.* $|\mathrm{G}| \in \{1,\, 2,\, 4,\, 8\}$. Nous pouvons récapituler ce qui précède comme suit

$\lvert\mathrm{G}\rvert = 1$	$\{\mathrm{id}\}$
$\lvert\mathrm{G}\rvert = 2$	$\langle r^2 \rangle,\, \langle s \rangle,\, \langle r,\, s \rangle,\, \langle r^2,\, s \rangle,\, \langle r^{-1},\, s \rangle,$
$\lvert\mathrm{G}\rvert = 4$	$\langle r \rangle,\, \langle r^2,\, s \rangle,$
$\lvert\mathrm{G}\rvert = 8$	D_8

À isomorphisme près il y a cinq sous-groupes de D_8 : $\{\mathrm{id}\}$, $\mathbb{Z}\!/_{2\mathbb{Z}}$, $\mathbb{Z}\!/_{4\mathbb{Z}}$, $\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}}$ et D_8.

Exercice 751

Caractériser géométriquement l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est

$$A = \frac{1}{3} \begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$$

Éléments de réponse 751

Les vecteurs colonnes de la matrice sont des vecteurs unitaires deux à deux orthogonaux. La matrice est donc orthogonale. De plus son déterminant est 1. Par suite A appartient à $\mathrm{SO}(3, \mathbb{R})$. La matrice A est donc une matrice de rotation. En réduisant nous obtenons que la trace de A vaut $1 + 2\cos\theta$ où θ est l'angle de la rotation (bien défini au signe près). Comme la trace de A vaut 2 nous avons $\cos\theta = \frac{1}{2}$ et $\theta = \frac{\pi}{3}$. L'axe correspond à la droite propre pour la valeur

propre 1. Nous avons

$$3(A-\mathrm{Id}) = \begin{pmatrix} -1 & -1 & 2 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{pmatrix}$$

Cet axe est donc la droite engendrée par le vecteur $(1,1,1)$.

Exercice 752

Soient A et B deux éléments de $\mathrm{SO}(3,\mathbb{R})$. Donner une condition géométrique nécessaire et suffisante pour que A et B commutent (cette conditions fait intervenir des droites particulières de $\mathbb{R}^3$ associées à A et B).

Éléments de réponse 752

Si A ou B est l'identité, alors A et B commutent.

Supposons que ni A, ni B ne soit l'identité. Ce sont alors deux rotations d'angle non nul. Si A et B commutent, alors l'axe de B est laissé invariant par A et l'axe de A est laissé invariant par B. Notons $\mathcal{D}_A$ l'axe de A et $\mathcal{P}_A$ son orthogonal (qui est donc dans le plan de rotation de A). Soit $\mathcal{D}$ une droite invariante par A, il s'agit donc d'une droite propre pour A. Si A n'est pas un demi-tour, la seule droite invariante pour A est son axe (car A n'a que 1 comme valeur propre) ; si A est un demi-tour, il y a en plus le sous-espace propre associé à -1 qui est $\mathcal{P}_A$. Un raisonnement analogue s'applique à B. Il s'en suit que si A et B commutent, alors A et B ont même axe ou alors ce sont des demi-tours et leurs axes sont orthogonaux.

Réciproquement supposons que A et B aient même axe $\mathcal{D}$. Choisisons une base orthonormale telle que le premier vecteur soit un vecteur directeur de $\mathcal{D}$. Dans cette base A et B s'écrivent

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\beta) & -\sin(\beta) \\ 0 & \sin(\beta) & \cos(\beta) \end{pmatrix}$$

où α et β sont les angles respectifs de A et B. Un calcul matriciel montre alors que A et B commutent.

De même si A et B sont des demi-tour d'axes orthogonaux alors dans une base orthonormale où les deux premiers vecteurs sont des vecteurs directeurs des axes de A et B nous avons

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

et par conséquent A et B commutent.

Exercice 753

Soient E un espace vectoriel euclidien de dimension 3 et S sa sphère unité. Si D est une droite vectorielle de E, on note σ_D la rotation d'angle π autour de D (appelée aussi demi-tour). Par conséquent σ_D appartient au groupe spécial orthogonal $\mathrm{SO}(E)$ dont on rappelle qu'il est engendré par les demi-tours.

1. Soit D une droite vectoriel, soit g un élément de $\mathrm{SO}(E)$. Reconnaître l'endomorphisme $g \circ \sigma_D \circ g^{-1}$.
2. Soit $g \in \mathrm{SO}(E)$. Montrer que g est un demi-tour si et seulement s'il existe $x \in S$ tel que $g(x) = -x$.

   Dans les deux questions suivantes, nous nous donnons un sous-groupe G de $\mathrm{SO}(E)$ agissant transitivement sur S.
3. Montrer que G contient un demi-tour.
4. En déduire que $\mathrm{G} = \mathrm{SO}(E)$.

Éléments de réponse 753

1. Les deux endomorphismes g et $g \circ \sigma_D \circ g^{-1}$ sont des rotations et ont même trace. Ces deux rotations ont même angle, ce sont toutes les deux des demi-tours. D est la droite propre pour la valeur propre 1, par suite $g(D)$ est la droite propre de $g \circ \sigma_D \circ g^{-1}$ pour la valeur propre 1. Il s'en suit que $g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)}$.
2. Soit g un élément de $\mathrm{SO}(E)$. Si g est un demi-tour σ_D, alors g a pour matrice dans une base orthonormale adaptée (e_1, e_2, e_3)
$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$
   Nous avons e_2 appartient à S et $g(e_2) = -e_2$.
3. Si G agit transitivement sur S, alors pour un $x \in S$ fixé il existe g tel que $g(x) = -x$ et donc par la question précédente g est un demi-tour dans G.
4. Comme G est un groupe et comme $\mathrm{SO}(E)$ est engendré par les demi-tours il suffit de montrer que G contient tous les demi-tours. D'après la question précédente il existe une droite D telle que σ_D appartient à G. Soit D' une autre droite. Soit $\overrightarrow{u}$ un vecteur directeur unitaire de D et $\overrightarrow{u'}$ un vecteur directeur unitaire de D'. Puisque G agit transitivement sur S il existe g dans G tel que $g(\overrightarrow{u}) = \overrightarrow{u'}$. Ainsi $g(D) = D'$. D'après 1. nous avons
$$g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)} = \sigma_{D'} \in \mathrm{G}.$$

Exercice 754

Soit $n \in \mathbb{N}^*$. Soit G le sous-ensemble de $M(n+1, \mathbb{R})$ donné par les matrices de la forme
$$M = \left(\begin{array}{c|c} & x_1 \\ A & \vdots \\ & x_n \\ \hline 0 \dots 0 & 1 \end{array}\right)$$
où $A \in \mathrm{GL}(n, \mathbb{R})$ et $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$.

1. Montrer que G est un groupe.
2. Expliciter de quelle manière le groupe affine $\mathrm{GA}(\mathbb{R}^n)$ de R^n est isomorphe au groupe $\mathrm{GL}(n,\mathbb{R}) \ltimes \mathbb{R}^n$. En particulier explique comment effectuer la composée de φ, $\varphi' \in \mathrm{GA}(\mathbb{R}^n)$ où φ (respectivement φ') pour partie linéaire $A \in \mathrm{GL}(n,\mathbb{R})$ (respectivement $A' \in \mathrm{GL}(n,\mathbb{R})$) et vecteur de translation $v \in \mathbb{R}^n$ (respectivement $v' \in \mathbb{R}^n$).
3. Montrer que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$.

Éléments de réponse 754

1. Montrons qu'il s'agit d'un sous-groupe de $\mathrm{GL}(n+1,\mathbb{R})$.

   L'inverse de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$ est la matrice $\left(\begin{array}{c|c} A^{-1} & \begin{matrix} z_1 \\ \vdots \\ z_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A^{-1}(-x_1, -x_2, \dots, -x_n)$.

   La composée de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$ avec $\left(\begin{array}{c|c} B & \begin{matrix} y_1 \\ \vdots \\ y_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$ est $\left(\begin{array}{c|c} AB & \begin{matrix} x_1+z_1 \\ \vdots \\ x_n+z_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A(y_1, y_2, \dots, y_n)$. Il s'agit donc bien d'un sous-groupe.
2. Identifions les éléments de $\mathrm{GA}(\mathbb{R}^n)$ qui fixent 0 avec $\mathrm{GL}(\mathbb{R}^n)$. Les translations sont le morphisme du noyau $\mathrm{GA}(\mathbb{R}^n) \to \mathrm{GL}(\mathbb{R}^n)$. Les translations forment un sous-groupe isomorphe à $\mathbb{R}^n$ par l'application $v \in \mathbb{R}^n \mapsto \tau_v$ où τ_v est la translation de vecteur v.

   Si φ, φ' s'écrivent $\varphi = \tau_v \circ A$ et $\varphi' = \tau_{v'} \circ A'$, alors

   $$\varphi \circ \varphi'(x) = A(A'x + v') + v = AA'x + (Av' + v).$$

   La composée $\varphi \circ \varphi'$ a pour partie linéaire AA' et a pour partie translation, la translation de vecteur $Av' + v$.
3. Montrons que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$. L'isomorphisme est donné par

   $$\psi\colon \mathrm{GA}(\mathbb{R}^n) \to \mathrm{G} \qquad\qquad \varphi = \tau_v \circ A \mapsto \left(\begin{array}{c|c} A & \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right)$$

Il s'agit d'une bijection qui est, d'après 1. et 2., un morphisme de groupes :

$$\begin{aligned}\psi(\varphi\circ\varphi') &= \left(\begin{array}{c|c} AA' & \begin{array}{c} v_1+w_1 \\ \vdots \\ v_n+w_n \end{array} \\ \hline 0\dots0 & 1 \end{array}\right) = \left(\begin{array}{c|c} A & \begin{array}{c} v_1 \\ \vdots \\ v_n \end{array} \\ \hline 0\dots0 & 1 \end{array}\right)\left(\begin{array}{c|c} A' & \begin{array}{c} v'_1 \\ \vdots \\ v'_n \end{array} \\ \hline 0\dots0 & 1 \end{array}\right) \\ &= \psi(\varphi)+\psi(\varphi')\end{aligned}$$

où $w = Av'$.

Exercice 755

Soit E un espace affine euclidien de dimension n. On appelle similitude de E toute transformation affine bijective de E dans lui-même dont la partie linéaire est la composée d'une homothétie et d'une isométrie linéaire.

1. Montrer que les similitudes forment un groupe.
2. Soit φ une similitude. Démontrer que si L est la partie linéaire de φ, alors L s'écrit de matrice unique sous la forme $L = HR$ où H est une homothétie linéaire et R un élément de $\mathrm{SO}(n,\mathbb{R})$ et que de plus H et R commutent.

   Soit φ une bijection de E. On dit que φ préserve les angles (non-orientés) si pour tous points $A \neq B$, $C \in E$, $\widehat{\varphi(A)\varphi(B)\varphi(C)} = \widehat{ABC}$. Nous allons montrer que les similitudes sont extactement les transformations qui préservent les angles.
3. Montrer que les similitudes préservent les angles.

   Soit φ une bijection de E qui préservent les angles.
4. Montrer que φ préserve l'alignement.
5. Montrer que φ est affine.
6. Choisissons une origine O dans E. Trouver une translation τ tells que $(\tau^{-1}\circ\varphi)(O) = O$. Posons $\varphi' = \tau^{-1}\circ\varphi$.
7. Soit $A \neq O$. Posons $\lambda = \frac{||\overrightarrow{O\varphi'(A)}||}{||\overrightarrow{OA}||}$. Si h_λ est l'homothétie de rapport λ et de centre O, montrer que $\psi = h_\lambda^{-1}\circ\varphi'$ préserve le produit scalaire et la norme. On pourra utiliser des triangles isométriques.
8. En déduire que ψ est une isométrie et conclure.

Éléments de réponse 755

Désignons par h_λ l'homothétie de rapport λ.

1. Rappelons que les similitudes linéaires sont les composées d'homothéties linéaires de rapport positif et d'isométries linéaires.

   Les similitudes linéaires forment un sous-groupe de $\mathrm{GL}(E)$. En effet soient R, S dans $\mathrm{O}(E)$. Comme $(h_\lambda R)^{-1} = R^{-1}h_\lambda^{-1} = R^{-1}h_{\lambda^{-1}} = h_{\lambda^{-1}}R^{-1}$, $(h_\lambda R)^{-1}$ est une similitude

linéaire. De même $(h_\lambda R)(h_\mu S) = h_{\lambda+\mu}T$ où T est l'isométrie linéaire RS donc $(h_\lambda R)(h_\mu S)$ est une similitude linéaire.

Les similitudes affines sont l'image réciproque des similitudes linéaires par le morphisme $\mathrm{GA}(E) \to \mathrm{GL}(E)$; il s'agit donc d'un sous-groupe du groupe affine $\mathrm{GA}(E)$.

2. Dans l'écriture $L = HR$, HR commutent car H est une homothétie et donc commute avec tous les éléments de $\mathrm{GL}(E)$. Supposons qu'il existe deux écritures $L = h_\lambda R = h_\mu S$ avec R, S isométries linéaires et λ, $\mu > 0$ alors $|\det L| = \lambda = \mu$ et donc $h_\lambda = h_\mu$ et $R = h_{\lambda^{-1}} L = h_{\mu^{-1}} L = S$. Il y a donc bien unicité.

3. Rappelons que l'angle $\widehat{ABC}$ est l'unique réel $\alpha \in [0, \pi]$ tel que
$$\cos\alpha = \frac{\langle \overrightarrow{BA}, \overrightarrow{BC}\rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||}.$$
Soit φ une similitude dont la partie linéaire L s'écrit $h_\lambda R$ avec $R \in \mathrm{O}(E)$. Nous avons
$$\begin{aligned}
\cos(\varphi(A)\widehat{\varphi(B)}\varphi(C)) &= \frac{\langle \overrightarrow{\varphi(B)\varphi(A)}, \overrightarrow{\varphi(B)\varphi(C)}\rangle}{||\overrightarrow{\varphi(B)\varphi(A)}||\,||\overrightarrow{\varphi(B)\varphi(C)}||} \\
&= \frac{\langle L(\overrightarrow{BA}), L(\overrightarrow{BC})\rangle}{||L(\overrightarrow{BA})||\,||L(\overrightarrow{BC})||} \\
&= \frac{\langle h_\lambda R(\overrightarrow{BA}), h_\lambda R(\overrightarrow{BC})\rangle}{||h_\lambda R(\overrightarrow{BA})||\,||h_\lambda R(\overrightarrow{BC})||} \\
&= \frac{\lambda^2\langle R(\overrightarrow{BA}), R(\overrightarrow{BC})\rangle}{\lambda^2||R(\overrightarrow{BA})||\,||R(\overrightarrow{BC})||} \\
&= \frac{\langle \overrightarrow{BA}, \overrightarrow{BC}\rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||} \\
&= \cos(\widehat{ABC})
\end{aligned}$$
Il en résulte que les similitudes préservent les angles.

4. Trois points A, B et C sont alignés si l'angle $\widehat{ABC}$ vaut 0 ou π. Si une transformation préserve les angles, elle préserve donc aussi l'alignement.

5. Puisque E est un espace vectoriel réel de dimension ≥ 2 une application bijective qui préserve l'alignement est affine. C'est le théorème fondamental de la géométrie affine.

6. La translation τ de vecteur $\overrightarrow{O\varphi(O)}$ convient et c'est la seule.

7. Soit $B \in E$. Les triangles OAB et $\psi(O)\psi(A)\psi(B)$ sont isométriques ; en effet ils ont trois angles égaux, $\psi(O) = O$ et $||\overrightarrow{O\psi(A)}|| = ||\overrightarrow{OA}||$. Par conséquent $||\overrightarrow{O\psi(B)}|| = ||\overrightarrow{OB}||$ et ψ est une application linéaire qui préserve la norme. Ensuite pour B, $C \neq O$ puisque ψ préserve les angles et $||\overrightarrow{OB}|| = ||\overrightarrow{OC}||$, on a $\langle \overrightarrow{OB}, \overrightarrow{OC}\rangle = \langle \overrightarrow{O\psi(B)}, \overrightarrow{O\psi(C)}\rangle$. Il s'en suit que ψ est une application linéaire orthogonale qui préserve aussi la norme.

8. Nous avons donc montré que $\varphi = \tau \circ h_\lambda \circ \psi$, *i.e.* la composée d'une translation et d'une similitude linéaire.

Exercice 756 Groupes et propriétés géométrique de l'orbite.

Soit E un espace affine euclidien. Soit f un élément du groupe $\mathrm{Isom}(E)$ des isométries de E. Soit G le sous-groupe de $\mathrm{Isom}(E)$ engendré par f. Soit p un point de E. Montrer que les assertions suivantes sont équivalentes :

(1) L'orbite de p sous G est bornée ;

(2) Toute orbite sous G d'un point de E est bornée ;

(3) f a un point fixe.

Éléments de réponse 756

Montrons que (3) implique (1).

Par hypothèse il existe $m \in E$ tel que $f(m) = m$. Pour tout $k \in \mathbb{N}$ nous avons

$$d(m, f^k(p)) = d(f^k(m), f^k(p)) = d(m, p)$$

ainsi l'orbite de p sous G est bornée.

Montrons que (1) implique (2).

Il existe $r > 0$ tel que $d(p, f^k(p)) \leq r$ pour tout $k \in \mathbb{N}$. Soit m un point de E alors $d(f^k(p), f^k(m)) = d(p, m)$. Par conséquent

$$d(p, f^k(m)) \leq d(p, f^k(p)) + d(f^k(p), f^k(m)) \leq r + d(p, m).$$

Montrons que (2) implique (3).

Le théorème de la forme réduite des isométries de E implique l'existence de $g \in \mathrm{Isom}(E)$ avec un point fixe p et $\overrightarrow{v} \in \ker(f - \mathrm{id}_E)$ tel que $f = t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$. Ainsi $f^k(A) = A + k\overrightarrow{v}$ et donc $d(A, f^k(A)) = k||\overrightarrow{v}|| \to +\infty$ si $\overrightarrow{v} \neq \overrightarrow{0}$. Puisque la suite $(f^k(A))_k$ est bornée nous obtenons que $\overrightarrow{v} = \overrightarrow{0}$ ainsi $f = g$ a un point fixe.

Exercice 757

Considérons un pentagone régulier $\mathcal{P}$: pour fixer les idées, l'ensemble des points du plan complexe dont des sommets ont pour affixes les racines cinquièmes de l'unité, autrement dit

$$\mathcal{P} = \{\mathrm{e}^{2\mathbf{i}k\pi/5} \,|\, k \in \{0,\, 1,\, 2,\, 3,\, 4\}\}$$

Désignons par O l'origine du plan complexe. Notons ρ la rotation de centre O et d'angle $\frac{2\pi}{5}$ et σ la symétrie qui à un nombre complexe associe son conjugué

$$\rho\colon z \mapsto z\mathrm{e}^{2\mathbf{i}\pi/5}, \qquad\qquad \sigma\colon z \mapsto \overline{z}.$$

1. Vérifier que ρ et σ laissent invariant l'ensemble $\mathcal{P}$.
2. Vérifier que les puissances successives de ρ sont des rotations dont on précisera l'angle. Déterminer l'ordre de ρ.

3. Pour $0 \leq n \leq 4$ montrer que $\sigma\rho^n$ et $\rho^n\sigma$ sont des symétries par rapport à un axe passant par O donc on précisera l'angle par rapport à l'axe réel.
4. Quel est l'ordre d'une symétrie ?
5. Montrer que le produit de deux des symétries de la question 3. est une puissance de ρ.
6. Montrer que le plus petit groupe contenant σ et ρ possède dix éléments. Comment s'appelle ce groupe ?

Éléments de réponse 757

Exercice 758

Soit T un tétraèdre régulier de $\mathbb{R}^3$, notons A_1, A_2, A_3 et A_4 ses sommets. Rappelons que $\mathrm{Isom}(T)$ désigne le groupe des isométries de $\mathbb{R}^3$ préservant T.

1. Expliciter de façon synthétique (sans faire de listes !) un morphisme injectif φ de $\mathrm{Isom}(T)$ vers le groupe symétrique $\mathfrak{S}_4$ (et justifier l'injectivité).
2. Quelle est la préimage de la transposition (1 2) par le morphisme φ ? Et celle de la permutation (1 2)(3 4) ?
3. Montrer que φ est un isomorphisme entre $\mathrm{Isom}(T)$ et $\mathfrak{S}_4$.
4. En utilisant l'action de $\mathrm{Isom}(T)$ sur les paires d'arêtes opposées de T, montrer qu'il existe un morphisme surjectif de $\mathrm{Isom}(T)$ vers $\mathfrak{S}_3$.
5. En déduire que $\mathfrak{S}_3$ est isomorphe à un quotient de $\mathfrak{S}_4$, en précisant le sous-groupe distingué mis en jeu dans ce quotient.

Éléments de réponse 758

1. Un morphisme de $\mathrm{Isom}(T)$ vers $\mathfrak{S}_4$ est donné par
$$\varphi\colon \mathrm{Isom}(T) \to \mathfrak{S}_4 \qquad\qquad f \mapsto \sigma$$
où $f(A_i) = A_{\sigma(i)}$. Ce morphisme est injectif car tout $f \in \mathrm{Isom}(T)$ peut être vu comme un élément de $\mathrm{GL}(3,\mathbb{R})$ en prenant le centre du tétraèdre comme origine, et si $f(A_i) = A_i$ pour $i = 1, 2, 3$, ces trois points formant une base de $\mathbb{R}^3$, on en déduit que $f = \mathrm{id}$.
2. Soit P le plan passant par A_3, A_4 et le milieu du segment $[A_1, A_2]$. Alors la symétrie orthogonale S_P de plan P
   - ◇ fixe A_3, A_4
   - ◇ échange A_1 et A_2, autrement dit $\varphi(S_P) = (1\ 2)$.

   Par ailleurs soit D la droite passant par les milieux des segments $[A_1, A_2]$ et $[A_3, A_4]$, alors la rotation $R_{D,\pi}$ d'axe D et d'angle π échange A_1 et A_2 d'une part, A_3 et A_4 d'autre part. Ainsi $\varphi(R_{D,\pi}) = (1\ 2)(3\ 4)$.

3. On vient de voir que (1 2) appartient à l'image de π ; on montre de même que toute transposition $(i\ j)$ est dans l'image de φ. Comme les transpositions engendrent $\mathfrak{S}_4$ on en déduit que l'image de φ est $\mathfrak{S}_4$. Il en résulte que φ est injective et surjective, c'est un isomorphisme.

4. Notons P_1, P_2, P_3 les 3 paires d'arêtes opposées. On définit un morphisme de $\mathrm{Isom}(T)$ vers $\mathfrak{S}_3$ en posant

$$\psi\colon \mathrm{Isom}(T) \to \mathfrak{S}_3 \qquad\qquad f \mapsto \sigma$$

où $f(P_i) = P_{\sigma(i)}$. Une rotation R d'angle $\frac{2\pi}{3}$ et d'axe passant par un sommet et le milieu de la face opposée est envoyée par ψ sur un 3-cycle. D'autre part la symétrie orthogonale S_P où P est le plan passant par A_3, A_4 et le milieu du segment $[A_1, A_2]$ est envoyée sur une transposition. Puisque $\mathfrak{S}_3$ est engendré par tout choix d'une transposition et d'un 3-cycle on en déduit que ψ est surjectif.

5. Nous appliquons le théorème d'isomorphisme au morphisme surjectif $\psi \circ \varphi$ obtenu en composant les morphismes des questions précédentes. Nous obtenons

$$\mathfrak{S}_4 \big/ \ker(\psi \circ \varphi) \simeq \mathfrak{S}_3.$$

Ainsi $\ker(\psi \circ \varphi)$ est un sous-groupe distingué de $\mathfrak{S}_4$ d'ordre $\frac{24}{6} = 4$, c'est donc le sous-groupe

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 759

Montrer que le groupe affine $\mathrm{GA}(\mathcal{E})$ de l'espace affine dont l'espace vectoriel associé est E est isomorphe à un produit semi-direct de E et $\mathrm{GL}(E)$.

Éléments de réponse 759

Fixons un point O de $\mathcal{E}$. Soit $\mathrm{GA}_O(\mathcal{E})$ le sous-groupe de $\mathrm{GA}(\mathcal{E})$ formé des transformations affines qui laissent fixe le point O.

Soit $\mathrm{T}(\mathcal{E})$ le groupe des translations.

Le groupe $\mathrm{T}(\mathcal{E})$ est distingué dans $\mathrm{GA}(\mathcal{E})$. En effet soit $f \in \mathrm{GA}(\mathcal{E})$ une transformation affine ; notons $\overrightarrow{f}$ sa partie linéaire. Pour tout point M de $\mathcal{E}$ nous avons

$$f(M + \overrightarrow{u}) = f(M) + \overrightarrow{f}(\overrightarrow{u})$$

i.e.

$$(f \circ t_{\overrightarrow{u}})(M) = (t_{\overrightarrow{f}(\overrightarrow{u})} \circ f)(M)$$

ou encore

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f}(\overrightarrow{u})}.$$

Notons qu'une translation qui laisse fixe un point est égale à l'identité ; autrement dit $\mathrm{T}(\mathcal{E}) \cap \mathrm{GA}_O(\mathcal{E}) = \{\mathrm{id}\}$.

Enfin toute transformation affine est composée d'une transformation affine laissant fixe le point O et d'une translation, c'est-à-dire $\mathrm{T}(\mathcal{E})\mathrm{GA}_O(\mathcal{E}) = \mathrm{GA}(\mathcal{E})$. En effet une transformation affine $f \in \mathrm{GA}(\mathcal{E})$ s'écrit

$$f = t_{\overrightarrow{Of(O)}} \circ \left(t_{\overrightarrow{f(O)O}} \circ f \right)$$

et $t_{\overrightarrow{f(O)O}} \circ f$ laisse fixe le point O.

Le groupe $\mathrm{GA}(\mathcal{E})$ est donc le produit semi-direct du sous-groupe des translations par le sous-groupe laissant fixe O. [(2)]

Observons maintenant que l'action du sous-groupe $\mathrm{GA}_O(\mathcal{E})$ sur le sous-groupe distingué $\mathrm{T}(\mathcal{E})$ est donnée par la formule

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f(\overrightarrow{u})}}$$

Comme $\mathrm{T}(\mathcal{E})$ est isomorphe à E et comme $\mathrm{GA}_O(\mathcal{E})$ est isomorphe à $\mathrm{GL}(E)$ via l'application $f \mapsto \overrightarrow{f}$ nous avons

$$\mathrm{GA}(\mathcal{E}) \simeq E \rtimes_\rho \mathrm{GL}(E)$$

où $\rho(f) = \overrightarrow{f}$. Le produit de deux éléments de ce produit semi-direct

$$(\overrightarrow{u}, f)(\overrightarrow{v}, g) = (\overrightarrow{u} + f(\overrightarrow{v}), fg).$$

Exercice 760 [Le groupe diédral]

Considérons un polygone régulier ayant un sommet P de coordonnées $(1, 0)$ et centré à l'origine du repère.

1. Déterminer le groupe D_6 des isométries du plan qui conservent un triangle équilatéral. Établir la table de D_6.
2. Déterminer le groupe D_8 des isométries du plan qui conservent un carré. Déterminer les ordres des éléments de D_8. Établir la table de D_8.
3. Déterminer le groupe D_{2n} des isométries du plan qui conservent un polygone régulier à n côtés.
4. Soit $n \geq 2$ un entier. Considérons le groupe $\mathbb{Z}/n\mathbb{Z}$ et un générateur $[a]$ de ce groupe. Soit $\tau \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par $\tau([c]) = -[c]$.

   Soit $\rho\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par

   $$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

   Montrer que D_{2n} est isomorphe au produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ le long de ρ.

2. Soit G un groupe. Soient N et H deux sous-groupes de G tels que
   - $\mathrm{N} \lhd \mathrm{G}$,
   - $\mathrm{N} \cap \mathrm{H} = \{e\}$,
   - $\mathrm{G} = \mathrm{NH}$.

   Alors $\mathrm{G} \simeq \mathrm{N} \rtimes \mathrm{H}$.

Éléments de réponse 760

Notons O l'origine de $\mathbb{R}^2$. Munissons $\mathbb{R}^2$ de l'orientation géométrique.

1. Commençons par déterminer les isométries (*i.e.* les symétries axiales et les rotations centrées en O) qui fixent un des sommets du triangle équilatéral. En dehors de l'identité il y a la symétrie d'axe la médiane issue du sommet considéré. Comme il y a trois sommets on obtient ainsi trois symétries dans D_6.

   Par ailleurs il y a les deux rotations centrées en O d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$.

   En ajoutant l'identité cela fait déjà 6 éléments dans D_6. Or une isométrie affine qui conserve le triangle équilatéral induit une permutation sur l'ensemble des sommets du triangle équilatéral qui sont au nombre de trois. Par suite D_6 est un sous-groupe de $\mathfrak{S}_3$.

   Il y a $3! = 6$ permutations de ces trois sommets donc $\mathrm{D}_6 \simeq \mathfrak{S}_3$ et nous avons listé tous les éléments de D_6.

   Désignons par A_1, A_2 et A_3 les sommets du triangle équilatéral. Pour $1 \leq i \leq 3$ notons s_i la symétrie qui laisse le point A_i fixe, r_1 la rotation d'angle $\frac{2\pi}{3}$ et $r_2^2 = r_1$ la rotation d'angle $\frac{4\pi}{3}$.

   La table de $\mathrm{D}_6 \simeq \mathfrak{S}_3$ est la suivante

	id	s_1	s_2	s_3	r_1	r_2
id	id	s_1	s_2	s_3	r_1	r_2
s_1	s_1	id	r_1	r_2	s_2	s_3
s_2	s_2	r_2	id	r_1	s_3	s_1
s_3	s_3	r_1	r_2	id	s_1	s_2
r_1	r_1	s_3	s_1	s_2	r_2	id
r_2	r_2	s_2	s_3	s_1	id	r_1

2. Notons qu'une isométrie qui préserve un carré envoie chaque sommet sur un sommet, chaque côté sur un côté et chaque diagonale sur une diagonale.

   Déterminons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui laissent fixe le point A_1. De telles isométries laissent donc fixe la diagonale $[A_1, A_3]$ et donc le point A_3. Il n'y en a donc qu'une non triviale : la symétrie par rapport à cette diagonale.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_2. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$. Il en résulte que A_3 a pour image A_4. Il y a deux telles isométries

   - ◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_2]$ et $[A_3, A_4]$ qui envoie A_4 sur A_3 et A_2 sur A_1 ;
   - ◇ la rotation d'angle $\frac{3\pi}{2}$ qui envoie A_4 sur A_1 et A_2 sur A_3.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_4. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$; le point A_3 a donc pour image le point A_2. Il y en a donc deux :

◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_4]$ et $[A_2, A_3]$ qui envoie A_4 sur A_1 et A_2 sur A_3 ;

◇ la rotation d'angle $\frac{\pi}{2}$ qui envoie A_4 sur A_3 et A_2 sur A_1.

Restent les isométries qui envoient A_1 sur A_3 en conservant le carré. La diagonale $[A_2, A_4]$ est alors préservée. Il y en a deux :

◇ la symétrie par rapport à la diagonale $[A_2, A_4]$;

◇ la rotation d'angle π.

Notations :

◇ r_1 la rotation d'angle $\frac{\pi}{2}$;

◇ r_2 la rotation d'angle π ;

◇ r_3 la rotation d'angle $\frac{3\pi}{2}$;

◇ s_{12} la symétrie d'axe la médiatrice de $[A_1, A_2]$;

◇ s_{23} la symétrie d'axe la médiatrice de $[A_2, A_3]$;

◇ s_{13} la symétrie d'axe la médiatrice de $[A_1, A_3]$;

◇ s_{24} la symétrie d'axe la médiatrice de $[A_2, A_4]$.

Chacune des symétries est d'ordre 2 ; r_1 et r_3 sont d'ordre 4 et r_2 est d'ordre 2.

La table de D_8 est

	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
id	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
r_1	r_1	r_2	r_3	id	s_{13}	s_{24}	s_{23}	s_{12}
r_2	r_2	r_3	id	r_1	s_{23}	s_{12}	s_{24}	s_{13}
r_3	r_3	id	r_1	r_2	s_{24}	s_{13}	s_{12}	s_{23}
s_{12}	s_{12}	s_{24}	s_{23}	s_{13}	id	r_2	r_3	r_1
s_{23}	s_{23}	s_{13}	s_{12}	s_{24}	r_2	id	r_1	r_3
s_{13}	s_{13}	s_{12}	s_{24}	s_{23}	r_1	r_3	id	r_2
s_{24}	s_{24}	s_{23}	s_{13}	s_{12}	r_3	r_1	r_2	id

3. Soit P un polygone régulier à n côtés. Numérotons les sommets de P_n dans le sens trigonométrique, il s'écrit $[A_1, A_2, \ldots, A_n]$.

Pour une isométrie conservant le polygone chaque sommet va sur un sommet, chaque côté va sur un côté donc si A_1 a pour image A_k alors A_2 a pour image soit A_{k-1} soit A_{k+1}. Dans le premier cas l'isométrie est une symétrie (car ce n'est pas un élément de $\mathrm{SO}(2, \mathbb{R})$), dans le second cas l'isométrie est une rotation d'angle $\frac{2k\pi}{n}$. Les axes de symétrie possibles sont

◇ si n est pair les droites déterminées par un sommet quelconque et le centre (il y en a $\frac{n}{2}$) et les droites déterminées par les médiatrices des côté (il y en a $\frac{n}{2}$) ;

◇ si n est impair, les droites déterminées par un sommet quelconque et le centre qui sont les droites déterminées par les médiatrices des côtés (il y en a n).

Soit r la rotation d'angle $\frac{2\pi}{n}$ et soit s l'une des symétries de D_{2n}. Le groupe D_{2n} est engendré par s et r.

4. Le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ est d'ordre $2n$. Si $\beta = ([0],[1])$ et $\alpha = ([1],[0])$, alors
   ◇ $\beta^2 = ([0],[0])$ où $([0],[0])$ est l'élément neutre du produit semi-direct, *i.e.* β est d'ordre 2 ;
   ◇ $\alpha^n = ([0],[0])$, *i.e.* α est d'ordre n ;
   ◇ et

   $$\beta\alpha\beta^{-1} = ([0],[1])([1],[0])([0],[1]) = ([0],[1])([1],[1]) = ([n-1],[0]) = \alpha^{n-1}.$$

   En effet, rappel : soient N et H deux groupes. Soit Aut(N) le groupe des automorphismes de groupe de N. Soit $\varphi\colon \mathrm{H} \to \mathrm{Aut(N)}$ un morphisme qui définit une opération de H sur N par la formule $h \cdot n = \varphi(h)(n)$.

   On définit sur l'ensemble produit $\mathrm{N} \times \mathrm{H}$ une loi par

   $$(n,h)(n',h') = \big(n(h \cdot n'), hh'\big).$$

   Alors $\mathrm{N} \times \mathrm{H}$, muni de cette loi, est un groupe appelé *produit semi-direct* de N par H relativement à φ et noté $\mathrm{N} \rtimes_\varphi \mathrm{H}$ ou plus simplement $\mathrm{N} \rtimes \mathrm{H}$.

   Ici $\mathrm{H} = \mathbb{Z}/2\mathbb{Z}$, $\mathrm{N} = \mathbb{Z}/n\mathbb{Z}$ et $\varphi = \rho$. Par suite

   $$(n,h)(n',h') = \big(n + \rho(h)(n'), h + h'\big).$$

   et

   $$\begin{aligned}
   ([0],[1])([1],[0])([0],[1]) &= ([0],[1])([1] + \rho([0])([0]), [0]+[1]) \\
   &= ([0],[1])([1],[1]) \\
   &= ([0] + \rho([1])([1]), [1]+[1]) \\
   &= (\rho([1])([1]), [2]) \\
   &= ([0] + (-[1]), [0]) \\
   &= ([n-1],[0])
   \end{aligned}$$

   Nous avons

   $$\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} = \{e,\, \alpha,\, \ldots,\, \alpha^{n-1},\, \beta,\, \beta\alpha,\, \beta\alpha^2,\, \ldots,\, \beta\alpha^{n-1}\}.$$

   Rappelons que

   $$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id}\rangle.$$

   Soit φ l'homomorphisme défini par

   $$\mathrm{D}_{2n} \to \mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \qquad \begin{cases} s \mapsto \beta \\ r \mapsto \alpha \end{cases}$$

Par construction c'est un isomorphisme.

Exercice 761

Soit $\tau \in \mathrm{Aut}\Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big)$ défini par $\tau([a],[b]) = ([b],[a])$.

Soit $\rho\colon \mathbb{Z}\!\diagup_{2\mathbb{Z}} \to \mathrm{Aut}\Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big)$ défini par

$$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

Montrer que D_8 est isomorphe au produit semi-direct de $\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}$ et $\mathbb{Z}\!\diagup_{2\mathbb{Z}}$ le long de ρ.

Éléments de réponse 761

Décrivons le produit semi-direct

$$\mathrm{G} = \Big(\mathbb{Z}\!\diagup_{2\mathbb{Z}} \times \mathbb{Z}\!\diagup_{2\mathbb{Z}}\Big) \rtimes_\rho \mathbb{Z}\!\diagup_{2\mathbb{Z}}$$

Le groupe G est engendré par $\beta = ([0],[0],[1])$ qui est d'ordre 2, $\alpha_1 = ([1],[0],[0])$ et $\alpha_2 = ([0],[1],[0])$. Nous avons $\beta\alpha_1 = \alpha_2\beta$, $\beta\alpha_2 = \alpha_1\beta$. En effet vérifions la première relation : d'une part

$$\begin{aligned}
\beta\alpha_1 &= ([0],[0],[1])([1],[0],[0]) \\
&= (([0],[0]) + \tau([1])([1],[0]),[1]+[0]) \\
&= (([0],[0]) + ([0],[1]),[1]+[0]) \\
&= ([0],[1],[1])
\end{aligned}$$

et d'autre part

$$\begin{aligned}
\alpha_2\beta &= ([0],[1],[0])([0],[0],[1]) \\
&= (([0],[1]) + \tau([0])([0],[0]),[0]+[1]) \\
&= (([0],[1]) + ([0],[0]),[0]+[1]) \\
&= ([0],[1],[1])
\end{aligned}$$

Le groupe G est d'ordre 8 et

$$\mathrm{G} = \{e,\, \alpha_1,\, \alpha_2,\, \alpha_1\alpha_2,\, \beta,\, \beta\alpha_1,\, \beta\alpha_2,\, \beta\alpha_1\alpha_2\}.$$

Isomorphisme entre D_8 et G : l'image d'un élément d'ordre 2 est d'ordre 2, l'image d'un élément d'ordre 4 est d'ordre 4. Les éléments d'ordre 4 de G sont $\beta\alpha_1$ et $\beta\alpha_2$. Soit φ l'homomorphisme entre ces deux groupes qui envoie r sur $\beta\alpha_1$. Alors $\varphi(r^3) = \beta\alpha_2$ et $\varphi(r^2) = \alpha_1\alpha_2$. Prenons $\varphi(s) = \beta$. Nous pouvons vérifier qu'on a bien un isomorphisme.

Exercice 762

1. Déterminer le groupe des isométries du plan qui conservent un rectangle non carré.
2. Établir la table de ce groupe.

Éléments de réponse 762

1. Considérons un rectangle $ABCD$ tel que "A est le coin en haut à gauche, B le coin en haut à droite, C le coin en bas à droite, D le coin en bas à gauche, $[AB]$ et $[CD]$ sont les longueurs et $[BC]$ et $[AD]$ les largeurs." Prenons pour origine du repère le centre du rectangle.

   Une isométrie qui conserve le rectangle laisse fixe le centre du rectangle donc le groupe recherché est isomorphe à un sous-groupe du groupe des isométries vectorielles. Par ailleurs une isométrie qui conserve le rectangle envoie chaque diagonale sur une diagonale.

   Une isométrie qui conserve le rectangle et laisse fixe le sommet A laisse fixe la diagonale $[AC]$ et donc le sommet C et tous les autres sommets. Ainsi la seule isométrie qui conserve le rectangle et laisse fixe le sommet A est l'identité. Il en est de même lorsque l'on remplace A par B (resp. C, resp. D). Une isométrie qui conserve le rectangle et qui n'est pas l'identité ne fixe donc aucun sommet.

   - ◇ ou bien A a pour image B alors C a pour image D et cette isométrie est la symétrie s_1 d'axe la médiatrice de $[AB]$;
   - ◇ ou bien A a pour image D, alors B a pour image C et cette isométrie est la symétrie s_2 d'axe la médiatrice de $[AD]$;
   - ◇ ou bien A et C sont échangés et cette isométrie est la rotation r d'angle π.

2. On a donc un groupe d'ordre 4, abélien, dont la table est :

	id	s_1	s_2	r
id	id	s_1	s_2	r
s_1	s_1	id	r	s_2
s_2	s_2	r	id	s_1
r	r	s_2	s_1	id

Exercice 763

1. Déterminer le centre de $\mathfrak{S}_3$.
2. Déterminer le centre de D_8.
3. Déterminer le centre de D_{12}.
4. Déterminer le centre de D_{4n}.

Éléments de réponse 763

1. Rappelons que $\mathfrak{S}_3 \simeq \mathrm{D}_6$. Le centre de $\mathfrak{S}_3$ est trivial.

2., 3. et 4. Considérons le groupe D_{4n}. Le centre de D_{4n} ne contient pas les rotations r_k d'angle $\frac{2k\pi}{2n} = \frac{k\pi}{n}$, pour $k \neq n$, car elles ne commutent pas avec les symétries.

Par contre le retournement r_0 donné par $k = n$ (*i.e.* la rotation d'angle π) commute avec tous les éléments de D_{4n} :

- ◇ avec les rotations de D_{4n} car l'ensemble des rotations est un sous-groupe cyclique de D_{4n} ;
- ◇ avec les symétries orthogonales car ce retournement est la composée de deux symétries orthogonales par rapport à des axes orthogonaux (r_0 s'écrit ss' avec s symétrie orthogonale de D_{4n} et s' la symétrie orthogonale d'axe orthogonal à celui de s ; d'une part $r_0 s = s'ss = s'$ et $sr_0 s = sss' = s'$).

Le centre de D_{4n} est donc $\{\mathrm{id}, r_0\}$.

Exercice 764

Soit $n \geq 3$; le sous-ensemble $\{g \in \mathrm{D}_{2n} \,|\, g^2 = \mathrm{id}\}$ de D_{2n} est-il un sous-groupe de D_{2n} ?

Éléments de réponse 764

La composée de deux symétries orthogonales éléments de D_{2n} est une rotation d'angle deux fois l'angle formé par les deux axes. Par suite dès que $n \geq 3$ l'un de ces produits au moins est d'ordre différent de 2. Ainsi l'ensemble des éléments d'ordre 2 de D_{2n} n'est pas un sous-groupe de D_{2n}.

Exercice 765

Notons $\mathrm{OA}(2, \mathbb{R})$ le groupe des déplacements de $\mathbb{R}^2$. Soit G un sous-groupe de $\mathrm{OA}(2, \mathbb{R})$ qui contient les rotations centrées en deux points distincts.

Montrer que G contient une translation.

Éléments de réponse 765

Toute rotation se décompose en une composée de deux symétries orthogonales. Soient A et B les deux points qui sont centres des rotations que G contient. Soit s la symétrie orthogonale d'axe (AB). Soit s_1 la symétrie orthogonale d'axe une droite quelconque $\mathcal{D}_1$ passant par A différente de (AB). Soit s_2 la symétrie orthogonale d'axe la droite $\mathcal{D}_2$ passant par B parallèle à $\mathcal{D}_1$.

Les rotations $s_1 s$ et ss_2 appartiennent à G ; par suite $(s_1 s)(ss_2)$ appartient à G, *i.e.* $s_1 s_2$ est dans G. Or la composée $s_1 s_2$ est une translation donc G contient une translation.

Exercice 766

Les actions considérées ci-après sont les actions naturelles.

1. Montrer que l'action de $\mathrm{GL}(n, \mathbb{R})$ sur $\mathbb{R}^n$ n'est pas transitive mais qu'elle définit sur l'ensemble des bases de $\mathbb{R}^n$ une action transitive.
2. Montrer que $\mathrm{SO}(2, \mathbb{R})$ agit transitivement sur le cercle unité de $\mathbb{R}^2$.

3. Montrer que $\mathrm{SO}(3,\mathbb{R})$ agit transitivement sur la sphère unitée de $\mathbb{R}^3$.

Éléments de réponse 766

1. Deux vecteurs quelconques de $\mathbb{R}^n$ sont dans la même orbite pour l'action de $\mathrm{GL}(n,\mathbb{R})$ sur $\mathbb{R}^n$ à condition qu'aucun des deux ne soit nul : l'orbite du vecteur nul est réduite à ce vecteur nul. L'action considérée n'est donc pas transitive.

   Par contre deux bases quelconques de $\mathbb{R}^n$ sont images l'une de l'autre par une unique application linéaire bijective. L'action de $\mathrm{GL}(n,\mathbb{R})$ sur l'ensemble des bases de $\mathbb{R}^n$ est donc transitive.

2. Deux vecteurs quelconques de $\mathbb{R}^2$ sont dans la même orbite pour l'action de $\mathrm{SO}(2,\mathbb{R})$ sur $\mathbb{R}^2$ à condition qu'ils aient même norme ; les éléments du cercle unité ont norme 1, par suite l'action de $\mathrm{SO}(2,\mathbb{R})$ est transitive sur le cercle unité.

3. Même chose qu'à la question précédente.

Exercice 767

Soit G un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$. Déterminer l'orbite d'un point A de $\mathbb{R}^2 \setminus \{O\}$ quand G est le sous-groupe engendré par :

1. une symétrie par rapport à une droite ;
2. une rotation d'angle $\frac{\pi}{2}$;
3. une rotation d'angle $\frac{2\pi}{n}$ ($n > 0$ entier) ;
4. une rotation d'angle $\frac{2\pi}{n}$ ($n > 0$ entier) et une symétrie par rapport à une droite D (penser à distinguer deux cas).

Éléments de réponse 767

Notons que comme on considère l'action naturelle de $\mathrm{GL}(2,\mathbb{R})$ sur $\mathbb{R}^2$ les rotations dont on parle sont les rotations centrées en l'origine O du repère, les symétries dont on parle sont les symétries d'axes les droites qui passent par l'origine O du repère.

1. Si A est sur l'axe de la symétrie s considérée, alors son orbite est réduite à $\{A\}$; si A n'est pas sur cet axe, alors l'orbite de A est $\{A, s(A)\}$.
2. L'orbite de A est formée des quatre sommets du carré centré à l'origine (dont A).
3. L'orbite de A est formée des n sommets du polygone P régulier à n côtés centré à l'origine (dont A).
4. Soit P le polygone régulier à n côtés centré à l'origine. Si l'axe de la symétrie s est l'un des axes de symétrie de P l'orbite de A est l'ensemble des sommets de P ; sinon l'orbite de A est la réunion de l'ensemble des sommets de P et ceux de P' où P' est l'image de P par s.

Exercice 768

Rappelons que $\mathrm{SL}(2,\mathbb{R})$ désigne le groupe des applications linéaires de déterminant 1 de $\mathbb{R}^2$ dans lui-même.

Rappelons aussi que $\mathrm{SO}(2,\mathbb{R})$ désigne le groupe des applications linéaires orthogonales directes de $\mathbb{R}^2$ dans lui-même.

Notons $x \cdot y$ le produit scalaire usuel sur $\mathbb{R}^2$.

1. Soit G un sous-groupe fini de $\mathrm{SL}(2,\mathbb{R})$. Soit $g \in \mathrm{G}$. Soit $\varphi_g \colon \mathbb{R}^2 \to \mathbb{R}$ l'application définie par
$$\varphi_g(x,y) = g(x) \cdot g(y).$$
Montrer que $\psi = \sum_{g\in\mathrm{G}} \varphi_g$ est une forme bilinéaire symétrique définie positive sur $\mathbb{R}^2$.
2. Montrer que pour $g \in \mathrm{G}$ nous avons $\psi(g(x), g(y)) = \psi(x,y)$.
Montrer que la matrice d'un élément de G dans la base $\{e_1, e_2\}$ orthonormée pour ψ est de la forme
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
En déduire que G est un sous-groupe fini de $\mathrm{SO}(2,\mathbb{R})$.
3. Quel est l'ordre d'un élément g de G ? En déduire que g est une rotation d'angle $\frac{2k\pi}{n}$ avec k et n convenables.
4. Montrer que G est cyclique.

Éléments de réponse 768

1. Remarquons que pour tout $g \in \mathrm{G}$ nous avons $\varphi_g(x,y) = \varphi_g(y,x)$. De plus
$$\begin{aligned} \varphi_g(x+x',y) &= g(x+x')g(y) \\ &= (g(x)+g(x'))g(y) \\ &= g(x)g(y) + g(x')g(y) \\ &= \varphi_g(x,y) + \varphi_g(x',y') \end{aligned}$$
et
$$\varphi_g(\lambda x, y) = g(\lambda x)g(y) = (\lambda g(x))g(y) = \lambda g(x)g(y) = \lambda\varphi_g(x,y).$$
Il en résulte que ψ est une forme bilinéaire symétrique.
Si $\psi(x,x) = 0$, alors
$$\sum_{g\in\mathrm{G}} \varphi_g(x,x) = \sum_{g\in\mathrm{G}} g(x)^2 = 0.$$
Or dans $\mathbb{R}^2$ une somme de carrés ne peut être nulle que si chacun des carrés est nul donc $g(x) = 0$ pour tout $g \in \mathrm{G}$. Toutes les applications linéaires $g \in \mathrm{G}$ sont de déterminant 1 donc inversibles ; il s'en suit que $x = 0$ et ψ est définie. C'est une forme définie positive puisque pour tout x, $\psi(x,x)$ est une somme de carrés.

2. Nous avons
$$\psi(g(x), g(y)) = \sum_{h\in \mathrm{G}} h(g(x))h(g(y)).$$
Puisque G est un groupe le morphisme $h \mapsto hg$ de G dans lui-même est injectif donc un isomorphisme car G est fini. Il s'en suit que
$$\sum_{h\in \mathrm{G}} h(g(x))h(g(y)) = \sum_{h\in \mathrm{G}} h'(x)h'(y)$$
autrement dit $\psi(g(x), g(y)) = \psi(x, y)$.

Les éléments de G préservent le produit scalaire associé à ψ donc G est un sous-groupe (fini) du groupe orthogonal associé à ce produit scalaire (qui est le groupe orthogonal classique) et la matrice d'un élément $g \in \mathrm{G}$ est donc de la forme
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

3. L'ordre d'un élément de G est fini et divise l'ordre de G. Le groupe G est fini d'ordre n donc si $g \in \mathrm{G}$ est d'ordre k_0, alors g est la rotation d'angle $\frac{2k\pi}{n}$ avec $kk_0 = n$.
4. Tout élément de $\langle g\rangle \subset \mathrm{G}$, où g est la rotation d'angle $\frac{2k\pi}{n}$ s'écrit g_0^k où g_0 est la rotation d'angle $\frac{2\pi}{n}$. Par suite $\mathrm{G} \subset \langle g_0\rangle$; or $|\mathrm{G}| = |\langle g_0\rangle|$ donc $\mathrm{G} = \langle g_0\rangle$ et le groupe G est cyclique.

Exercice 769 [Quelques propriétés de $\mathrm{SL}(2,\mathbb{R})$]

Désignons par $\mathrm{SL}(2,\mathbb{R})$ le groupe des matrices carrées de taille 2×2 à coefficients réels et de déterminant 1.

Pour $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ notons $t_u = a + d$.

1. Quel est le polynôme caractéristique P_u de u ? Quelles sont ses valeurs propres ?
2. Montrer que $P_u(u) = 0$.
3. Si P_u admet une racine double, montrer qu'alors
   - ◇ ou bien $u = \mathrm{Id}$, ou bien $u = -\mathrm{Id}$;
   - ◇ ou bien il existe $v \in \mathrm{SL}(2,\mathbb{R})$ tel que
   $$vuv^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{ou} \quad vuv^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
   - ◇ ou bien il existe $w \in \mathrm{SL}(2,\mathbb{R})$ tel que
   $$wuw^{-1} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{ou} \quad wuw^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$
4. Si P_u admet deux racines distinctes réelles, montrer qu'il existe $v \in \mathrm{SL}(2,\mathbb{R})$ et $a \in \mathbb{R}^*$ tels que $vuv^{-1} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Y a-t-il une réciproque ?

5. Si P_u admet deux racines complexes non réelles distinctes montrer qu'il existe $v \in \mathrm{SL}(2,\mathbb{R})$ et a, $b \in \mathbb{R}$, $b \neq 0$, tels que $a^2+b^2=1$ et $vuv^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
6. En déduire pour tout $u \in \mathrm{SL}(2,\mathbb{R})$ l'équivalence, si $n \notin \{1, 2\}$, entre les deux assertions suivantes :
   - ◇ u est d'ordre n ;
   - ◇ il existe $k \in \mathbb{N}$ premier avec n tel que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$.
7. Soit $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ formé des matrices à coefficients dans $\mathbb{Z}$. Montrer que dans $\mathrm{SL}(2,\mathbb{Z})$ il y a :
   - ◇ un élément d'ordre 2 ;
   - ◇ une infinité d'éléments d'ordre 4, explicitez-les ;
   - ◇ une infinité d'éléments d'ordre 3, explicitez-les ;
   - ◇ une infinité d'éléments d'ordre 6, explicitez-les ;
   - ◇ aucun élément d'ordre n si $n \notin \{1, 2, 3, 4, 6\}$.

Éléments de réponse 769

1. Soit P_u le polynôme caractéristique de u. Le produit des racines de P_u est égal à $\det u$ qui vaut 1 (puisque $u \in \mathrm{SL}(2,\mathbb{R})$). La somme des racines de P_u est égale à $\mathrm{trace}(u) = t_u = a+d$. Par conséquent $P_u = X^2 - t_u X + 1$.
2. L'endomorphisme associé à u annule son polynôme caractéristique (théorème de Cayley-Hamilton) donc $P_u(u) = 0$.
3. Supposons que P_u admette une racine double. Alors $t_u^2 = 4$ et ou bien $P_u = (X-1)^2$, ou bien $P_u = (X+1)^2$. Nous avons l'alternative suivante :
   - ◇ ou bien u est diagonalisable et u est semblable à id ou $-$id, *i.e.* u est égal à id ou $-$id ;
   - ◇ ou bien u n'est pas diagonalisable et est semblable à sa forme de Jordan ; nous allons distinguer le cas $P_u = (X-1)^2$ du cas $P_u = (X+1)^2$.
     i) si $P_u = (X-1)^2$, alors u est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par suite il existe $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0$.
     Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et $u = v^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$.

Si $\det v_0 < 0$, $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0 = v_0^{-1} \sigma \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \sigma v_0 = v_0'^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v_0'$$

Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. D'une part $v \in \mathrm{SL}(2, \mathbb{R})$ d'autre part

$$u = v^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$$

ii) Supposons que $P_u = (X+1)^2$ alors u est semblable à $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2, \mathbb{R})$ tel que $u = v_0^{-1} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0$. Soit $v = \lambda v_0$. Nous avons $\det v = \lambda^2 \det v_0$.

Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$ alors v appartient à $\mathrm{SL}(2, \mathbb{R})$ et $u = v^{-1} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$.

Si $\det v_0 < 0$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0 = v_0^{-1} \sigma \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \sigma v_0 = v_0'^{-1} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v_0'$$

Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. Ainsi v appartient à $\mathrm{SL}(2, \mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v.$$

4. Supposons que P_u admette deux racines réelles distinctes. Leur produit étant 1, elles sont inverses l'une de l'autre. La matrice u est donc semblable à une matrice de la forme $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2, \mathbb{R})$ tel que $u = v_0^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v_0$.

Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$ alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2, \mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$$

Si $\det v_0 < 0$ et si $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda \sigma v_0$ appartient à $\mathrm{SL}(2, \mathbb{R})$ et

$$u = v^{-1} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} v.$$

La réciproque est vraie pour $\alpha \neq \pm 1$.

5. Supposons que P_u admette deux racines complexes distinctes. Elles sont conjuguées et de module 1. Comme $u \in \mathrm{SL}(2,\mathbb{R})$ est de déterminant 1, c'est la matrice, dans la base canonique de $\mathbb{R}^2$, d'une application orthogonale directe g, donc ici (puisque g n'a pas de valeur propre réelle) la matrice d'une rotation d'angle ϑ. Par conséquent u est semblable à $\begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$. Ainsi u est semblable à une matrice du type $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ où $\alpha^2+\beta^2 = 1$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v_0$.

   Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v.$$

   Si $\det v_0 < 0$ et si λ est tel que $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} v_0$ et

$$u = v^{-1}\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} v.$$

6. Supposons que $n > 2$.
   - ◇ Si $u = \pm\mathrm{id}$, alors l'ordre de u est 1 ou 2.
   - ◇ Si $u = v^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$, si $u = v^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$, si $u = v^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$, si $u = v^{-1}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v$, si $u = v^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$, alors l'ordre de u est infini.
   - ◇ Reste le cas où $u = v^{-1}\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v$ avec $\alpha^2+\beta^2 = 1$, alors u est la matrice d'une rotation d'angle φ.

   Ainsi $u \in \mathrm{SL}(2,\mathbb{R})$ est d'ordre n si et seulement si u est la matrice d'une rotation d'angle φ et d'ordre n. Une rotation r d'angle φ est d'ordre n si et seulement si $\varphi = \frac{2k\pi}{n}$ avec k et n premiers entre eux (sinon r serait d'ordre strictement inférieur à n). La trace de l'endomorphisme r est égale à $2\cos\left(\frac{2k\pi}{n}\right)$ et à t_u. Par suite $u \in \mathrm{SL}(2,\mathbb{R})$ est d'ordre n si et seulement si $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux.
7. Les éléments d'ordre n de $\mathrm{SL}(2,\mathbb{Z})$ sont des éléments d'ordre n de $\mathrm{SL}(2,\mathbb{R})$. D'après les questions qui précèdent
   - ◇ il y a un seul élément d'ordre 2 dans $\mathrm{SL}(2,\mathbb{Z})$, c'est $-\mathrm{id}$;
   - ◇ il y a une infinité d'éléments d'ordre 4 : ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = 0$;

- ◇ il y a une infinité d'éléments d'ordre 3 ; ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = -1$;
- ◇ il y a une infinité d'éléments d'ordre 6 ; ce sont les matrices u de $\mathrm{SL}(2,\mathbb{Z})$ telles que $t_u = 1$;
- ◇ pour qu'un élément u de $\mathrm{SL}(2,\mathbb{Z})$ soit d'ordre $n > 2$ il faut et il suffit que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux et que t_u appartienne à $\mathbb{Z}$. Or $2\cos\left(\frac{2k\pi}{n}\right)$ est entier seulement lorsque $n = 3$, 4 et 6. Il s'en suit qu'il n'y a pas d'éléments d'ordre $n \neq 1$, 2, 3, 4, 6 dans $\mathrm{SL}(2,\mathbb{Z})$.

Exercice 770

Soit D_{2n} le groupe diédral d'ordre $2n$ engendré par r d'ordre n et s d'ordre 2 tels que $rs = sr^{-1}$. Autrement dit

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id}\rangle.$$

Exprimer $r^2sr^{-1}s^{-1}r^3s^3$ sous la forme r^is.

Éléments de réponse 770

Nous avons

$$r^2sr^{-1}s^{-1}r^3s^3 = r^2(sr^{-1})s^{-1}r^3(s^2s) = r^2(rs)s^{-1}r^3s = r^2r(ss^{-1})r^3s = r^6s.$$

Exercice 771

Faire la liste de tous les sous-groupes de D_8.

Éléments de réponse 771

Rappelons que

$$\mathrm{D}_8 = \langle r,\, s \,|\, r^4 = s^2 = \mathrm{id},\, rs = sr^{-1}\rangle = \{\mathrm{id},\, r,\, r^2,\, r^3,\, s,\, rs,\, r^2s,\, r^3s\}.$$

Bien entendu $\{\mathrm{id}\}$ et D_8 sont des sous-groupes de D_8.

Le groupe D_8 ne possède que deux éléments d'ordre 4, à savoir r et r^3 Chacun d'eux engendre le groupe $\langle r\rangle$ qui est cyclique d'ordre 4.

Le groupe D_8 possède cinq éléments d'ordre 2 qui sont r^2 et r^is avec $0 \leq i \leq 3$. Il y a donc cinq sous-groupes cycliques d'ordre 2 :

$$\langle r^2\rangle, \qquad \langle s\rangle \qquad \langle rs\rangle \qquad \langle r^2s\rangle \qquad \langle r^{-1}s\rangle.$$

Le groupe D_8 possède un sous-groupe d'ordre 4 non cyclique : $\langle r^2,\, s\rangle$ qui est abélien et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ via

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \langle r^2,\, s\rangle \qquad\qquad (i,j) \mapsto r^{2i}s^j.$$

En effet les groupes $\mathrm{G}_1 = \langle r^2\rangle$ et $\mathrm{G}_2 = \langle s\rangle$ satisfont les propriétés suivantes :

- ◇ $\mathrm{G}_1 \cap \mathrm{G}_2 = \{\mathrm{id}\}$;

◇ G_1 et G_2 commutent ;

◇ $G_1G_2 = \langle r^2, s\rangle$

donc $\langle r, s^2\rangle$ est isomorphe au produit direct de G_1 et G_2, et G_1 et G_2 sont cycliques d'ordre 2.

Le groupe D_8 ne contient pas d'autre sous-groupe ; en effet rappelons que si G est un sous-groupe de D_8, alors $|G|$ divise $|D_8| = 8$, *i.e.* $|G| \in \{1, 2, 4, 8\}$. Nous pouvons récapituler ce qui précède comme suit

$\|G\| = 1$	$\{\mathrm{id}\}$
$\|G\| = 2$	$\langle r^2\rangle$, $\langle s\rangle$, $\langle r, s\rangle$, $\langle r^2, s\rangle$, $\langle r^{-1}, s\rangle$,
$\|G\| = 4$	$\langle r\rangle$, $\langle r^2, s\rangle$,
$\|G\| = 8$	D_8

À isomorphisme près il y a cinq sous-groupes de D_8 : $\{\mathrm{id}\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et D_8.

Exercice 772

Soient E un espace vectoriel euclidien de dimension 3 et S sa sphère unité. Si D est une droite vectorielle de E, on note σ_D la rotation d'angle π autour de D (appelée aussi demi-tour). Par conséquent σ_D appartient au groupe spécial orthogonal $\mathrm{SO}(E)$ dont on rappelle qu'il est engendré par les demi-tours.

1. Soit D une droite vectoriel, soit g un élément de $\mathrm{SO}(E)$. Reconnaître l'endomorphisme $g \circ \sigma_D \circ g^{-1}$.
2. Soit $g \in \mathrm{SO}(E)$. Montrer que g est un demi-tour si et seulement s'il existe $x \in S$ tel que $g(x) = -x$.

   Dans les deux questions suivantes, nous nous donnons un sous-groupe G de $\mathrm{SO}(E)$ agissant transitivement sur S.
3. Montrer que G contient un demi-tour.
4. En déduire que $G = \mathrm{SO}(E)$.

Éléments de réponse 772

1. Les deux endomorphismes g et $g \circ \sigma_D \circ g^{-1}$ sont des rotations et ont même trace. Ces deux rotations ont même angle, ce sont toutes les deux des demi-tours. D est la droite propre pour la valeur propre 1, par suite $g(D)$ est la droite propre de $g \circ \sigma_D \circ g^{-1}$ pour la valeur propre 1. Il s'en suit que $g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)}$.
2. Soit g un élément de $\mathrm{SO}(E)$. Si g est un demi-tour σ_D, alors g a pour matrice dans une base orthonormale adaptée (e_1, e_2, e_3)
$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$
   Nous avons e_2 appartient à S et $g(e_2) = -e_2$.

3. Si G agit transitivement sur S, alors pour un $x \in S$ fixé il existe g tel que $g(x) = -x$ et donc par la question précédente g est un demi-tour dans G.
4. Comme G est un groupe et comme $\mathrm{SO}(E)$ est engendré par les demi-tours il suffit de montrer que G contient tous les demi-tours. D'après la question précédente il existe une droite D telle que σ_D appartient à G. Soit D' une autre droite. Soit $\overrightarrow{u}$ un vecteur directeur unitaire de D et $\overrightarrow{u'}$ un vecteur directeur unitaire de D'. Puisque G agit transitivement sur S il existe g dans G tel que $g(\overrightarrow{u}) = \overrightarrow{u'}$. Ainsi $g(D) = D'$. D'après 1. nous avons
$$g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)} = \sigma_{D'} \in \mathrm{G}.$$

Exercice 773

Soit $n \in \mathbb{N}^*$. Soit G le sous-ensemble de $M(n+1, \mathbb{R})$ donné par les matrices de la forme
$$M = \left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$$
où $A \in \mathrm{GL}(n, \mathbb{R})$ et $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$.

1. Montrer que G est un groupe.
2. Expliciter de quelle manière le groupe affine $\mathrm{GA}(\mathbb{R}^n)$ de R^n est isomorphe au groupe $\mathrm{GL}(n, \mathbb{R}) \ltimes \mathbb{R}^n$. En particulier expliquer comment effectuer la composée de $\varphi, \varphi' \in \mathrm{GA}(\mathbb{R}^n)$ où φ (resp. φ') pour partie linéaire $A \in \mathrm{GL}(n, \mathbb{R})$ (resp. $A' \in \mathrm{GL}(n, \mathbb{R})$) et vecteur de translation $v \in \mathbb{R}^n$ (resp. $v' \in \mathbb{R}^n$).
3. Montrer que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$.

Éléments de réponse 773

1. Montrons qu'il s'agit d'un sous-groupe de $\mathrm{GL}(n+1, \mathbb{R})$.

   L'inverse de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$ est la matrice $\left(\begin{array}{c|c} A^{-1} & \begin{matrix} z_1 \\ \vdots \\ z_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A^{-1}(-x_1, -x_2, \dots, -x_n)$.

   La composée de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$ avec $\left(\begin{array}{c|c} B & \begin{matrix} y_1 \\ \vdots \\ y_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$ est $\left(\begin{array}{c|c} AB & \begin{matrix} x_1 + z_1 \\ \vdots \\ x_n + z_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A(y_1, y_2, \dots, y_n)$. Il s'agit donc bien d'un sous-groupe.

2. Identifions les éléments de $\mathrm{GA}(\mathbb{R}^n)$ qui fixent 0 avec $\mathrm{GL}(\mathbb{R}^n)$. Les translations sont le morphisme du noyau $\mathrm{GA}(\mathbb{R}^n) \to \mathrm{GL}(\mathbb{R}^n)$. Les translations forment un sous-groupe isomorphe à $\mathbb{R}^n$ par l'application $v \in \mathbb{R}^n \mapsto \tau_v$ où τ_v est la translation de vecteur v.

   Si φ, φ' s'écrivent $\varphi = \tau_v \circ A$ et $\varphi' = \tau_{v'} \circ A'$, alors

   $$\varphi \circ \varphi'(x) = A(A'x + v') + v = AA'x + (Av' + v).$$

   La composée $\varphi \circ \varphi'$ a pour partie linéaire AA' et a pour partie translation, la translation de vecteur $Av' + v$.

3. Montrons que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$. L'isomorphisme est donné par

   $$\psi \colon \mathrm{GA}(\mathbb{R}^n) \to \mathrm{G} \qquad\qquad \varphi = \tau_v \circ A \mapsto \left(\begin{array}{c|c} A & \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right)$$

   Il s'agit d'une bijection qui est, d'après 1. et 2., un morphisme de groupes :

   $$\begin{aligned} \psi(\varphi \circ \varphi') &= \left(\begin{array}{c|c} AA' & \begin{matrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} A & \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right) \left(\begin{array}{c|c} A' & \begin{matrix} v'_1 \\ \vdots \\ v'_n \end{matrix} \\ \hline 0 \dots 0 & 1 \end{array}\right) \\ &= \psi(\varphi) + \psi(\varphi') \end{aligned}$$

   où $w = Av'$.

Exercice 774

Soit E un espace affine euclidien de dimension n. On appelle similitude de E toute transformation affine bijective de E dans lui-même dont la partie linéaire est la composée d'une homothétie et d'une isométrie linéaire.

1. Montrer que les similitudes forment un groupe.
2. Soit φ une similitude. Démontrer que si L est la partie linéaire de φ, alors L s'écrit de matrice unique sous la forme $L = HR$ où H est une homothétie linéaire et R un élément de $\mathrm{SO}(n, \mathbb{R})$ et que de plus H et R commutent.

   Soit φ une bijection de E. On dit que φ préserve les angles (non-orientés) si pour tous points $A \neq B$, $C \in E$, $\varphi(A)\widehat{\varphi(B)}\varphi(C) = \widehat{ABC}$. Nous allons montrer que les similitudes sont extactement les transformations qui préservent les angles.

3. Montrer que les similitudes préservent les angles.

   Soit φ une bijection de E qui préservent les angles.

4. Montrer que φ préserve l'alignement.
5. Montrer que φ est affine.

6. Choisissons une origine O dans E. Trouver une translation τ tells que $(\tau^{-1} \circ \varphi)(O) = O$. Posons $\varphi' = \tau^{-1} \circ \varphi$.

7. Soit $A \neq O$. Posons $\lambda = \frac{||\overrightarrow{O\varphi'(A)}||}{||\overrightarrow{OA}||}$. Si h_λ est l'homothétie de rapport λ et de centre O, montrer que $\psi = h_\lambda^{-1} \circ \varphi'$ préserve le produit scalaire et la norme. On pourra utiliser des triangles isométriques.

8. En déduire que ψ est une isométrie et conclure.

Éléments de réponse 774

Désignons par h_λ l'homothétie de rapport λ.

1. Rappelons que les similitudes linéaires sont les composées d'homothéties linéaires de rapport positif et d'isométries linéaires.

   Les similitudes linéaires forment un sous-groupe de $\mathrm{GL}(E)$. En effet soient R, S dans $\mathrm{O}(E)$. Comme $(h_\lambda R)^{-1} = R^{-1}h_\lambda^{-1} = R^{-1}h_{\lambda^{-1}} = h_{\lambda^{-1}}R^{-1}$, $(h_\lambda R)^{-1}$ est une similitude linéaire. De même $(h_\lambda R)(h_\mu S) = h_{\lambda+\mu}T$ où T est l'isométrie linéaire RS donc $(h_\lambda R)(h_\mu S)$ est une similitude linéaire.

   Les similitudes affines sont l'image réciproque des similitudes linéaires par le morphisme $\mathrm{GA}(E) \to \mathrm{GL}(E)$; il s'agit donc d'un sous-groupe du groupe affine $\mathrm{GA}(E)$.

2. Dans l'écriture $L = HR$, HR commutent car H est une homothétie et donc commute avec tous les éléments de $\mathrm{GL}(E)$. Supposons qu'il existe deux écritures $L = h_\lambda R = h_\mu S$ avec R, S isométries linéaires et λ, $\mu > 0$ alors $|\det L| = \lambda = \mu$ et donc $h_\lambda = h_\mu$ et $R = h_{\lambda^{-1}}L = h_{\mu^{-1}}L = S$. Il y a donc bien unicité.

3. Rappelons que l'angle $\widehat{ABC}$ est l'unique réel $\alpha \in [0, \pi]$ tel que

$$\cos\alpha = \frac{\langle \overrightarrow{BA}, \overrightarrow{BC} \rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||}.$$

Soit φ une similitude dont la partie linéaire L s'écrit $h_\lambda R$ avec $R \in \mathrm{O}(E)$. Nous avons

$$\begin{aligned}
\cos(\varphi(A)\widehat{\varphi(B)}\varphi(C)) &= \frac{\langle\overrightarrow{\varphi(B)\varphi(A)},\, \overrightarrow{\varphi(B)\varphi(C)}\rangle}{||\overrightarrow{\varphi(B)\varphi(A)}||\,||\overrightarrow{\varphi(B)\varphi(C)}||} \\
&= \frac{\langle L(\overrightarrow{BA}),\, L(\overrightarrow{BC})\rangle}{||L(\overrightarrow{BA})||\,||L(\overrightarrow{BC})||} \\
&= \frac{\langle h_\lambda R(\overrightarrow{BA}),\, h_\lambda R(\overrightarrow{BC})\rangle}{||h_\lambda R(\overrightarrow{BA})||\,||h_\lambda R(\overrightarrow{BC})||} \\
&= \frac{\lambda^2\langle R(\overrightarrow{BA}), R(\overrightarrow{BC})\rangle}{\lambda^2||R(\overrightarrow{BA})||\,||R(\overrightarrow{BC})||} \\
&= \frac{\langle\overrightarrow{BA},\, \overrightarrow{BC}\rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||} \\
&= \cos(\widehat{ABC})
\end{aligned}$$

Il en résulte que les similitudes préservent les angles.

4. Trois points A, B et C sont alignés si l'angle $\widehat{ABC}$ vaut 0 ou π. Si une transformation préserve les angles, elle préserve donc aussi l'alignement.
5. Puisque E est un espace vectoriel réel de dimension ≥ 2 une application bijective qui préserve l'alignement est affine. C'est le théorème fondamental de la géométrie affine.
6. La translation τ de vecteur $\overrightarrow{O\varphi(O)}$ convient et c'est la seule.
7. Soit $B \in E$. Les triangles OAB et $\psi(O)\psi(A)\psi(B)$ sont isométriques ; en effet ils ont trois angles égaux, $\psi(O) = O$ et $||\overrightarrow{O\psi(A)}|| = ||\overrightarrow{OA}||$. Par conséquent $||\overrightarrow{O\psi(B)}|| = ||\overrightarrow{OB}||$ et ψ est une application linéaire qui préserve la norme. Ensuite pour B, $C \neq O$ puisque ψ préserve les angles et $||\overrightarrow{OB}|| = ||\overrightarrow{OC}||$, on a $\langle\overrightarrow{OB}, \overrightarrow{OC}\rangle = \langle\overrightarrow{O\psi(B)}, \overrightarrow{O\psi(C)}\rangle$. Il s'en suit que ψ est une application linéaire orthogonale qui préserve aussi la norme.
8. Nous avons donc montré que $\varphi = \tau \circ h_\lambda \circ \psi$, *i.e.* la composée d'une translation et d'une similitude linéaire.

Exercice 775 Groupes et propriétés géométriques de l'orbite.

Soit E un espace affine euclidien. Soit f un élément du groupe $\mathrm{Isom}(E)$ des isométries de E. Soit G le sous-groupe de $\mathrm{Isom}(E)$ engendré par f. Soit p un point de E. Montrer que les assertions suivantes sont équivalentes :

(1) L'orbite de p sous G est bornée ;

(2) Toute orbite sous G d'un point de E est bornée ;

(3) f a un point fixe.

Éléments de réponse 775

Montrons que (3) implique (1).

Par hypothèse il existe $m \in E$ tel que $f(m) = m$. Pour tout $k \in \mathbb{N}$ nous avons

$$d(m, f^k(p)) = d(f^k(m), f^k(p)) = d(m, p)$$

ainsi l'orbite de p sous G est bornée.

Montrons que (1) implique (2).

Il existe $r > 0$ tel que $d(p, f^k(p)) \leq r$ pour tout $k \in \mathbb{N}$. Soit m un point de E alors $d(f^k(p), f^k(m)) = d(p, m)$. Par conséquent

$$d(p, f^k(m)) \leq d(p, f^k(p)) + d(f^k(p), f^k(m)) \leq r + d(p, m).$$

Montrons que (2) implique (3).

Le théorème de la forme réduite des isométries de E implique l'existence de $g \in \mathrm{Isom}(E)$ avec un point fixe p et $\overrightarrow{v} \in \ker(f - \mathrm{id}_E)$ tel que $f = t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$. Ainsi $f^k(A) = A + k\overrightarrow{v}$ et donc $d(A, f^k(A)) = k||\overrightarrow{v}|| \to +\infty$ si $\overrightarrow{v} \neq \overrightarrow{0}$. Puisque la suite $(f^k(A))_k$ est bornée nous obtenons que $\overrightarrow{v} = \overrightarrow{0}$ ainsi $f = g$ a un point fixe.

2.2. Géométrie

Exercice 776

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction continue. Montrer que l'ensemble des primitives $F : \mathbb{R} \to \mathbb{R}$ de f est un $\mathbb{R}$-espace affine et donner sa dimension.

Éléments de réponse 776

Exercice 777

Soient A, B deux points distincts de l'espace affine $\mathbb{R}^n$.

1. Montrer que le segment $[A, B]$ est l'ensemble des barycentres des familles $\big((A, \alpha), (B, \beta)\big)$, où $\alpha, \beta \geq 0$ et $(\alpha, \beta) \neq (0, 0)$.
2. Montrer que le droite (AB) est l'ensemble des barycentres des familles $\big((A, \alpha), (B, \beta)\big)$, où $\alpha, \beta \in \mathbb{R}$ et $\alpha + \beta \neq 0$.

Éléments de réponse 777

Exercice 778 [Quelques lieux géométriques]

1. Soient z_1, z_2, z_3 les trois racines du polynôme $P(z) = z^3 - 4z + 8\sqrt{2}$ et A_1, A_2 et A_3 les points du plan complexe d'affixes respectives z_1, z_2 et z_3. Quelle est l'affixe de l'isobarycentre de A_1, A_2 et A_3 ?

2. Soient A, B, C trois points de l'espace affine $\mathbb{R}^n$. Déterminer l'ensemble des points $M \in \mathbb{R}^n$ tels que
$$\overrightarrow{MA} - 2\overrightarrow{MB} + \overrightarrow{MC} \;=\; \vec{0}.$$
3. Soient A, B, C trois points du plan affine $\mathbb{R}^2$. Déterminer l'ensemble des points $M \in \mathbb{R}^2$ tels que
$$\|2\overrightarrow{MA} - \overrightarrow{MB} + 2\overrightarrow{MC}\| \;=\; \|\overrightarrow{MA} + \overrightarrow{MB} + \overrightarrow{MC}\|.$$

Éléments de réponse 778

Exercice 779

Dans l'espace affine $\mathbb{R}^3$, soient $ABCD$ un tétraèdre et S, T, U, V les points définis par
$$\overrightarrow{AS} \;=\; \frac{1}{2}\overrightarrow{AB}, \quad \overrightarrow{AU} \;=\; \frac{1}{3}\overrightarrow{AD}, \quad \overrightarrow{DT} \;=\; \frac{1}{2}\overrightarrow{DC}, \quad \overrightarrow{BV} \;=\; \frac{1}{3}\overrightarrow{BC}.$$

1. Exprimer respectivement S, T, U, V comme barycentres de A, B, de A, D, de D, C et de B, C avec des coefficients que l'on explicitera.
2. Utiliser ce qui précède pour montrer que les points S, T, U et V sont coplanaires.

Éléments de réponse 779

Exercice 780

Cnsidérons l'ensemble
$$X \;:=\; \left\{ \begin{pmatrix} 1+2a+b & 1-b \\ 0 & a+b \end{pmatrix} \;;\; (a,b) \in \mathbb{R}^2 \right\}$$

1. Montrer que X est un sous-espace affine de $M_2(\mathbb{R})$.
2. Donner un point de X.
3. Donner la direction de X.

Éléments de réponse 780

Exercice 781

Soit E l'ensemble des fonctions $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ telles que $f(x) + f(-x) = 1$ pour tout $x \in \mathbb{R}$.

1. Montrer que E est un sous-espace affine de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
2. Donner un point de E.
3. Donner la direction de E.

Éléments de réponse 781

Exercice 782

Montrer que l'ensemble des matrices réelles de taille $n \times n$ dont la trace vaut 2 est un hyperplan affine de $M_n(\mathbb{R})$ (i.e. un sous-espace affine de dimension $\dim M_n(\mathbb{R}) - 1$) dont on précisera la direction.

Éléments de réponse 782

Exercice 783

Soient X et Y deux espaces affines de directions respectives E et F. Soit $f\colon X \to Y$ une application affine de partie linéaire $\overrightarrow{f} : E \to F$.

1. Soit X' un sous-espace affine de X de direction E'. Montrer que $f(X')$ est un sous-espace affine de Y de direction $\overrightarrow{f}(E')$.
2. Soit Y' un sous-espace affine de Y de direction F'. Montrer que si $f^{-1}(Y')$ est non vide, alors $f^{-1}(Y')$ est un sous-espace affine de X de direction $(\overrightarrow{f})^{-1}(F')$.
3. Donner un exemple où $f^{-1}(Y')$ est vide.

Éléments de réponse 783

Exercice 784

Soient X et Y deux espaces affines de directions respectives E et F. Soit $f\colon X \to Y$ une application affine de partie linéaire $\overrightarrow{f}\colon E \to F$.

1.a) Montrer que $f\colon X \to Y$ est injective si et seulement si $\overrightarrow{f}\colon E \to F$ est injective.

1.b) Montrer que $f\colon X \to Y$ est surjective si et seulement si $\overrightarrow{f}\colon E \to F$ est surjective.

1.c) Montrer que $f\colon X \to Y$ est bijective si et seulement si $\overrightarrow{f}\colon E \to F$ est bijective.

2.a) Montrer que si f (ou de façon équivalente $\overrightarrow{f}$) est injective, alors f transforme une droite en une droite.

3.b) En déduire que les translations et les homothéties (de rapport non nul) transforment une droite en une droite.

3.a) Montrer que si f (ou de façon équivalente $\overrightarrow{f}$) est injective, alors f transforme deux droites parallèles en deux droites parallèles.

3.b) En déduire que les translations et les homothéties (de rapport non nul) transforment deux droites parallèles en deux droites parallèles.

Éléments de réponse 784

Exercice 785 [Sur les homothéties et les translations]
Soit X un espace affine de direction E.

1. Quelles sont les homothéties $h\colon X \to X$ de partie linéaire $\overrightarrow{h} = \mathrm{Id}_E$? Quels sont leurs points fixes ?
2. Soit $\lambda \in \mathbb{R} \setminus \{0, 1\}$. Montrer que $h\colon X \to X$ est une application affine de partie linéaire $\lambda \mathrm{Id}_E$ si et seulement si h est une homothétie de rapport λ. Quels sont les points fixes d'une telle application ?
3. Soient f, $g\colon X \to X$ deux applications affines. Montrer que $f \circ g$ est affine de partie linéaire $\overrightarrow{f} \circ \overrightarrow{g}$. En déduire que la composition :
   (a) de deux translations est une translation,
   (b) de deux homothéties, de rapports non nuls λ et λ', est une homothétie de rapport $\lambda\lambda'$ si $\lambda\lambda' \neq 1$ (préciser son centre) et une translation sinon (préciser le vecteur associé),
   (c) de deux symétries centrales (*i.e.* de deux homothéties de rapport -1) est une translation (préciser le vecteur associé),
   (d) d'une symétrie centrale et d'une translation est une symétrie centrale (préciser son centre).

Éléments de réponse 785

Exercice 786 [**Projections affines**]
Soient X un espace affine de direction E et Y un sous-espace affine de X de direction F. Soit $G \subset E$ un supplémentaire de F dans E, *i.e.* un sous-espace vectoriel de E tel que $F \oplus G = E$.

1. Soit $M \in X$. Montrer qu'il existe un unique $M' \in Y$ tel que $\overrightarrow{MM'} \in G$ (faire un dessin). On appelle M' le projeté de M sur Y parallèlement à G.
2. Montrer que l'application $p\colon X \to X$ définie par $p(M) = M'$ pour tout $M \in X$ est une projection (*i.e.* vérifie $p \circ p = p$) et qu'elle est affine, de partie linéaire la projection vectorielle sur F parallèlement à G.

Éléments de réponse 786

Exercice 787
Dans le plan affine $\mathbb{R}^2$, soient A, B, C trois points tels que $\overrightarrow{AB}$ et $\overrightarrow{AC}$ ne soient pas colinéaires. Soit D le point tel que $(ABCD)$ soit un parallélogramme. Quelles sont les coordonnées de D dans le repère $(A; \overrightarrow{AB}, \overrightarrow{AC})$ (pourquoi est-ce un repère ?) ?

Éléments de réponse 787

Exercice 788

Dans le plan affine $\mathbb{R}^2$ considérons A et B deux points distincts. Soit O le milieu du segment $[A, B]$. En utilisant les produits scalaires, démontrer les résultats (connus) suivants :

1. les points M tels que $d(M, A) = d(M, B)$ décrivent la médiatrice du segment $[A, B]$,
2. les points M tels que $\overrightarrow{MA} \perp \overrightarrow{MB}$ décrivent le cercle de centre O et de rayon $\frac{d(A,B)}{2}$.

Éléments de réponse 788

Exercice 789 [**Inégalité de Cauchy-Schwarz et inégalité triangulaire**]

Soient u et v deux vecteurs de $\mathbb{R}^n$.

1. Démontrer l'inégalité de Cauchy-Schwarz lorsque $v = 0$.
2. On suppose $v \neq 0$. Soit $x \in \mathbb{R}$. En développant le produit scalaire $(u + x.v \,|\, u + x.v)$, montrer l'inégalité de Cauchy-Schwarz.
3. En déduire l'inégalité triangulaire.

Éléments de réponse 789

Exercice 790

Soient A, B, C trois points non alignés du plan affine $\mathbb{R}^2$. Soit G le centre de gravité du triangle ABC (*i.e.* l'isobarycentre de A, B, C).

1. Rappeler pourquoi les médianes de ABC se coupent en G.
2. Rappeler pourquoi les médiatrices de ABC sont concourantes. On note O leur point de concours.
3. On note respectivement A', B', C' le milieu du segment $[B, C]$, $[A, C]$, $[A, B]$. En considérant l'homothétie $h_{G,-2}$ de centre G et de rapport -2, montrer que les trois hauteurs de ABC sont concourantes. On note H leur point de concours.

   Indication. Montrer qu'une homothétie transforme une droit en une droite parallèle.
4. Montrer que O, G et H sont alignés et vérifient la relation d'Euler : $\overrightarrow{OH} = 3\overrightarrow{OG}$.

Éléments de réponse 790

Exercice 791 [**Cercles d'Appolonius**]

Soient A et B deux points distincts du plan affine $\mathbb{R}^2$. Soit $k \in \mathbb{R}^{+*}$. On s'intéresse à l'ensemble S_k des points M du plan tels que $\frac{d(A,M)}{d(B,M)} = k$.

1. Déterminer la nature de S_1.

   On suppose dans la suite que $k \neq 1$.
2. Soit $M \in \mathbb{R}^2$. Montrer que $M \in S_k$ si et seulement si $\overrightarrow{MA} + k\overrightarrow{MB} \perp \overrightarrow{MA} - k\overrightarrow{MB}$.

3. En introduisant des barycentres bien choisis, en déduire que S_k est un cercle dont on précisera les caractéristiques.

Éléments de réponse 791

Exercice 792 [**Projection orthogonale, Distance à un sous-espace affine**]

Soient F un sous-espace vectoriel de $\mathbb{R}^n$, Y un sous-espace affine de $\mathbb{R}^n$ de direction F et $F^\perp$ l'orthogonal de F.

1. Soit $M \in \mathbb{R}^n$. Montrer qu'il existe un unique $M' \in Y$ tel que $\overrightarrow{MM'} \in F^\perp$ (faire un dessin). On appelle M' le projeté orthogonal de M sur Y.
2. Soient $A \in \mathbb{R}^n$ et $B \in Y$. Montrer que $d(A, Y) = d(A, B)$ si et seulement si $B = p(A)$. Autrement dit : $p(A)$ est l'unique point de Y minimisant la distance de A à Y (faire un dessin).

Éléments de réponse 792

Exercice 793

Soient F un sous-espace vectoriel de $\mathbb{R}^n$ et $F^\perp$ son orthogonal. On rappelle le résultat suivant, admis en cours : $F \oplus F^\perp = \mathbb{R}^n$. En déduire que $(F^\perp)^\perp = F$.

Éléments de réponse 793

Exercice 794

1.a) Dans $\mathbb{R}^2$, donner une équation de la droite passant par $A = (1, 1)$ et $B = (3, -2)$. Même question avec $C = (1, 2)$ et $D = (-2, 1)$.

1.b) Dans $\mathbb{R}^2$, donner une équation de la droite passant par $C = (1, 2)$ et $D = (-2, 1)$.

2. Dans $\mathbb{R}^2$, donner une équation de la droite passant par $A = (2, 3)$ et orthogonale à la droite dirigée par $\overrightarrow{u} = (1, 2)$.

3.a) Dans $\mathbb{R}^3$,donner une équation du plan contenant $A = (1, 2, 3)$, $B = (0, 1, 0)$ et $C = (0, 0, 1)$.

3.b) Dans $\mathbb{R}^3$,donner une équation du plan contenant $C = (0, 0, 1)$, $D = (0, 0, 2)$ et $E = (1, 0, 1)$.

4. Dans $\mathbb{R}^3$, donner une équation du plan passant par $A = (1, 2, 3)$ et orthogonal à la droite dirigée par $\overrightarrow{u} = (1, 2, 3)$.

Éléments de réponse 794

Exercice 795

1. Donner une équation paramétrique de la droite $D \subset \mathbb{R}^2$ d'équation $3x + 2y - 1 = 0$.
2. Donner une équation paramétrique du plan $P \subset \mathbb{R}^3$ d'équation $3x + 2y - z + 1 = 0$.

3. Donner une équation paramétrique de la droite $D \subset \mathbb{R}^3$ définie par les équations $3x+y-z-2=0$ et $x+y=0$. On montrera d'abord qu'il s'agit bien d'une droite.

Éléments de réponse 795

Exercice 796

1. Dans $\mathbb{R}^2$ considérons $A=(x_0,y_0)$ et D la droite d'équation $ax+by+c=0$, où $(a,b)\neq(0,0)$. Calculer $d(A,D)$.
2. Dans $\mathbb{R}^3$ considérons $A=(x_0,y_0,z_0)$ et P le plan d'équation $ax+by+cz+d=0$, où $(a,b,c)\neq(0,0,0)$. Calculer $d(A,P)$.

Éléments de réponse 796

Exercice 797

Soit $D\subset\mathbb{R}^3$ la droite dirigée par $\overrightarrow{u}=(2,-1,0)$ et passant par $A=(0,1,1)$. Calculer $d(B,D)$, où $B=(1,1,-2)$.

Éléments de réponse 797

Exercice 798 [**Produit vectoriel**]

On rappelle la définition du produit vectoriel : pour tous $\overrightarrow{u}_1=(a_1,b_1,c_1)$ et $\overrightarrow{u}_2=(a_2,b_2,c_2)$ dans $\mathbb{R}^3$,

$$\overrightarrow{u}_1\wedge\overrightarrow{u}_2 \;:=\; (b_1c_2-c_1b_2\,,\,c_1a_2-a_1c_2\,,\,a_1b_2-b_1a_2)\;\in\;\mathbb{R}^3\,.$$

1. Montrer que, pour tout $(x,y,z)\in\mathbb{R}^3$,
$$\begin{vmatrix} x & a_1 & a_2\\ y & b_1 & b_2\\ z & c_1 & c_2\end{vmatrix} \;=\; \big(\,\overrightarrow{u}_1\wedge\overrightarrow{u}_2\,|\,(x,y,z)\,\big)\,.$$
2. En déduire que $\overrightarrow{u}_1\wedge\overrightarrow{u}_2=\overrightarrow{0}$ si et seulement si $\overrightarrow{u}_1$ et $\overrightarrow{u}_2$ sont colinéaires et que, dans le cas contraire, $(\overrightarrow{u}_1,\overrightarrow{u}_2,\overrightarrow{u}_1\wedge\overrightarrow{u}_2)$ est une base de $\mathbb{R}^3$. Rappeler, dans ce dernier cas, l'équation du plan vectoriel $\mathrm{Vect}(\overrightarrow{u}_1,\overrightarrow{u}_2)$.
3. Montrer que $\overrightarrow{u}_1\perp\overrightarrow{u}_1\wedge\overrightarrow{u}_2$ et que $\overrightarrow{u}_2\perp\overrightarrow{u}_1\wedge\overrightarrow{u}_2$.
4. Supposons que $\overrightarrow{u}_1$ et $\overrightarrow{u}_2$ ne soient pas colinéaires. Soit $P\subset\mathbb{C}^3$ un plan dirigé par le plan vectoriel $\mathrm{Vect}(\overrightarrow{u}_1,\overrightarrow{u}_2)$ et $D\subset\mathbb{C}^3$ une droite. Montrer que D et P sont orthogonaux si et seulement si D est dirigée par la droite vectorielle $\mathrm{Vect}(\overrightarrow{u}_1\wedge\overrightarrow{u}_2)$.

Éléments de réponse 798

Exercice 799 [Intersection de deux plans]

Dans $\mathbb{R}^3$, soient P_1 et P_2 les plans d'équations $a_1x+b_1y+c_1z+d_1=0$, $(a_1,b_1,c_1)\neq 0$, et $a_2x+b_2y+c_2z+d_2=0$, $(a_2,b_2,c_2)\neq 0$.

1. Montrer que P_1 et P_2 sont parallèles si et seulement si (a_1, b_1, c_1) et (a_2, b_2, c_2) sont colinéaires.
2. Dans le cas contraire, montrer que $P_1 \cap P_2$ est une droite, dirigée par $\mathrm{Vect}((a_1, b_1, c_1) \wedge (a_2, b_2, c_2))$.

Éléments de réponse 799

Exercice 800

1. Déterminer la composée de deux symétries vectorielles orthogonales planes.
2. Déterminer l'ordre de la composée de deux symétries vectorielles orthogonales planes.

Éléments de réponse 800

1. Le déterminant d'une symétrie orthogonale est -1 ; la composée $r = s's$ de deux telles symétries s et s' est donc une isométrie directe, c'est-à-dire une rotation.

   Déterminons l'angle θ de la rotation à partir des axes respectifs $\mathbb{R}\overrightarrow{u}$ et $\mathbb{R}\overrightarrow{u'}$ ($\overrightarrow{u}$ et $\overrightarrow{u'}$ unitaires) des symétries s et s'. Pour cela il suffit de déterminer l'image de $\overrightarrow{u}$ par r, ou plutôt l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$. Puisque $s(\overrightarrow{u}) = \overrightarrow{u}$ nous avons $r(\overrightarrow{u}) = s'(\overrightarrow{u})$ donc l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$ est aussi l'angle $(\overrightarrow{u}, s'(\overrightarrow{u}))$. Comme une symétrie renverse l'orientation nous avons
   $$(\overrightarrow{u}, \overrightarrow{u'}) = -(s'(\overrightarrow{u}), s'(\overrightarrow{u'}))$$
   d'où
   $$(\overrightarrow{u}, \overrightarrow{u'}) = (s'(\overrightarrow{u'}), s'(\overrightarrow{u})).$$
   Puisque $\overrightarrow{u'}$ appartient à l'axe de s' nous obtenons
   $$(\overrightarrow{u}, \overrightarrow{u'}) = (\overrightarrow{u'}, s'(\overrightarrow{u})).$$
   Il en résulte que
   $$\theta = (\overrightarrow{u}, s'(\overrightarrow{u})) = (\overrightarrow{u}, \overrightarrow{u'}) + (\overrightarrow{u'}, s'(\overrightarrow{u})) = 2(\overrightarrow{u}, \overrightarrow{u'})$$
   Notons que $\overrightarrow{u}$ peut être remplacé par $-\overrightarrow{u}$ ou $\overrightarrow{u'}$ par $-\overrightarrow{u'}$. L'angle $(\overrightarrow{u}, \overrightarrow{u'})$ n'est donc défini qu'à π près à partir de la donnée des deux symétries (ce n'est pas étonnant : la seule donnée intrinsèque est l'angle de droites $(\mathbb{R}\overrightarrow{u}, \mathbb{R}\overrightarrow{u'})$). Mais grâce à la multiplication par 2 l'angle θ se trouve être bien défini à 2π près.
2. Déterminons l'ordre de cette composée. L'ordre d'une rotation est infini si l'angle de la rotation n'est pas égal à $\frac{2k\pi}{n}$ pour n et k entiers. L'ordre de la rotation d'angle $\frac{2k\pi}{n}$ pour n et k premiers entre eux est n.

Exercice 801

1. Montrer que toute rotation plane se décompose en le produit de deux symétries.

2. Que pouvons-nous dire pour les rotations de l'espace ?

Éléments de réponse 801

1. Montrons que toute rotation plane se décompose en le produit de deux symétries.

   D'après l'exercice précédent on peut décomposer toute rotation plane d'angle θ en le produit de deux symétries orthogonales : l'axe de la première est choisi au hasard, l'axe de la seconde fait un angle de $\frac{\theta}{2}$ avec la première.

2. Il y a un résultat analogue pour une rotation de l'espace d'axe $\mathbb{R}u$ et d'angle θ. Elle se décompose en le produit de deux symétries orthogonales par rapport à deux plans vectoriels contenant $\mathbb{R}u$ et qui font un angle égal à $\frac{\theta}{2}$ entre eux : la restriction de la rotation au plan vectoriel orthogonal à $\mathbb{R}u$ est une rotation plane.

Exercice 802

Quelle est la matrice de la rotation de $\mathbb{R}^3$ d'angle θ autour de l'axe $\mathbb{R}e_2$?

Éléments de réponse 802

Le vecteur e_2 est vecteur propre pour la valeur propre 1 de la matrice, *i.e.* c'est un vecteur fixe pour la rotation considérée.

L'image de e_1 est dans le plan (e_1, e_3) et est égale à $\cos\theta e_1 - \sin\theta e_3$.

L'image de e_3 est dans le plan (e_1, e_3) et est égale à $\sin\theta e_1 + \cos\theta e_3$.

La matrice cherchée est donc

$$\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$$

Exercice 803

Soit $M \in \mathrm{O}(3,\mathbb{R})$ de déterminant -1. Montrer que -1 est valeur propre de M.

Éléments de réponse 803

Puisque une isométrie vectorielle conserve les normes, ses valeurs propres sont de module 1. Ceci est donc vrai pour une matrice M de $\mathrm{O}(3,\mathbb{R})$ qui est la matrice d'une isométrie vectorielle. Si de plus $\det M = -1$, alors le produit des racines du polynôme caractéristique de M est -1. Par suite

- ou bien toutes les racines du polynôme caractéristique de M sont réelles et dans ce cas l'une ou trois d'entre elles sont égales à -1 ;
- ou bien deux d'entre elles sont complexes conjuguées, leur produit étant égal à 1 la dernière est -1.

Exercice 804

Soit M une matrice orthogonale 2×2 et de déterminant -1.

Montrer que M est la matrice d'une symétrie orthogonale.

Éléments de réponse 804

Les racines du polynôme caractéristique de M sont de module 1. Si elles sont complexes conjuguées mais dans ce cas le déterminant de M est 1 : contradiction. Elles sont donc toutes les deux réelles, l'une valant 1 et l'autre -1.

Il s'en suit que M est la matrice de la symétrie orthogonale d'axe la droite vectorielle propre associée à la valeur propre 1.

Exercice 805

Soit $M \in \mathrm{SO}(3, \mathbb{R})$ la rotation d'angle θ. Montrer que

$$\cos\theta = \frac{1}{2}\Big(\mathrm{Tr}\, M - 1\Big).$$

Éléments de réponse 805

Si M est la matrice d'une rotation d'angle θ, alors M est semblable à la matrice

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Par suite $\mathrm{Tr}\, M = 2\cos\theta + 1$ et $\cos\theta = \frac{1}{2}\Big(\mathrm{Tr}\, M - 1\Big)$.

Exercice 806

Soit s une symétrie plane d'axe $\mathcal{D}$.

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrer que la composée $t \circ s$ (resp. $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.
2. Soit r une rotation de centre C. Montrer que la composée $r \circ s$ (resp. $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.
3. Soient s' et s'' deux symétries axiales. Montrer que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

Éléments de réponse 806

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrons que la composée $t \circ s$ (resp. $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.

   Supposons $\overrightarrow{v}$ normal à $\mathcal{D}$. Soit $t'(\mathcal{D}') = \mathcal{D}'$ où t' est la translation de vecteur $\overrightarrow{v}/2$. La droite $\mathcal{D}'$ est une droite de points fixes par ts qui est donc la symétrie orthogonale d'axe $\mathcal{D}'$.

Soit t'' la translation de vecteur $-\overrightarrow{v}/2$. Posons $\mathcal{D}'' = t''(\mathcal{D})$. La droite $\mathcal{D}''$ est une droite de points fixes par st qui est donc la symétrie orthogonale d'axe $\mathcal{D}''$.

Si ts est une symétrie orthogonale s' et si A est un point de l'axe de symétrie, nous avons $ts(A) = A$ donc $\overrightarrow{s(A)A} = \overrightarrow{v}$. Par suite $\overrightarrow{v}$ est normal à la droite $\mathcal{D}$ et d'après ce qui précède st est une symétrie orthogonale.

Si st est une symétrie, nous arrivons à la même conclusion.

2. Soit r une rotation de centre C. Montrons que la composée $r \circ s$ (resp. $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que C appartienne à $\mathcal{D}$. Soit θ l'angle de la rotation r. Considérons la rotation r' de centre C et d'angle $-\frac{\theta}{2}$. Alors $\mathcal{D}' = r'(\mathcal{D})$ est une droite de points fixes de $s \circ r$ qui est une symétrie d'axe $\mathcal{D}'$.

   Soit r'' la rotation de centre C et d'angle $\frac{\theta}{2}$. Alors $\mathcal{D}'' = r''(\mathcal{D})$ est une droite de points fixes de $r \circ s$ qui est une symétrie d'axe $\mathcal{D}''$.

   Réciproquement supposons que $r \circ s$ soit une symétrie orthogonale d'axe $\mathcal{D}'$. Soit C' l'intersection de $\mathcal{D}$ et $\mathcal{D}'$. Nous avons $rs(C') = C'$ ainsi que $s(C') = C'$. Par conséquent $C' = r(C')$ et C' est le centre de la rotation r, c'est-à-dire C qui est donc sur $\mathcal{D}$. Dans ce cas $s \circ r$ est aussi une symétrie orthogonale.

   La conclusion est identique en supposant a priori que $s \circ r$ est une symétrie.

3. Soient s' et s'' deux symétries axiales. Montrons que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient sécants en un point C. Alors $s' \circ s''$ est une rotation de centre C et d'après 2. $ss's''$ est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient parallèles alors $s' \circ s''$ est une translation de vecteur orthogonal à la direction commune et d'après 1. $ss's''$ est une symétrie si et seulement si cette direction commune est celle de $\mathcal{D}$.

Exercice 807

Montrer que pour une translation t de vecteur $\overrightarrow{u}$ et une symétrie s d'axe $\mathcal{D}$ nous avons $t \circ s = s \circ t$ si et seulement si $\overrightarrow{u}$ est dans la direction de $\mathcal{D}$.

Éléments de réponse 807

Si $st = ts$, alors pour tout point M de $\mathcal{D}$ nous avons $st(M) = ts(M) = t(M)$ donc $t(M)$ appartient à $\mathcal{D}$ et $\overrightarrow{u} = \overrightarrow{Mt(M)}$ est parallèle à $\mathcal{D}$.

Réciproquement supposons que $\overrightarrow{u}$ soit parallèle à $\mathcal{D}$. Posons $M' = ts(M)$ et $M'' = st(M)$. Nous avons $\overrightarrow{Ms(M)} = \overrightarrow{t(M)s(t(M))} = \overrightarrow{t(M)M''}$. Par conséquent $\overrightarrow{s(M)M''} = \overrightarrow{Mt(M)} = \overrightarrow{u}$ et donc $\overrightarrow{s(M)M''} = \overrightarrow{s(M)t(s(M))} = \overrightarrow{s(M)M'}$ $M'' = M'$. Il s'en suit que $st = ts$.

Exercice 808

Soit $\mathcal{R}$ l'ensemble des points à coordonnées entières dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$.
Quelles sont les isométries affines qui conservent $\mathcal{R}$?

Éléments de réponse 808

Si une isométrie affine qui conserve l'ensemble $\mathcal{R}$ a exactement un point fixe, c'est une rotation autour de l'un des points de $\mathcal{R}$ d'angle $\frac{k\pi}{2}$, ou une rotation d'angle $\frac{k\pi}{2}$ autour de l'un des centres des carrés du type $[O, A, B, C]$ où O est le centre du repère, A a pour coordonnées $(1, 0)$, B a pour coordonnées $(1, 1)$, C a pour coordonnées $(0, 1)$. Enfin il y a aussi les symétries centrales autour des milieux des segments du type OA, AB, BC et CO.

Si une isométrie affine qui conserve l'ensemble $\mathcal{R}$ a une droite de points fixes, alors c'est une symétrie orthogonale par rapport aux droites du type OA, AB, BC et CO (côtés des carrés du type $[O, A, B, C]$) ainsi que AC et OC (diagonales des carrés du type $[O, A, B, C]$) et des médiatrices des segments OA et AB.

Si une isométrie affine qui conserve l'ensemble $\mathcal{R}$ n'a pas de point fixe, alors soit c'est une translation de vecteur $\in \mathbb{Z}e_1 + \mathbb{Z}e_2$ (où (e_1, e_2) est la base canonique de $\mathbb{R}^2$), soit c'est un produit d'une translation de ce type avec les autres isométries affines déjà trouvées.

Exercice 809

Soit $\mathfrak{S}$ la représentation graphique dans un repère orthonormal de la fonction sinus.
Quelles sont les isométries affines qui conservent la figure $\mathfrak{S}$?

Éléments de réponse 809

La figure $\mathfrak{S}$ est conservée par la rotation de centre l'origine du repère et d'angle π, par les translations de vecteurs $2k\pi e_1$ pour $k \in \mathbb{Z}$ et par les composées de telles applications.

Exercice 810

Déterminer les isométries affines qui conservent l'ensemble $\mathfrak{F}$ des points de coordonnées $(n, 0)$, $n \in \mathbb{Z}$, dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$ du plan affine euclidien.

Éléments de réponse 810

La figure $\mathfrak{F}$ est l'ensemble des points à coordonnées entières de l'axe des abscisses. Elle est conservée par

- ◇ les rotations de centre les points de $\mathfrak{F}$ ou les milieux des segments joignant deux points de $\mathfrak{G}$ et d'angle π,
- ◇ la symétrie orthogonale par rapport à l'axe des x,
- ◇ la symétrie orthogonale par rapport à n'importe quelle droite verticale qui passe par des points de $\mathfrak{F}$ ou par le milieu du segment joignant deux points de $\mathfrak{F}$,
- ◇ toutes les translations de vecteur $\in \mathbb{Z}e_1$,
- ◇ les composées de telles applications.

Exercice 811

Caractériser géométriquement l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est

$$A = \frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$$

Éléments de réponse 811

Les vecteurs colonnes de la matrice sont des vecteurs unitaires deux à deux orthogonaux. La matrice est donc orthogonale. De plus son déterminant est 1. Par suite A appartient à $\mathrm{SO}(3,\mathbb{R})$. La matrice A est donc une matrice de rotation. En réduisant nous obtenons que la trace de A vaut $1 + 2\cos\theta$ où θ est l'angle de la rotation (bien défini au signe près). Comme la trace de A vaut 2 nous avons $\cos\theta = \frac{1}{2}$ et $\theta = \frac{\pi}{3}$. L'axe correspond à la droite propre pour la valeur propre 1. Nous avons

$$3(A - \mathrm{Id}) = \begin{pmatrix} -1 & -1 & 2 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{pmatrix}$$

Cet axe est donc la droite engendrée par le vecteur $(1,1,1)$.

Exercice 812

Soient A et B deux éléments de $\mathrm{SO}(3,\mathbb{R})$. Donner une condition géométrique nécessaire et suffisante pour que A et B commutent (cette conditions fait intervenir des droites particulières de $\mathbb{R}^3$ associées à A et B).

Éléments de réponse 812

Si A ou B est l'identité, alors A et B commutent.

Supposons que ni A, ni B ne soit l'identité. Ce sont alors deux rotations d'angle non nul. Si A et B commutent, alors l'axe de B est laissé invariant par A et l'axe de A est laissé invariant par B. Notons $\mathcal{D}_A$ l'axe de A et $\mathcal{P}_A$ son orthogonal (qui est donc dans le plan de rotation de A). Soit $\mathcal{D}$ une droite invariante par A, il s'agit donc d'une droite propre pour A. Si A n'est pas un demi-tour, la seule droite invariante pour A est son axe (car A n'a que 1 comme valeur propre) ; si A est un demi-tour, il y a en plus le sous-espace propre associé à -1 qui est $\mathcal{P}_A$. Un raisonnement analogue s'applique à B. Il s'en suit que si A et B commutent, alors A et B ont même axe ou alors ce sont des demi-tours et leurs axes sont orthogonaux.

Réciproquement supposons que A et B aient même axe $\mathcal{D}$. Choisisons une base orthonormale telle que le premier vecteur soit un vecteur directeur de $\mathcal{D}$. Dans cette base A et B s'écrivent

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\beta) & -\sin(\beta) \\ 0 & \sin(\beta) & \cos(\beta) \end{pmatrix}$$

où α et β sont les angles respectifs de A et B. Un calcul matriciel montre alors que A et B commutent.

De même si A et B sont des demi-tour d'axes orthogonaux alors dans une base orthonormale où les deux premiers vecteurs sont des vecteurs directeurs des axes de A et B nous avons

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

et par conséquent A et B commutent.

CHAPITRE 3

APPENDICE 2 : EXERCICES, ANNEAUX ET CORPS

Exercice 813

1. L'ensemble $\{b\sqrt{3} \,|\, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?
2. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?
3. L'ensemble $\{a + b\pi \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?
4. L'ensemble $\{a + b\sqrt{9} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?
5. L'ensemble $\{a + b\sqrt[3]{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?
6. L'ensemble $\{a + b\sqrt{3} + c\sqrt{5} \,|\, a, b, c \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un anneau ?

Éléments de réponse 813 à compléter

1. L'ensemble $\{b\sqrt{3} \,|\, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un anneau.
2. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est un anneau.
3. L'ensemble $\{a+b\pi \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est-pas un anneau.
4. L'ensemble $\{a + b\sqrt{9} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est un anneau.
5. L'ensemble $\{a + b\sqrt[3]{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un anneau.

6. L'ensemble $\{a + b\sqrt{3} + c\sqrt{5} \,|\, a, b, c \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un anneau.

Exercice 814

1. L'ensemble $\{b\sqrt{3} \,|\, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?
2. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?
3. L'ensemble $\{a + b\pi \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?
4. L'ensemble $\{a + b\sqrt{9} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?
5. L'ensemble $\{a + b\sqrt[3]{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?
6. L'ensemble $\{a + b\sqrt{3} + c\sqrt{5} \,|\, a, b, c \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est-il un corps ?

à compléter

Éléments de réponse 814

1. L'ensemble $\{b\sqrt{3} \,|\, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un corps.
2. L'ensemble $\{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est un corps.
3. L'ensemble $\{a + b\pi \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un corps.
4. L'ensemble $\{a + b\sqrt{9} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels est un corps.
5. L'ensemble $\{a + b\sqrt[3]{3} \,|\, a, b \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un corps.
6. L'ensemble $\{a + b\sqrt{3} + c\sqrt{5} \,|\, a, b, c \in \mathbb{Q}\}$ muni de l'addition et de la multiplication des réels n'est pas un corps.

3.1. Anneaux et morphismes entre anneaux

Exercice 815

Vérifier que l'ensemble $\{*\}$ muni de la seule addition et de la seule multiplication possible est un anneau pour lequel $0 = 1 = *$.

Éléments de réponse 815

Toutes les égalités à vérifier sont forcément vérifiées puisque de part et d'autre de l'égalité on ne peut avoir que $*$ comme résultat.

Exercice 816

Montrer que le seul anneau pour lequel $0 = 1$ est l'anneau réduit à un élément 0 avec l'addition $0 + 0 = 0$ et $0 \cdot 0 = 0$.

Éléments de réponse 816

Commençons par remarquer que dans un anneau $0 \cdot a$ vaut toujours 0. En effet $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Par suite, en ajoutant $-(0 \cdot a)$ de chaque côté de l'égalité, on trouve $0 = 0 \cdot a$. Si A est un anneau dans lequel $0 = 1$, alors $a = 1 \cdot a = 0 \cdot a = 0$, *i.e.* tout élément est nul.

Exercice 817

Trouver deux matrices M et N de taille 2×2 telles que $MN \neq NM$.

Éléments de réponse 817

Presque tous les couples de matrices conviennent. Si $M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $N = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$, alors $NM = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix}$ tandis que $MN = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$.

Exercice 818

Considérons un ensemble à trois éléments $\{0, 1, 2\}$. Montrer qu'il existe au plus une façon de construire une table d'addition et de multiplication qui donne une structure d'anneau.

Éléments de réponse 818

- L'addition avec 0 est entièrement déterminée : $0 + a = a$ pour tout a.
- Pour l'addition avec 1, il faut trouver les valeurs possibles pour $1 + 1$ et $1 + 2$:
  - ◇ Déterminons $1 + 1$.
    Si $1 + 1 = 1$, après addition de l'inverse -1 de 1 pour l'addition, nous obtenons $1 = 0$ ce qui est exclu. Si $1 + 1 = 0$, alors l'inverse -2 de 2 ne pourrait être ni 1 ni 0 car ces nombres sont les inverses respectifs de 1 et 0. Donc l'inverse -2 de 2 serait 2, *i.e.* $2 + 2 = 0$. Mais alors on ne peut pas donner de valeur raisonnable à $2 + 1$: pas 0 car 1 et 2 ne sont pas inverses, pas 1 car $2 \neq 0$ et pas 2 car $1 \neq 0$. La contradiction ne peut être levée que si $1 + 1 \neq 0$. La seule possibilité restante est donc $1 + 1 = 2$.
  - ◇ Déterminons $1 + 2$.
    Puisque $1 + 1 = 2$, 1 n'est pas son propre inverse. L'élément 1 doit avoir un inverse -1 qui ne peut être ni 0, ni 1, donc c'est 2 : $1 + 2 = 0$. Il reste à déterminer $2 + 2$:
    $$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 0 + 1 = 1.$$

La table d'addition est maintenant entièrement terminée.

Pour la table de multiplication, la multiplication avec 0 est connue : $0 \cdot a = 0$ pour tout élément a. En effet $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Par suite, en ajoutant $-(0 \cdot a)$ de chaque côté de l'égalité, on trouve $0 = 0 \cdot a$.

Par définition du neutre mutliplicatif 1, nous avons $1 \cdot a = a$.

Il reste uniquement à déterminer $2 \cdot 2$:

$$2 \cdot 2 = (1+1) \cdot 2 = 1 \cdot 2 + 1 \cdot 2 = 2 + 2 = 1$$

Ainsi nous avons les tables

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Exercice 819

Trouver l'élément neutre pour l'addition dans l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Trouver l'élément neutre pour la multiplication dans l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 819

Si $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, alors le neutre pour l'addition est $(\overline{0}, \overline{0})$ tandis que le neutre pour la multiplication est $(\overline{1}, \overline{1})$.

Exercice 820

Montrer que les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne diffèrent pas l'un de l'autre par un simple changement de nom des éléments.

Éléments de réponse 820

Les tables de $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ sont respectivement

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

et

$+$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(0,1)$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(0,1)$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$

$\cdot$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$

Dans $\mathbb{Z}/4\mathbb{Z}$ il y a un élément a tel que $a^2 = \overline{0}$, c'est $a = 2$.

Supposons qu'il existe un isomorphisme d'anneaux

$$\phi\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Alors

$$\big(\phi(a)\big)^2 \overset{\phi \text{ iso}}{=} \phi(a^2) \overset{a^2 = \overline{0}}{=} \phi(\overline{0}) \overset{\phi \text{ iso}}{=} \overline{0}.$$

Autrement dit il existe b non nul dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tel que $b^2 = \overline{0}$: contradiction (cf table de multiplication de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Les deux anneaux ne sont donc pas isomorphes.

Exercice 821

Vérifier pour chacun des exemples $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}[X]$, { fonctions de $\mathbb{R}$ dans $\mathbb{R}$} que vous savez qui sont les éléments 0 et 1 et que vous comprenez comment on fait la multiplication, l'addition et qui est l'élément $-a$ associé à un élément a.

Éléments de réponse 821

Additionner et multiplier des fractions, des complexes ou des polynômes ne posent pas de problèmes. La seule difficulté concerne les fonctions. Si f et g sont deux fonctions, on définit leur somme par sa valeur en tout point : $(f+g)(x) = f(x)+g(x)$ et de même pour la multiplication. Le neutre pour l'addition est la fonction constante égale à 0 tandis que le neutre pour la

multiplication est la fonction constante égale à 1. La fonction $-f$ inverse de la fonction f est celle qui en tout point x prend la valeur $-f(x)$.

Exercice 822

Dresser les tables d'addition et de multiplication de l'ensemble $\mathbb{Z}/6\mathbb{Z}$.
Vérifier que les éléments $\overline{0}$ et $\overline{1}$ satisfont les propriétés voulues dans un anneau.
Vérifier avec $a = \overline{2}$, $b = \overline{3}$, $c = \overline{4}$ que la distributivité est vérifiée.

Éléments de réponse 822

Les tables d'addition et de multiplication de l'ensemble $\mathbb{Z}/6\mathbb{Z}$ sont :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

À l'aide de ces tables on vérifie facilement que

◇ d'une part

$$a \cdot (b + c) = \overline{2} \cdot (\overline{3} + \overline{4}) \overset{\text{table}}{=} \overline{2} \cdot \overline{1} \overset{\overline{1} \text{ neutre pour } \cdot}{=} \overline{2};$$

◇ d'autre part

$$a \cdot b + a \cdot c = \overline{2} \cdot \overline{3} + \overline{2} \cdot \overline{4} \overset{\text{table}}{=} \overline{0} + \overline{2} \overset{\overline{0} \text{ neutre pour } +}{=} \overline{2}.$$

Exercice 823

Vérifier que la différence entre deux multiples de 6 est encore un multiple de 6.

De même, vérifier que le produit entre un multiple de 6 et un entier quelconque est encore un multiple de 6.

Éléments de réponse 823

Si $a = 6x$ et $b = 6y$ sont deux multiples de 6, alors $a - b = 6(x - y)$ est un multiple de 6.

Si $a = 6x$ et c est quelconque, alors $ac = 6xc$ est bien un multiple de 6.

Autrement dit $6\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$.

Exercice 824

Écrire les tables d'addition et de multiplication de l'anneau produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Éléments de réponse 824

$+$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{2})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{2})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{0},\overline{0})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{0},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{2})$
$(\overline{1},\overline{2})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{1})$

$\cdot$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{2})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{2})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{2})$
$(\overline{0},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$

Exercice 825

Vérifier que les lois d'addition et de multiplication données sur le produit $A \times B$ définissent bien un anneau.

Éléments de réponse 825

Montrons par exemple la distributivité et l'existence d'un inverse pour l'addition :

◇ Pour la distributivité il faut voir

$$(a_1, b_1)\big((a_2, b_2) + (a_3, b_3)\big) = (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3).$$

Or d'une part

$$\begin{aligned}(a_1, b_1)\big((a_2, b_2) + (a_3, b_3)\big) &= (a_1, b_1)(a_2 + a_3, b_2 + b_3)\\ &= \big(a_1(a_2 + a_3), b_1(b_2 + b_3)\big)\\ &= (a_1a_2 + a_1a_3, b_1b_2 + b_1b_3)\end{aligned}$$

et d'autre part

$$\begin{aligned}(a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3) &= (a_1a_2, b_1b_2) + (a_1a_3, b_1b_3)\\ &= (a_1a_2 + a_1a_3, b_1b_2 + b_1b_3)\end{aligned}$$

d'où $(a_1, b_1)\big((a_2, b_2) + (a_3, b_3)\big) = (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3)$.

◇ Soit $(a, b) \in A \times B$. L'addition

$$(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0_A, 0_B)$$

montre que (a, b) admet bien un inverse, à savoir $(-a, -b)$.

Exercice 826

1. Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.
2. Soit $\mathbb{Z}[x^n]$ l'ensemble des polynômes défini par

$$\mathbb{Z}[x^n] = \{\, \sum a_i x^i \,|\, a_i \neq 0 \Rightarrow \, i \text{ est un multiple de } n.\}$$

L'ensemble $\mathbb{Z}[x^n]$ est-il un sous-anneau de $\mathbb{Z}[x]$?

3. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui s'annulent au point $x = 3$ forme-t-il un sous-anneau de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$?

Éléments de réponse 826

1. Un sous-anneau de $\mathbb{Z}$ doit contenir 0 et 1 par définition donc aussi $\underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}} = n$.

Par suite il contient tous les nombres positifs. Mais s'il contient un nombre positif n, il contient aussi son inverse $-n$. Ainsi un sous-anneau de $\mathbb{Z}$ contient tous les éléments de $\mathbb{Z}$. Par conséquent il est égal à $\mathbb{Z}$.

2. Les polynômes constants 0 et 1 sont bien dans $\mathbb{Z}[x^n]$. Soient deux polynômes $P = \sum p_i x^{in}$ et $Q = \sum q_i x^{in} \in \mathbb{Z}[x^n]$. Alors $-P = \sum(-p_i)x^{in}$ est bien dans $\mathbb{Z}[x^n]$ ainsi que $P + Q = \sum(p_i + q_i)x^{in}$. Pour le produit nous avons la formule $PQ = \sum_k (\sum_{i+j=k} p_i q_j)x^{kn}$ qui est bien une somme de monômes dont les exposants sont multiples de n. Il en résulte que $\mathbb{Z}[x^n]$ est un sous-anneau de $\mathbb{Z}[x]$.
3. Non, l'ensemble des fonctions s'annulant en 3 ne forme pas un sous-anneau de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. En effet la fonction constante 1 (le neutre multiplicatif) n'est pas dans cet ensemble.

Exercice 827

Vérifier que les propriétés

- $\diamond$ $0 \cdot x = 0$;
- $\diamond$ l'inverse $-a$ est unique, *i.e.* $a + b = a + c = 0 \Rightarrow b = c$;
- $\diamond$ $-1 \cdot a + a = 0$.

sont vérifiées dans tout anneau.

Éléments de réponse 827

- $\diamond$ Puisque $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, en ajoutant $-(0 \cdot a)$ de chaque côté de l'égalité on obtient $0 = 0 \cdot a$.
- $\diamond$ Pour montrer que l'inverse est unique, si $a+b = a+c$, nous obtenons en ajoutant l'inverse $-a$ des deux côtés de l'égalité la relation voulue $b = c$.
- $\diamond$ Enfin $-1 \cdot a + a = -1 \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0$.

Exercice 828

Soit f l'unique morphisme $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Que valent $f(5)$ et $f(-2)$?

Éléments de réponse 828

Posons $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. L'élément $f(5)$ vaut $\overline{1}$ et $f(-2)$ vaut $\overline{2}$.

3.2. L'anneau $\mathbb{Z}$

Exercice 829

1. Montrer que les inversibles de $\mathbb{Z}$ sont 1 et -1.
2. Montrer que pour un élément $z \in \mathbb{Z}$, les trois conditions suivantes sont équivalentes :
   a) z est irréductible ;
   b) z est différent de 1 et -1 et les seuls éléments qui divisent z sont 1, -1, z et $-z$.

c) la valeur absolue $|z|$ de z est un nombre premier.

Éléments de réponse 829

1. Les éléments 1 et -1 sont inversibles d'inverse respectif 1 et -1. L'élément nul n'est pas inversible : pour tout a nous avons $0 \cdot a = 0 \neq 1$. Enfin un élément a différent de 0, 1, -1 ne peut être inversible. En effet, $|a| > 1 > 0$; par suite l'inverse b de a vérifie $0 < |b| = \frac{1}{|a|} < 1$ ce qui n'est pas possible puisque $b \in \mathbb{Z}$.
2. Montrons que *a*) $\Rightarrow$ *b*). Si z est irréductible, alors il est différent de 1 et -1 puisque non inversible. Soit a un diviseur de z : $z = ab$. Si a est inversible, alors $a = 1$ ou $a = -1$. Sinon, puisque z est irréductible, c'est b qui est inversible et qui vaut 1 ou -1 ; dans ce cas a vaut z ou $-z$. Un diviseur a de z est donc bien dans l'ensemble $\{1, -1, z, -z\}$.

   Montrons que *b*) $\Rightarrow$ *c*) par contraposée. Supposons que $|z|$ n'est pas un nombre premier de sorte que $|z| = pq$ avec q et q différents de 1. Alors l'écriture $z = p\frac{z}{p}$ montre que z n'est pas irréductible car p et $\frac{z}{p}$ ne sont pas inversibles.

   Montrons que *c*) $\Rightarrow$ *a*). Soit z un nombre entier de valeur absolue un nombre premier. Montrons que z est irréductible. Soit $z = pq$ une écriture en produit. Nous avons $|z| = |p|\,|q|$ qui est une écriture du nombre premier $|z|$ en produit. Il en résulte que $|p|$ ou $|q|$ est égal à 1. Autrement dit p (ou q) vaut ± 1 et est inversible.

Exercice 830

1. Montrer que l'ensemble $12\mathbb{Z} = \{\ldots, -24, -12, 0, 12, 24, \ldots\}$ est un idéal de $\mathbb{Z}$. Nous le désignerons par le seul symbole (12).
2. Donner un idéal plus grand que (12) au sens de l'inclusion.
3. Montrer que l'ensemble $12\mathbb{Z}$ est le plus petit idéal de $\mathbb{Z}$ contenant le nombre 12.
4. Donner sans démonstration une généralisation de cet énoncé.
5. Montrer que $(12) = (-12)$.
6. Y a-t-il d'autres a tels que $(12) = (a)$?

Éléments de réponse 830

1. Si $a = 12x$ et $b = 12y$ sont deux multiples de 12, alors $a - b = 12(x - y)$ est un multiple de 12. Si c est quelconque, alors $ac = 12xc$ est bien un multiple de 12.
2. L'idéal $(6) = \{\ldots, -24, -18, -12, -6, 0, 6, 12, 18, 24, \ldots\}$ est plus grand que (12).
3. Si un idéal contient le nombre 12, alors il contient tous les multiples $12a$ de 12 par définition d'un idéal, *i.e.* il contient $12\mathbb{Z} = (12)$.
4. L'idéal (a) est le plus petit idéal contenant le nombre a.

5. Puisque (12) contient le nombre -12, il contient le plus petit idéal contenant le nombre -12, à savoir (-12), *i.e.* $(12) \supset (-12)$. Par symétrie $(-12) \supset (12)$. Finalement $(12) = (-12)$.
6. Soit a un nombre tel que $(12) = (a)$. Puisque a appartient à (a), a appartient à (12), c'est-à-dire par définition de l'idéal (12), $a = 12b$. Par symétrie entre a et 12, il existe c tel que $12 = ac$. D'où $12 = 12bc$, c'est-à-dire $bc = 1$. Comme b et c appartiennent à $\mathbb{Z}$, b et c valent ± 1, *i.e.* $a = 12$ ou $a = -12$. Les seuls nombres a tels que $(a) = (12)$ sont donc 12 et -12.

Exercice 831

Trouver un exemple dans la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$ qui montre qu'on peut avoir $b = \lambda\mu b$ sans avoir $\lambda\mu = 1$ ou $b = 0$.

Éléments de réponse 831

Nous avons $\overline{2} = \overline{3} \cdot \overline{1} \cdot \overline{2}$ et $\overline{2} \neq \overline{0}$, $\overline{3} \cdot \overline{1} \neq \overline{1}$.

Exercice 832

Si A est un anneau non intègre et $a \in A$, donner une condition sur a pour qu'on puisse simplifier par a (indication : examiner la démonstration faite pour caractériser les anneaux intègres).

Éléments de réponse 832

Nous pouvons simplifier dans un anneau par un élément a (*i.e.* $ab = ac \Rightarrow b = c$) si a n'est pas diviseur de 0, *i.e.* si le seul d tel que $ad = 0$ est $d = 0$.

Exercice 833

1. Montrer que deux idéaux (a) et (b) dans un anneau intègre A sont égaux si et seulement si a et b sont associés.
2. En particulier si $A = \mathbb{Z}$, les éléments b tels que $(a) = (b)$ sont $b = a$ et $b = -a$.

Éléments de réponse 833

1. Supposons $(a) = (b)$. Si $a = b = 0$, alors a et b sont associés. Si $(a, b) \neq (0, 0)$, supposons quitte à échanger le rôle de a et b que $b \neq 0$. Puisque $a \in (a)$, nous avons $a \in (b)$, c'est-à-dire, par définition de (b), $a = bc$ pour un certain c. Par symétrie entre a et b il existe d tel que $b = ad$. D'où $b = bcd$. Comme l'anneau est intègre, nous pouvons simplifier par $b \neq 0$, d'où $cd = 1$. Puisque c et d sont inversibles a et b sont associés.

   Réciproquement, montrons que si a et b sont associés, alors $(a) = (b)$. Supposons donc que a et b soient associés. Par symétrie il suffit de montrer que $(a) \subset (b)$. Étant donné qu'il existe c inversible tel que $a = bc$, $a \in (b)$ par définition de (b). Comme (b) est un idéal, s'il contient a il contient tous les multiples de a. Autrement dit $(a) \subset (b)$.

2. Plaçons-nous dans le cas particulier $A = \mathbb{Z}$. Les éléments b tels que $(a) = (b)$ sont $b = a$ et $b = -a$.

Exercice 834

Les propositions suivantes sont-elles équivalentes ?

◇ a et b sont associés.

◇ a divise b et b divise a.

Éléments de réponse 834

Dans un anneau intègre les propositions sont équivalentes. En effet d'une part a divise b peut se traduire par $(b) \subset (a)$ et d'autre part b divise a peut se traduire par $(a) \subset (b)$. Ainsi a divise b et b divise a peut se traduire par $(a) = (b)$. Mais d'après l'exercice précédent $(a) = (b)$ si et seulement si a et b sont associés (dans un anneau intègre). Finalement a divise b et b divise a si et seulement si a et b sont associés.

Exercice 835

1. Soit A un anneau ; si a et b sont deux éléments de A, nous désignons par (a, b) l'ensemble
$$\{r \in A \,|\, \exists\, x,\, y \in A,\, r = ax + by\}.$$
Montrons que le plus petit idéal de l'anneau A contenant les éléments a et b est (a, b).
2. Énoncer sans démonstration une généralisation décrivant le plus petit idéal contenant des éléments $a_1,\, a_2,\, \ldots,\, a_n$.

Éléments de réponse 835

1. Si un idéal contient les éléments a et b, alors puisqu'un idéal est stable par multiplication par un élément quelconque, il contient nécessairement les nombres ax et by ; comme un idéal est stable par somme, il contient $ax + by$ pour tous x, y. Par suite un idéal contenant a et b contient (a, b).

   Montrons que (a, b) est un idéal. Si $m = ax + by$ et $n = a'x + b'y$ sont deux éléments de (a, b), alors $m - n = (a - a')x + (b - b')y$ est bien dans (a, b). Si p est un élément quelconque, alors $mp = (ap)x + (bp)y$ appartient à (a, b). Il en résulte que (a, b) est un idéal.

   Finalement le plus petit idéal d'un anneau A contenant les éléments a et b est l'ensemble (a, b).
2. Le plus petit idéal contenant les éléments $a_1,\, a_2,\, \ldots,\, a_n$ est l'ensemble

   $(a_1,\, a_2,\, \ldots,\, a_n) = \{r \in A \,|\, \exists\, x_1,\, x_2,\, \ldots,\, x_n \in A \text{ t.q. } r = a_1x_1 + a_2x_2 + \ldots + a_nx_n\}$

   Autrement dit, le plus petit idéal contenant les a_i est l'ensemble des combinaisons linéaires des a_i à coefficients dans A.

Exercice 836

1. Calculer un générateur de l'idéal $(30, 36)$.
2. Calculer un générateur de l'idéal $(30, 36, 10)$.

Éléments de réponse 836

1. Par définition

$$(30, 36) = \{r \in \mathbb{Z} \,|\, \exists\, x_1,\, x_2 \in A \text{ t.q. } r = 30x_1 + 36x_2\}$$

Nous en déduisons

$$\begin{aligned}
(30, 36) &= \{30x_1 + 36x_2 \,|\, x_1,\, x_2 \in A\} \\
&= \{30x_1 + (30 + 6)x_2 \,|\, x_1,\, x_2 \in A\} \\
&= \{30(x_1 + x_2) + 6x_2 \,|\, x_1,\, x_2 \in A\} \\
&= \{30y_1 + 6x_2 \,|\, y_1,\, x_2 \in A\} \\
&= \{6(5y_1) + 6x_2 \,|\, y_1,\, x_2 \in A\} \\
&= \{6(5y_1 + x_2) \,|\, y_1,\, x_2 \in A\} \\
&= \{6y_2 \,|\, y_2 \in A\} \\
&= (6)
\end{aligned}$$

2. D'après a) nous avons $(30, 36, 10) = (6, 10)$. Les divisions $10 = 1 \times 6 + 4$, $6 = 1 \times 4 + 2$ et $4 = 2 \times 2 + 0$ assurent que $(6, 10) = (6, 4) = (4, 2) = (2)$. Un générateur de l'idéal $(30, 36, 10)$ est donc (2).

Exercice 837

1. Si d est un pgcd des a_i dans $\mathbb{Z}$, quels sont les autres pgcd des a_i ?
2. Un anneau principal est un anneau dans lequel touts les idéaux sont principaux. Traiter la question précédente dans un anneau principal et intègre quelconque.

Éléments de réponse 837

1. Un pgcd est un générateur a d'un idéal. Or nous avons vu qu'un nombre a tel que $(a) = \mathcal{I}$ est défini au signe près dans $\mathbb{Z}$. Les deux pgcd possibles sont donc a et $-a$.
2. Plaçons-nous dans un anneau intègre ; nous avons vu en exercice que les générateurs d'un idéal sont définis à multiplication par un inversible près. Autrement dit si a et b sont deux pgcd, il existe un élément c inversible tel que $a = bc$ (remarque : puisque dans $\mathbb{Z}$ les inversibles sont 1 et -1 nous retrouvons bien le fait qu'un pgcd est défini au signe près).

Exercice 838

Rappelons la définition suivante : Soit d un générateur de l'idéal $(a_1, a_2, \ldots, a_n)$, *i.e.* un nombre tel que $(d) = (a_1, a_2, \ldots, a_n)$. Alors d est un pgcd des a_i. La réciproque est vrai : si d est un pgcd des a_i, alors $(d) = (a_1, a_2, \ldots, a_n)$.

Calculer $\text{pgcd}(12, 20)$ avec cette définition de pgcd et vérifier que cela correspond à ce que vous attendiez.

Éléments de réponse 838

Les divisions $20 = 1 \times 12 + 8$, $12 = 1 \times 8 + 4$, $8 = 2 \times 4 + 0$ montrent que $(20, 12) = (12, 8) = (8, 4) = (4)$. Le pgcd (au signe près) est donc 4.

Si nous écrivons les décompositions $20 = 2 \times 2 \times 5$ et $12 = 2 \times 2 \times 3$, nous retrouvons que les termes en commun sont $2 \times 2 = 4$.

Exercice 839

Soient $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_n$ sont des idéaux d'un anneau A. Montrer que l'intersection $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \ldots \cap \mathcal{I}_n$ est un idéal de A.

Éléments de réponse 839

Si x et y sont dans $\mathcal{I}$, alors, par définition de l'intersection, ils sont dans chaque $\mathcal{I}_k$; par conséquent $x - y$ est dans chaque $\mathcal{I}_k$ puisque $\mathcal{I}_k$ est un idéal. Il s'en suit que $x - y$ appartient à $\mathcal{I}$.

Le même type de raisonnement montre que si a est un élément quelconque, alors ax appartient à $\mathcal{I}$.

Il en résulte que $\mathcal{I}$ est un idéal.

Exercice 840

Relire la démonstration de l'existence et de l'unicité de la factorisation des entiers de $\mathbb{Z}$ et dire à quel endroit a été utilisé (implicitement) la description des idéaux de $\mathbb{Z}$, dans l'existence ou dans l'unicité ?

Éléments de réponse 840

Après avoir relu la démonstration de l'existence et de l'unicité de la factorisation des entiers de $\mathbb{Z}$ nous pouvons dire que nous avons utilisé (implicitement) la description des idéaux de $\mathbb{Z}$ dans l'unicité. En fait nous avons utilisé le Corollaire 44 qui vient du théorème de Bezout et le théorème de Bezout a lui-même été établi en montrant que les idéaux de $\mathbb{Z}$ sont principaux.

Exercice 841

Soient $z = z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n}$ et $w = w_1^{b_1} w_2^{b_2} \ldots w_p^{b_p}$ deux nombres entiers différents de 0 et 1 et leur décomposition en puissance d'irréductibles deux à deux distincts.

1. Dire pourquoi on peut supposer que $p = n$ et que $z_i = w_i$ pour tout entier i. On se place désormais dans ce cadre.

2. Rappeler comment on calcule le pgcd et le ppcm à partir de cette décomposition.
3. Donner une démonstration de votre affirmation pour le pgcd.

Éléments de réponse 841

1. Il suffit d'ajouter des éléments avec des puissances 0. Par exemple pour $6 = 2 \cdot 3$ et $5 = 5$ nous pouvons prendre les décompositions $6 = 2^1 3^1 5^0$ et $5 = 2^0 3^0 5^1$.
2. Si $z = z_1^{a_1} z_2^{a_2} \dots z_n^{a_n}$ et $w = z_1^{b_1} z_2^{b_2} \dots z_n^{b_n}$, alors en posant $M_i = \max(a_i, b_i)$ et $m_i = \min(a_i, b_i)$, nous avons
$$\text{pgcd}(z, w) = \prod z_i^{m_i}, \qquad \text{ppcm}(z, w) = \prod z_i^{M_i}.$$
3. Il est clair $D = \prod z_i^{m_i}$ divise à la fois z et w. Pour montrer que ce nombre est bien le pgcd il suffit de montrer que c'est le plus grand diviseur. Soit d un diviseur commun à z et w ; soit $d = \prod z_i^{d_i}$ la décomposition de z en facteurs premiers. Pour montrer que d divise D (donc que D est plus grand au sens de la divisibilité) il suffit de voir que d_i est plus petit que $m_i = \min(a_i, b_i)$. Par symétrie il suffit de traiter le cas $i = 1$. Notons que $z_1^{d_1}$ divise d et que d divise z. Par conséquent $z_1^{d_1}$ divise $z = z_1^{a_1} z_2^{a_2} \dots z_n^{a_n}$. Étant donné que $z_1^{d_1}$ est premier avec $z_2^{a_2} z_3^{a_3} \dots z_n^{a_n}$ il divise $z_1^{a_1}$. Mais ceci n'est possible que si $d_1 \leq a_1$. Un raisonnement analogue montre que $d_1 \leq b_1$; finalement nous obtenons donc que $d_1 \leq \min(a_1, b_1) = m_1$.

Exercice 842

Calculer le ppcm de 28 et 36.

Éléments de réponse 842

Le pgcd d est tel que $(d) = (28, 36)$. Les divisions $36 = 1 \times 28 + 8$, $28 = 3 \times 8 + 4$ et $8 = 4 \times 2$ montrent que $(28, 36) = (4)$. Par suite le pgcd est 4 et le ppcm est $\frac{28 \times 36}{4} = 7 \times 36$.

Exercice 843

1. Considérons trois nombres a_1, a_2, $a_3 \in \mathbb{Z}$. On procède de la façon suivante. On calcule le ppcm m_{12} de a_1 et a_2, puis le ppcm m_{123} de m_{12} et de a_3. Montrer que m_{123} est le ppcm des a_i.
2. Calculer le ppcm de 28, 36, 45 par cette méthode.
3. Généraliser à un nombre quelconque d'éléments.

Éléments de réponse 843

1. Considérons trois nombres a_1, a_2 et $a_3 \in \mathbb{Z}$. Soit m_{12} le ppcm de a_1 et a_2. Soit m_{123} le ppcm de m_{12} et a_3. Montrons que m_{123} est le ppcm des a_i. Soient
$$a_1 = \prod n_i^{m_i}, \qquad a_2 = \prod n_i^{p_i}, \qquad a_3 = \prod n_i^{r_i}$$
les décompositions en puissances d'irréductibles de a_1, a_2, respectivement a_3. Alors $m_{12} = \prod n_i^{\max(m_i,p_i)}$ et $m_{123} = \prod n_i^{\max(\max(m_i,p_i),r_i)}$ tandis que $\text{ppcm}(a_1,a_2,a_3) = \prod n_i^{\max(m_i,p_i,r_i)}$. À partir de $\max(\max(m_i,p_i),r_i) = \max(m_i,p_i,r_i)$, nous obtenons que $m_{123} = \text{ppcm}(a_1,a_2,a_3)$.
2. Calculons le ppcm de 28, 36 et 45 par cette méthode. Nous avons vu dans un exercice précédent que $\text{ppcm}(28,36) = 7 \times 36$. Par ailleurs
$$\text{ppcm}(7 \times 36, 45) = 9\text{ppcm}\left(7 \times \frac{36}{9}, \frac{45}{9}\right) = 9\text{ppcm}(7 \times 4, 5) = 9 \times 7 \times 4 \times 5 = 1260.$$
d'où $\text{ppcm}(28,26,45) = 9 \times 14 \times 4 \times 5$.
3. Généralisons à un nombre quelconque d'éléments. Si $m_{12\ldots k}$ est le ppcm des nombres a_1, a_2, …, a_k, nous avons la formule $m_{12\ldots k} = \text{ppcm}(m_{12\ldots k-1}, a_k)$.

Exercice 844

1. Calculer le pgcd et le ppcm de 6557 et 6873 par votre ancienne méthode.
2. Calculer le pgcd et le ppcm de 6557 et 6873 avec les nouvelles méthodes.

Éléments de réponse 844

— Il est extrêmement difficile de trouver les facteurs de ces nombres à la main...

— Les divisions
$$6873 = 1 \times 6557 + 316, \quad 6557 = 316 \times 20 + 237, \quad 316 = 237 \times 1 + 79, \quad 237 = 3 \times 79$$
montrent que $\text{pgcd}(6557, 6873) = 79$. Il en résulte que $\text{ppcm}(6557, 6873) = \frac{6557 \times 6873}{79} = 570459$.

Exercice 845

Rappeler la propriété universelle de $\mathbb{Z}$.

Éléments de réponse 845

Rappelons la propriété universelle de $\mathbb{Z}$: soit A un anneau, il existe un unique morphisme d'anneaux $f\colon \mathbb{Z} \to A$; ce morphisme est défini par les formules $f(n) = n \cdot 1$ et $f(-n) = -n \cdot 1$ pour n positif.

Exercice 846

Posons $M_i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $i \in \mathbb{Z}$. Vérifier les formules $M_i + M_j = M_{i+j}$ et $M_i M_j = M_{ij}$.

Vérifier les formules $M_i + M_j = M_{i+j}$ et $M_i M_j = M_{ij}$.

Éléments de réponse 846

Un calcul direct montrent que $M_i + M_j = M_{i+j}$ et $M_i M_j = M_{ij}$.

Exercice 847

Vérifier que l'anneau A contenant les matrices $M_i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $i \in \mathbb{Z}$, et $\mathbb{Z}$ sont deux anneaux isomorphes.

Éléments de réponse 847

Vérifions que l'anneau A contenant les matrices $M_i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $i \in \mathbb{Z}$ et $\mathbb{Z}$ sont deux anneaux isomorphes.

Considérons l'application $f\colon \mathbb{Z} \to A$ qui envoie 1 sur M_1, bien définie par propriété universelle de $\mathbb{Z}$. Cette application envoie i sur M_i (rappelons la propriété universelle de $\mathbb{Z}$: soit A un anneau, il existe un unique morphisme d'anneaux $f\colon \mathbb{Z} \to A$; ce morphisme est défini par les formules $f(n) = n \cdot 1$ et $f(-n) = -n \cdot 1$ pour n positif.). Nous avons

$$f(i+j) = M_{i+j} = M_i + M_j = f(i) + f(j)$$

d'après l'exercice précédent. De même $f(ij) = f(i)f(j)$. De plus $f(1) = M_1$ et M_1 est le neutre multiplicatif de A. Il s'en suit que f est un morphisme d'anneaux ; de plus il est bijectif : c'est donc un isomorphisme.

Exercice 848

Soient A et B deux anneaux isomorphes. Montrer que si A contient un élément de carré nul, alors B contient également un élément de carré nul.

Éléments de réponse 848

Soit $f\colon A \to B$ un isomorphisme d'anneaux. Soit $a \in A$ l'élément de carré nul. Soit $b \in B$ son image par f : $f(a) = b$. Nous avons

$$b^2 = b \cdot b = f(a) \cdot f(a) = f(a \cdot a) = f(a^2) = f(0) = 0.$$

Par suite B contient un élément de carré nul, à savoir b.

Exercice 849

1. Montrer que les inversibles de $\mathbb{Q}[x]$ sont les polynômes constants non nuls.
2. Montrer qu'on ne peut pas remplacer $\mathbb{Q}$ par $\mathbb{Z}$ dans la question précédente.
   Par quoi peut-on remplacer $\mathbb{Q}$?

Éléments de réponse 849

1. Soit P un polynôme inversible. Montrons que P est une constante. Soit Q l'inverse de P, *i.e.* $PQ = 1$. D'après la formule des degrés $\deg P + \deg Q = 0$. La seule possibilité est $\deg P = \deg Q = 0$, autrement dit P et Q sont des constantes non nulles.

   Réciproquement si $P = p$ est une constante non nulle, alors P est un polynôme inversible d'inverse le polynôme constant $\frac{1}{p} \in \mathbb{Q}$.
2. La constante $3 \in \mathbb{Z}[X]$ n'est pas inversible. Nous pouvons remplacer $\mathbb{Q}$ par un corps quelconque.

Exercice 850

Soit A un anneau commutatif, soit a un élément de A. Montrer que si a est inversible et si $a = a_1 a_2 \dots a_n$ est une décomposition de a sous forme d'un produit, alors tous les a_i sont inversibles.

Éléments de réponse 850

Par symétrie il suffit de montrer que a_1 est inversible. Soit b l'inverse de a. L'écriture $1 = ab = a_1 \cdot (a_2 a_3 \dots a_n b)$ montre que a_1 est inversible d'inverse $a_2 a_3 \dots a_n b$ (rappelons que comme A est commutatif il suffit de vérifier qu'il existe b dans A tel que $ab = 1$).

Exercice 851

Vérifier que la relation « être le plus petit au sens de la divisibilité » est une relation d'ordre sur $\mathbb{N}$.

Éléments de réponse 851

Cela donne pour la relation de divisibilité :

- $\diamond$ x divise x : c'est vrai : $x = x \times 1$;
- $\diamond$ si x divise y et y divise z, *i.e.* $y = kx$ et $z = \ell y$, alors $z = (\ell k)x$ ce qui montre que x divise z d'où le second point ;
- $\diamond$ si x divise y et y divise x, alors $y = kx$ et $x = \ell y$ donc $x = k\ell x$. Si $x \neq 0$, alors $k\ell = 1$ et comme k et ℓ sont positifs (nous travaillons dans $\mathbb{N}$) nous avons $k = \ell = 1$ et $x = y$. Enfin si $x = 0$, alors $y = kx = 0 = x$ également.

3.3. Anneau quotient et anneau produit

Exercice 852

1. Montrer que la relation $\mathcal{R}$ définie sur $\mathbb{Z}^2$ par $a\mathcal{R}b$ si a est congru à b modulo $d \in \mathbb{Z}$ est une relation d'équivalence.
2. Montrer que si $d \neq 0$, il existe un unique nombre r tel que $a \equiv r\ (d)$ et tel que $0 \leq r < |d|$.

Éléments de réponse 852

1. Il faut montrer que la relation est réflexive, symétrique et transitive, c'est-à-dire que
   - $\diamond$ $x\mathcal{R}x : x \equiv x\ (d)$ pour tout x ;
   - $\diamond$ $x\mathcal{R}y \Rightarrow y\mathcal{R}x : x \equiv y\ (d) \Rightarrow y \equiv x\ (d)$;
   - $\diamond$ $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z : x \equiv y\ (d)$ et $y \equiv z\ (d) \Rightarrow x \equiv z\ (d)$.

   Le premier point est immédiat : $x - x = 0$ est divisible par d donc $x \equiv x\ (d)$.

   Passons au second point. Si $y - x$ est divisible par d, alors $y - x = kd$ pour un certain k dans $\mathbb{Z}$; ainsi $x - y = \underbrace{(-k)}_{\in\mathbb{Z}} d$ et $x - y$ est divisible par d.

   Enfin si $y - x$ est divisible par d et $z - y$ est divisible par d, alors $y - x = kd$ pour un certain $k \in \mathbb{Z}$ et $z - y = \ell d$ pour un certain $\ell \in \mathbb{Z}$. Il en résulte que
   $$z - x = z + \underbrace{(-y + y)}_{0} - x = (z - y) + (y - x) = \ell d + kd = \underbrace{(\ell + k)}_{\in\mathbb{Z}} d$$
   i.e. $z - x$ est divisible par d ou encore $x\mathcal{R}z$.
2. Soit $d \in \mathbb{Z}$, $d \neq 0$. Supposons qu'il existe deux nombres distincts r_1 et r_2 tels que $a \equiv r_1\ (d)$, $0 \leq r_1 < |d|$ et $a \equiv r_2\ (d)$, $0 \leq r_2 < |d|$. Quitte à réindicer les r_i supposons que $r_1 \geq r_2$. En particulier $a - r_1 = kd$ pour un certain $k \in \mathbb{Z}$ et $a - r_2 = \ell d$ pour un certain $\ell \in \mathbb{Z}$. Ainsi
   $$r_1 - r_2 = (a - kd) + (\ell d - a) = \ell d - kd = (\ell - k)d.$$
   Finalement d'une part $r_1 - r_2$ est divisible par d et d'autre part $0 \leq r_1 - r_2 < |d|$ (en effet par hypothèse $r_1 \geq r_2$ et par ailleurs $r_1 < |d|$ et $-r_2 < 0$ entraînent $r_1 - r_2 \leq |d|$). Il s'en suit que $r_1 - r_2 = 0$: contradiction. Par conséquent si $d \neq 0$, il existe un unique nombre r tel que $\begin{cases} a \equiv r\ (d) \\ 0 \leq r < |d| \end{cases}$

Exercice 853

Soient a, b et $d \in \mathbb{Z}$.

Montrer que $a \equiv b\ (d)$ si et seulement si a et b ont le même reste pour la division par d.

Éléments de réponse 853

Considérons la relation $\mathcal{R}$ définie sur $\mathbb{Z}^2$ par $a\mathcal{R}b$ si a est congru à b modulo $d \in \mathbb{Z}$. D'après l'exercice précédent c'est une relation d'équivalence.

Soit r le reste de la division de a par d. Alors par définition $0 \leq r < |d|$ et $r \equiv a\ (d)$, *i.e.* $0 \leq r < |d|$ et $a\mathcal{R}r$. Puisque $a \equiv b\ (d)$, *i.e.* $a\mathcal{R}b$, nous avons par transitivité de la relation d'équivalence $r\mathcal{R}b$, *i.e.* $r \equiv b\ (d)$. Donc, par définition du reste ($0 \leq r < |d|$), r est également le reste de la division de b par d.

Réciproquement, si a et b ont même reste r par division par d, alors $a \equiv r\ (d)$ et $b \equiv r\ (d)$, *i.e.* $a\mathcal{R}r$ et $b\mathcal{R}r$. Puisque $\mathcal{R}$ est symétrique $b\mathcal{R}r$ entraîne $r\mathcal{R}b$. Comme $\mathcal{R}$ est transitive, $a\mathcal{R}r$ et $r\mathcal{R}b$ impliquent $a\mathcal{R}b$, soit $a \equiv b\ (d)$.

Exercice 854

Soient a, b et d trois éléments de $\mathbb{Z}$. Montrer que si $a \equiv a'\ (d)$ et $b \equiv b'\ (d)$, alors $a+b \equiv a'+b'\ (d)$.

Éléments de réponse 854

Si $a \equiv a'\ (d)$ et $b \equiv b'\ (d)$, alors $a - a' = kd$ pour un certain $d \in \mathbb{Z}$ et $b - b' = \ell d$ pour un certain $\ell \in \mathbb{Z}$. Il s'en suit que

$$(a' + b') - (a + b) = (a' - a) + (b' - b) = kd + \ell d = (k + \ell)d$$

c'est-à-dire $a + b \equiv a' + b'\ (d)$.

Exercice 855

Soit E_ℓ l'ensemble des éléments de $\mathbb{Z}$ congrus à ℓ modulo 3. Montrer que E_0, E_1 et E_2 forment une partition de $\mathbb{Z}$.

Éléments de réponse 855

Montrons d'abord que les E_i sont disjoints. Par symétrie montrons simplement que E_0 et E_1 sont disjoints. Supposons que $E_0 \cap E_1 \neq \emptyset$. Soit $x \in E_0 \cap E_1$. D'une part $x \in E_0$, *i.e.* x s'écrit 3ℓ pour un certain $\ell \in \mathbb{Z}$, d'autre part $x \in E_1$, c'est-à-dire x s'écrit $3k + 1$ pour un certain $k \in \mathbb{Z}$; en particulier $3\ell = 3k + 1$, ou encore $3(\ell - k) = 1$, soit 3 divise 1 : contradiction ! Ainsi $E_0 \cap E_1 = \emptyset$.

Montrons maintenant que les E_i recouvrent $\mathbb{Z}$, c'est-à-dire que tout $x \in \mathbb{Z}$ est dans l'un des E_i. Quand on divise x par 3, le reste est 0, 1 ou 2. Si c'est 0 (resp. 1, resp. 2), alors x est dans E_0 (resp. E_1, resp. E_2). Tout élément est donc bien dans l'un des E_i.

Exercice 856

Soit $\mathcal{R}$ une relation d'équivalence sur E. Soient e, f deux éléments de E. Désignons par $\overline{e}$ (resp. $\overline{f}$) la classe d'équivalence de e (resp. f).

1. Montrer que les ensembles $\overline{e}$ et $\overline{f}$ sont soit d'intersection vide, soit égaux.
2. Montrer que $\overline{e} = \overline{f}$ si et seulement si $e \in \overline{f}$.
3. Montrer que $\overline{e} = \overline{f}$ si et seulement si $e\mathcal{R}f$.

Éléments de réponse 856

1. Supposons que $\overline{e} \cap \overline{f} \neq \emptyset$. Montrons qu'alors $\overline{e} = \overline{f}$. Par hypothèse $\overline{e}$ et $\overline{f}$ contiennent toutes deux un élément g. Soit x un élément de $\overline{e}$. Alors
   - $\diamond$ $x\mathcal{R}e$ (car $x \in \overline{e}$),
   - $\diamond$ $e\mathcal{R}g$ (car $g \in \overline{e}$),
   - $\diamond$ $g\mathcal{R}f$ (car $g \in \overline{f}$).

Par transitivité nous obtenons $x\mathcal{R}f$. Ainsi $\overline{e} \subset \overline{f}$.

De manière analogue nous avons l'inclusion $\overline{f} \subset \overline{e}$ [1].

Il en résulte que $\overline{e} = \overline{f}$.

Finalement ou bien $\overline{e} \cap \overline{f} = \emptyset$ ou bien $\overline{e} \cap \overline{f} \neq \emptyset$ auquel cas $\overline{e} = \overline{f}$.

2. Commençons par montrer que si $\overline{e} = \overline{f}$, alors $e \in \overline{f}$. Supposons donc que $\overline{e} = \overline{f}$. Puisque e appartient à $\overline{e}$, alors e appartient à $\overline{f}$.

   Montrons maintenant que si $e \in \overline{f}$, alors $\overline{e} = \overline{f}$. Si e appartient à $\overline{f}$, alors comme e appartient à $\overline{e}$ nous obtenons e appartient à $\overline{e} \cap \overline{f}$; en particulier $\overline{e} \cap \overline{f} \neq \emptyset$. D'après 1. nous obtenons l'égalité $\overline{e} = \overline{f}$.

3. Les conditions $e \in \overline{f}$ et $e\mathcal{R}f$ sont identiques, la question 3. est donc la même que la question 2.

Exercice 857

Considérons $A = \mathbb{Z}$, $\mathcal{I} = (3)$ et $\mathcal{R}$ la relation d'équivalence associée à l'idéal $\mathcal{I}$.

1. Décrire $\overline{3}$, $\overline{4}$, $\overline{6}$.
2. Donner une condition nécessaire et suffisante pour que $\overline{x} = \overline{3}$.
3. Combien y a-t-il de classes d'équivalences ?
4. Donner sans démonstration une condition nécessaire et suffisante pour que les classes $\overline{x}$, $\overline{y}$ et $\overline{z}$ forment une partition de $\mathbb{Z}$.

Éléments de réponse 857

Considérons $A = \mathbb{Z}$, $\mathcal{I} = (3)$ et $\mathcal{R}$ la relation d'équivalence associée à l'idéal $\mathcal{I}$, *i.e.*

$$x\mathcal{R}y \iff x - y \in \mathcal{I} \iff x - y \in (3)$$

1. Par définition

$$\overline{3} = \{x \in \mathbb{Z} \,|\, x\mathcal{R}3\} = \{x \in \mathbb{Z} \,|\, x - 3 \in (3)\}$$

   Or $x - 3 \in (3)$ si et seulement si $x - 3 = 3\ell$ pour un certain entier ℓ si et seulement si $x = 3(\ell + 1)$ pour un certain entier ℓ si et seulement si $x = 3k$ pour un certain entier k si et seulement si $x \in (3)$ donc

$$\overline{3} = \{x \in \mathbb{Z} \,|\, x \in (3)\} = (3) = \{3k \,|\, k \in \mathbb{Z}\}.$$

---

1. Soit x un élément de $\overline{f}$. Alors
   - $x\mathcal{R}f$ (car $x \in \overline{f}$),
   - $f\mathcal{R}g$ (car $g \in \overline{f}$),
   - $g\mathcal{R}e$ (car $g \in \overline{e}$).

Par transitivité nous obtenons $x\mathcal{R}e$. Par suite $\overline{f} \subset \overline{e}$.

Par définition

$$\overline{4} = \{x \in \mathbb{Z} \,|\, x\mathcal{R}4\} = \{x \in \mathbb{Z} \,|\, x - 4 \in (3)\}$$

Or $x - 4 \in (3)$ si et seulement si $x - 4 = 3\ell$ pour un certain entier ℓ si et seulement si $x = 4 + 3\ell$ pour un certain entier ℓ si et seulement si $x = 1 + 3(\ell + 1)$ pour un certain entier ℓ si et seulement si $x = 1 + 3k$ donc

$$\overline{4} = \{1 + 3k \,|\, k \in \mathbb{Z}\}.$$

Par définition

$$\overline{6} = \{x \in \mathbb{Z} \,|\, x\mathcal{R}6\} = \{x \in \mathbb{Z} \,|\, x - 6 \in (3)\}$$

Or $x - 6 \in (3)$ si et seulement si $x - 6 = 3\ell$ pour un certain entier ℓ si et seulement si $x = 6 + 3\ell$ pour un certain entier ℓ si et seulement si $x = 3(\ell + 2)$ pour un certain entier ℓ si et seulement si $x = 3k$ pour un certain entier k donc

$$\overline{6} = \{3k \,|\, k \in \mathbb{Z}\}.$$

2. Donnons une condition nécessaire et suffisante pour que $\overline{x} = \overline{3}$.

   Nous avons : $\overline{x} = \overline{3}$ si et seulement si $x\mathcal{R}3$ si et seulement si $x \equiv 3$ (3) si et seulement si $x \equiv 0$ (3) si et seulement si 3 divise x.

3. Il y a trois classes d'équivalence qui sont $\overline{0}$, $\overline{1}$, $\overline{2}$ qui sont aussi les classes $\overline{3}$, $\overline{4}$ et $\overline{5}$.

4. Les classes $\overline{x}$, $\overline{y}$ et $\overline{z}$ forment une partition de $\mathbb{Z}$ si et seulement si les restes de la division par 3 de x, y et z sont tous les trois différents.

Exercice 858

Soit A un anneau. Soit $\mathcal{I} \subset A$ un idéal de A. Montrer que le morphisme d'anneaux $A \to {}^{A}\!/_{\mathcal{I}}$ est surjectif et que son noyau est l'idéal $\mathcal{I}$.

Éléments de réponse 858

Considérons un anneau A, $\mathcal{I}$ un idéal de A et $\mathcal{R}$ la relation d'équivalence associée à l'idéal $\mathcal{I}$, *i.e.*

$$x\mathcal{R}y \iff x - y \in \mathcal{I}.$$

Nous notons ${}^{A}\!/_{\mathcal{I}}$ l'ensemble des classes d'équivalence de A pour la relation d'équivalence définie par un idéal $\mathcal{I}$.

L'application $\Phi\colon A \to {}^{A}\!/_{\mathcal{I}}$, $a \mapsto \overline{a}$ est un morphisme d'anneaux.

Montrons que Φ est surjectif : par définition de ${}^{A}\!/_{\mathcal{I}}$ un élément de ${}^{A}\!/_{\mathcal{I}}$ est de la forme $\overline{a}$; c'est donc l'image de $a \in A$. Le morphisme est donc surjectif.

Montrons que le noyau de Φ est l'idéal $\mathcal{I}$. Si un élément a s'envoie sur $\overline{0}$, cela signifie que $\overline{a} = \overline{0}$ ce qui signifie que $a \in \overline{0}$ [2]. Or $\overline{0} = \mathcal{I}$ (en effet $\overline{0} = \{x \in A \,|\, x\mathcal{R}0\} = \{x \in A \,|\, x - 0 \in \mathcal{I}\} = \{x \in A \,|\, x - 0 \in \mathcal{I}\} = \mathcal{I}$) donc $a \in \overline{0}$ ce réécrit $a \in \mathcal{I}$. Autrement dit $\ker \Phi = \mathcal{I}$.

2. Soit $\mathcal{R}$ une relation d'équivalence sur E. Soient e, f deux éléments de E. Montrons que $\overline{e} = \overline{f}$ si et seulement si $e \in \overline{f}$.

Exercice 859

1. Montrer qu'il existe un unique morphisme d'anneaux $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Quelle est l'image de $\overline{4}$?
2. Soient m et n deux entiers positifs. Montrer que si m ne divise pas n, il n'existe pas de morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.
3. Montrer que si m divise n, il existe un unique morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

   Donner une formule pour ce morphisme.

   Montrer qu'il est surjectif.

   Donner un exemple qui montre qu'il n'est pas injectif en général.

Éléments de réponse 859

1. Montrons qu'il existe un unique morphisme d'anneaux $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

   Puisque

   $$6 \cdot 1_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}} = 6 \cdot \left(1_{\mathbb{Z}/2\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}\right) = \left(\overline{6}_{\mathbb{Z}/2\mathbb{Z}}, \overline{6}_{\mathbb{Z}/3\mathbb{Z}}\right) = \left(\overline{0}_{\mathbb{Z}/2\mathbb{Z}}, \overline{0}_{\mathbb{Z}/3\mathbb{Z}}\right) = 0_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}$$

   par propriété universelle de $\mathbb{Z}/6\mathbb{Z}$ il existe bien un unique morphisme d'anneaux $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

   Déterminons l'image de $\overline{4}_{\mathbb{Z}/6\mathbb{Z}}$:

   $$f(\overline{4}_{\mathbb{Z}/6\mathbb{Z}}) = (\overline{4}_{\mathbb{Z}/2\mathbb{Z}}, \overline{4}_{\mathbb{Z}/3\mathbb{Z}}) = (\overline{0}_{\mathbb{Z}/2\mathbb{Z}}, \overline{1}_{\mathbb{Z}/3\mathbb{Z}})$$

2. Soient m et n deux entiers positifs. Montrons que si m ne divise pas n, il n'existe pas de morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

   Remarquons que $\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n \text{ fois}} = \overline{n}$ est différent de $\overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ si m ne divise pas n. La propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ assure qu'il n'existe pas dans ce cas de morphisme d'anneaux.

3. Montrons que si m divise n, il existe un unique morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

   Première rédaction possible. Dans le cas où m divise n, nous avons $1 \cdot \overline{1}_{\mathbb{Z}/m\mathbb{Z}} = \overline{0}$. Ainsi la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ assure l'existence d'un morphisme d'anneaux $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ donné par la formule : $\varphi(\overline{k}_{\mathbb{Z}/n\mathbb{Z}}) = \overline{k}_{\mathbb{Z}/m\mathbb{Z}}$.

Commençons par montrer que si $\overline{e} = \overline{f}$, alors $e \in \overline{f}$. Supposons donc que $\overline{e} = \overline{f}$. Puisque e appartient à $\overline{e}$, alors e appartient à $\overline{f}$.

Montrons maintenant que si $e \in \overline{f}$, alors $\overline{e} = \overline{f}$. Si e appartient à $\overline{f}$, alors comme e appartient à $\overline{e}$ nous obtenons e appartient à $\overline{e} \cap \overline{f}$; en particulier $\overline{e} \cap \overline{f} \neq \emptyset$. D'après 1. nous obtenons l'égalité $\overline{e} = \overline{f}$.

Ce morphisme est évidemment surjectif puisque tout élément de $\overline{k}_{\mathbb{Z}/n\mathbb{Z}}$ a un antécédent, à savoir $\overline{k}_{\mathbb{Z}/m\mathbb{Z}}$.

Si $n = 4$ et $m = 2$, alors les éléments $\overline{2}_{\mathbb{Z}/4\mathbb{Z}}$ et $\overline{0}_{\mathbb{Z}/4\mathbb{Z}}$ s'envoient sur le même élément $\overline{0}_{\mathbb{Z}/2\mathbb{Z}}$ (car $\overline{0}_{\mathbb{Z}/2\mathbb{Z}} = \overline{2}_{\mathbb{Z}/2\mathbb{Z}}$) ; le morphisme $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ n'est donc pas injectif.

Autre rédaction possible. Soient m et n deux entiers positifs distincts tels que m divise n. Il existe un unique morphisme $\psi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$; d'après ce qui précède ψ est surjectif. Supposons ψ injectif alors ψ réalise un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$. Par conséquent $n = m$: contradiction.

Exercice 860

Soient A et B deux anneaux et $\mathcal{I} \subset A$ un idéal de A. Considérons la correspondance entre les morphismes $\varphi\colon A \to B$ et les morphismes $\overline{\varphi}\colon A/\mathcal{I} \to B$ donnée par le cours.

1. Montrer que φ est surjective si et seulement si $\overline{\varphi}$ est surjective.
2. Montrer que $\overline{\varphi}$ est injective si et seulement si $\ker\varphi = \{\mathrm{id}\}$.

Éléments de réponse 860

1. Montrons que φ est surjective si et seulement si $\overline{\varphi}$ est surjectif.

   Si $\overline{\varphi}$ est surjectif, alors φ est la composition de deux morphismes surjectifs donc est surjectif.

   Réciproquement si φ est surjectif, alors tout élément $b \in B$ s'écrit $\varphi(a) = \overline{\varphi}(p(a))$. Tout élément de b s'écrit donc comme $\overline{\varphi}$ d'un certain élément ce qui prouve la surjectivité de $\overline{\varphi}$.

2. ◇ Supposons $\overline{\varphi}$ injective. Soit $a \in A$ un élément tel que $0 = \varphi(a) = \overline{\varphi}(p(a))$. Par injectivité de $\overline{\varphi}$ nous avons donc $p(a) = 0$ ce qui signifie que a appartient à $\ker p = \mathcal{I}$. Autrement dit $\ker\varphi \subset \mathcal{I}$. Réciproquement, si $a \in \mathcal{I}$, alors
   $$\varphi(a) = \overline{\varphi}(p(a)) = \overline{\varphi}(0) = 0$$
   et $\mathcal{I} \subset \ker\varphi$.

   Nous avons donc montré que si $\overline{\varphi}$ est injective, alors $\ker\varphi = \mathcal{I}$.

   ◇ Supposons désormais que $\ker\varphi = \mathcal{I}$. Soit $p(a) = \overline{a} \in \ker\overline{\varphi}$. Alors $0 = \overline{\varphi}(\overline{a}) = \varphi(a)$. Par suite $a \in \ker\varphi = \mathcal{I}$ et $\overline{a} = \overline{0}$. Il en résulte que $\overline{\varphi}$ est injective puisque son noyau est réduit à $\overline{0}$.

Exercice 861

Montrer que $\mathbb{C}$ est isomorphe à l'anneau quotient $\mathbb{R}[X]/(X^2+1)$.

On pourra procéder de la manière suivante : considérer le morphisme d'anneaux $f\colon \mathbb{R}[X] \to \mathbb{C}$ qui envoie un polynôme P sur son évaluation $P(\mathbf{i})$ obtenue par substitution de X en $\mathbf{i}$. Montrer que ce morphisme se factorise en l'isomorphisme voulu.

Éléments de réponse 861

Considérons le morphisme d'anneaux

$$f\colon \mathbb{R}[X] \to \mathbb{C} \qquad\qquad P \mapsto P(\mathbf{i})$$

Le morphisme f envoie X^2+1 sur $\mathbf{i}^2+1=0$. De plus si $P=\mu(X^2+1)$ est un multiple de X^2+1, alors il s'envoie sur $f(\mu)\underbrace{f(X^2+1)}_{0}$, soit sur 0. Autrement dit l'idéal (X^2+1) formé des multiples de X^2+1 s'envoie sur 0. Par propriété universelle du quotient nous obtenons donc un morphisme

$$\widetilde{f}\colon \mathbb{R}[X]/(X^2+1) \to \mathbb{C}$$

Le morphisme f est surjectif : tout nombre complexe $a+\mathbf{i}b$ est l'image de l'élément $a+Xb$: $f(a+Xb)=a+\mathbf{i}b$. Il s'en suit que $\widetilde{f}$ est surjectif.

Montrons que $\widetilde{f}$ est injectif. Cela revient à montrer que le noyau de f est l'idéal (X^2+1). Soit P un polynôme ; effectuons la division $P=(X^2+1)Q+R$ où R est un polynôme de degré $<\deg(X^2+1)=2$. Écrivons R sous la forme $a+bX$. Nous avons

$$f(P)=\underbrace{f(X^2+1)}_{0}f(Q)+f(R)=\underbrace{f(R)}_{a+\mathbf{i}b}=a+\mathbf{i}b;$$

ainsi P appartient à $\ker f$ si et seulement si $f(P)=0$ si et seulement si $f(R)=0$ si et seulement si $a=b=0$. Autrement dit P appartient à $\ker f$ si et seulement si P est un multiple de X^2+1 si et seulement si P appartient à (X^2+1).

Exercice 862

1. Montrer qu'il existe un unique morphisme d'anneaux de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.
2. Décrire explicitement l'image de chaque élément.
3. Montrer que ce morphisme est un isomorphisme.

Éléments de réponse 862

1. Montrons qu'il existe un unique morphisme d'anneaux de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.
   Puisque
   $$6\cdot\overline{1}_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}}=(6\cdot\overline{1}_{\mathbb{Z}/2\mathbb{Z}},6\cdot\overline{1}_{\mathbb{Z}/3\mathbb{Z}})=(\overline{6},\overline{6})=(\overline{0},\overline{0})$$
   alors par propriété universelle de $\mathbb{Z}/6\mathbb{Z}$ il existe un unique morphisme de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ qui sera noté f dans la suite de l'exercice.
2. Décrivons explicitement l'image de chaque élément. Nous avons :

$f(\overline{0})=(\overline{0},\overline{0})$, $f(\overline{1})=(\overline{1},\overline{1})$, $f(\overline{2})=(\overline{0},\overline{2})$, $f(\overline{3})=(\overline{1},\overline{0})$, $f(\overline{4})=(\overline{0},\overline{1})$, $f(\overline{5})=(\overline{1},\overline{2})$.

3. Première rédaction possible : La question 2. assure que f est à la fois surjectif et injectif.
   Seconde rédaction possible : utiliser le théorème des restes chinois.

Exercice 863

1. Construire un morphisme d'anneaux de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. Montrer que ce morphisme d'anneaux n'est pas un isomorphisme d'anneaux.
3. Montrer que les anneaux $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

Éléments de réponse 863

1. Puisque
$$4 \cdot \overline{1}_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}} = (4 \cdot \overline{1}_{\mathbb{Z}/2\mathbb{Z}}, 4 \cdot \overline{1}_{\mathbb{Z}/2\mathbb{Z}}) = (\overline{4}, \overline{4}) = (\overline{0}, \overline{0})$$
alors par propriété universelle de $\mathbb{Z}/4\mathbb{Z}$ il existe un unique morphisme d'anneaux de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui sera noté f dans la suite de l'exercice.
2. Le morphisme f est donné par les formules
$$f(\overline{0}) = (\overline{0}, \overline{0}), \qquad f(\overline{1}) = (\overline{1}, \overline{1}), \qquad f(\overline{2}) = (\overline{0}, \overline{0}), \qquad f(\overline{3}) = (\overline{1}, \overline{1}).$$
Le morphisme n'est pas injectif puisque $\overline{0}$ et $\overline{2}$ ont la même image.
3. Première méthode : Si les deux anneaux étaient isomorphes, il existerait par définition un isomorphisme de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mais par propriété universelle de $\mathbb{Z}/4\mathbb{Z}$ un tel morphisme s'il existe est unique ; c'est donc celui construit au 1. mais nous avons vu au 2. que ce morphisme n'est pas un isomorphisme.

   Seconde méthode : utiliser le théorème des restes chinois.

Exercice 864

Montrer que la réciproque du théorème chinois des restes est vraie, à savoir que si n et m ne sont pas premiers entre eux, alors les anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ ne sont pas isomorphes.

Éléments de réponse 864

Supposons que n et m ne soient pas premiers entre eux. Alors leur ppcm μ est strictement plus petit que le produit mn. Raisonnons par l'absurde : supposons que les anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ soient isomorphes ; alors l'isomorphisme $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est unique par propriété universelle de $\mathbb{Z}/nm\mathbb{Z}$ et ce morphisme envoie $\overline{\mu}$ et $\overline{0}$ sur la même image $(\overline{0}, \overline{0})$: contradiction avec l'injectivité de ce morphisme.

Exercice 865

1. Montrer qu'un corps est un anneau intègre.
2. Donner un exemple d'anneau intègre qui n'est pas un corps.

Éléments de réponse 865

1. Montrons qu'un corps est un anneau intègre.

   Soit A un corps. Soient a et b deux éléments de A tels que $ab = 0$. Si $a = 0$, alors nous avons le résultat souhaité. Sinon puisque A est un corps, a admet un inverse a^{-1} et en multipliant chaque côté de l'égalité par cet inverse, nous obtenons $b = 0$.

2. L'anneau $\mathbb{Z}$ est un anneau intègre qui n'est pas un corps.

Exercice 866

1. Un élément $a \in A$ d'un anneau est appelé diviseur de 0 s'il existe $b \in A$ non nul tel que $ab = 0$. Montrer qu'un diviseur de 0 dans un anneau n'est jamais inversible.
2. Soit $\varphi(n)$ le nombre d'éléments $x \in \mathbb{Z}/n\mathbb{Z}$ admettant un inverse multiplicatif x^{-1}. Vérifier à la main que la formule $\varphi(4) = 2$ est exacte (on pourra utiliser le 1. pour montrer que certains éléments ne sont pas inversibles).

Éléments de réponse 866

1. Raisonnons par l'absurde, *i.e.* supposons que $a \in A$ soit un diviseur inversible de 0.

   Soit b un élément non nul de A tel que $ab = 0$. En multipliant chaque côté de l'égalité par l'inverse a^{-1} de a nous obtenons $b = 0$: contradiction.

2. Remarquons que $\overline{0}$ et $\overline{2}$ sont diviseurs de $\overline{0}$; en effet si nous multiplions $\overline{0}$ et $\overline{2}$ par $\overline{2} \neq \overline{0}$ nous obtenons $\overline{0}$.

   D'autre part $\overline{1}$ et $\overline{3}$ sont inversibles dans $\mathbb{Z}/4\mathbb{Z}$ d'inverse respectif $\overline{1}$ et $\overline{3}$:

   $$\overline{1}\,\overline{1} = \overline{1}, \qquad \overline{3}\,\overline{3} = \overline{9} = \overline{1}.$$

   Ainsi $\varphi(4) = 2$.

Exercice 867

1. Un élément (a, b) est inversible dans un anneau produit $A \times B$ si et seulement si ($a \in A$ est inversible et $b \in B$ est inversible).
2. Si A et B sont des ensembles finis, quel est le nombre d'éléments inversibles dans $A \times B$?
3. Quel est le nombre d'inversibles dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$?

Éléments de réponse 867

1. Montrons qu'un élément (a, b) est inversible dans un anneau produit $A \times B$ si et seulement si ($a \in A$ est inversible et $b \in B$ est inversible).

   Commençons par supposer que (a, b) est inversible ; notons (c, d) son inverse. Alors par définition du produit $(a, b) \cdot_{A\times B} (c, d) = (1_A, 1_B)$ se réecrit $(a \cdot_A c, b \cdot_B d) = (1_A, A_B)$. Autrement dit

   ◇ $a \cdot_A c = 1_A$, *i.e.* a est inversible dans A d'inverse c ;

◇ $b \cdot_B d = 1_B$, *i.e.* b est inversible dans B d'inverse d.

Réciproquement supposons que a soit inversible dans A d'inverse c (c'est-à-dire $a \cdot_A c = 1$) et que b soit inversible dans B d'inverse d (c'est-à-dire $b \cdot_B d = 1$). Alors

$$(a, b) \cdot_{A\times B} (c, d) = (a \cdot_A c, b \cdot_B d) = (1_A, 1_B).$$

Finalement un élément (a, b) est inversible dans un anneau produit $A\times B$ si et seulement si (a est inversible dans A et $b \in B$ est inversible dans B).

2. Déterminons lorsque A et B sont des ensembles finis, le nombre d'éléments inversibles dans $A \times B$.

   D'après 1. le nombre d'inversibles de $A \times B$ est le produit du nombre d'inversibles de A par le nombre d'inversibles de B.

3. Déterminons le nombre d'inversibles dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

   D'après 2. le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est $\varphi(n)\varphi(m)$.

Exercice 868

Quel est le noyau du morphisme de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Éléments de réponse 868

Rappelons que si A est un anneau et $\mathcal{I}$ un idéal de A, alors le noyau du morphisme $A \to A/\mathcal{I}$ est l'idéal $\mathcal{I}$. Ainsi le noyau du morphisme de l'anneau $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est $n\mathbb{Z}$.

Exercice 869

1. Calculer l'inverse de 13 dans $\mathbb{Z}/20\mathbb{Z}$.
2. Calculer l'inverse de 15 dans $\mathbb{Z}/8\mathbb{Z}$.

Éléments de réponse 869

1. Déterminons l'inverse de 13 dans $\mathbb{Z}/20\mathbb{Z}$.

   Commençons par calculer une relation de Bezout.

   ◇ $20 = 1 \cdot 13 + 7$,

   ◇ $13 = 1 \cdot 7 + 6$,

   ◇ $7 = 1 \cdot 6 + 1$,

   ◇ $6 = 6 \cdot 1 + 0$.

   Par suite le pgcd de 7 et 13 est 1 (le dernier reste non nul trouvé). Remplaçons dans cette dernière ligne à reste non nul 6 par son expression venant de la deuxième, *i.e.* remplaçons 6 par $13 - 7$:

$$1 = 7 - 6 = 7 - (13 - 7) = 2 \cdot 7 - 13$$

nous obtenons une nouvelle expression de 1 en fonction des termes 7 et 13. Enfin remplaçons 7 par $20-13$ qui vient de la première ligne :

$$1 = 2\cdot 7 - 13 = 2\cdot(20-13) - 13 = 2\cdot 20 - 3\cdot 13$$

c'est la relation de Bezout cherchée. En passant dans $\mathbb{Z}/20\mathbb{Z}$ nous obtenons $\overline{1} = -\overline{3}\cdot\overline{13}$. L'inverse de $\overline{13}$ est donc $-\overline{3} = \overline{17}$.

2. Déterminons l'inverse de 15 dans $\mathbb{Z}/8\mathbb{Z}$.

   Commençons par calculer une relation de Bezout.

   - $8 = 1\cdot 15 - 7$,
   - $15 = 2\cdot 7 + 1$,
   - $7 = 6\cdot 1 + 1$,
   - $1 = 1\cdot 1 + 0$.

   Par suite le pgcd de 7 et 15 est 1 (le dernier reste non nul trouvé). Remplaçons dans cette dernière ligne à reste non nul 1 par son expression venant de la deuxième, *i.e.* remplaçons 1 par $15 - 2\cdot 7$:

$$1 = 7 - 6\cdot 1 = 7 - 6\cdot(15 - 2\cdot 7) = 13\cdot 7 - 6\cdot 15$$

   nous obtenons une nouvelle expression de 1 en fonction des termes 7 et 15. Enfin remplaçons 7 par $15-8$ qui vient de la première ligne :

$$1 = 13\cdot 7 - 6\cdot 15 = 13\cdot(15-8) - 6\cdot 15 = 7\cdot 15 - 13\cdot 8$$

   c'est la relation de Bezout cherchée. En passant dans $\mathbb{Z}/8\mathbb{Z}$ nous obtenons $\overline{1} = \overline{7}\cdot\overline{15}$. L'inverse de $\overline{15}$ est donc $\overline{7}$.

3.4. Anneaux de polynômes

Exercice 870

1. Écrire les suites correspondant aux polynômes $1+X$ et $2+3X$ de $\mathbb{Z}[X]$. Faire le produit de ces suites en utilisant la définition.
2. Calculer le produit des polynômes de la manière usuelle et vérifier que l'on obtient bien le même résultat que précédemment.

Éléments de réponse 870

1. La suite (a_n) correspondant au polynôme $1+X$ de $\mathbb{Z}[X]$ est $(1,0,0,\ldots)$; la suite (b_n) correspondant au polynôme $2+3X$ de $\mathbb{Z}[X]$ est $(2,3,0,0,\ldots)$. Par définition le produit (c_n) de (a_n) et (b_n) est donné par $c_n = \sum_{i=0}^{n} a_i b_{n-i}$ ce qui conduit ici à

$$c_0 = 2, \qquad c_1 = 5, \qquad c_2 = 3, \qquad c_n = 0 \quad \forall n \geq 3.$$

2. Multiplions $1+X$ et $2+3X$ de la manière usuelle :
$$(1+X)(2+3X) = 2+3X+2X+3X^2 = 2+5X+3X^2$$
La suite correspondant au polynôme $2+5X+3X^2$ est $(2,5,3,0,0,\ldots)$: nous retrouvons donc bien le même résultat que précédemment.

Exercice 871

Montrer que A est un sous-anneau de $A[X]$. Plus précisément montrer que
$$A \to A[X], \qquad a \mapsto (a,0,0,\ldots) = a+0X+0X^2+\ldots$$
est un morphisme d'anneaux injectif.

Éléments de réponse 871

Considérons l'application
$$\varphi\colon A \to A[X], \qquad a \mapsto (a,0,0,\ldots) = a+0X+0X^2+\ldots$$
Remarquons que $\varphi(1) = (1,0,0,\ldots) = 1+0X+0X^2+\ldots = 1$.

Soient a et b dans A, alors d'une part $\varphi(a-b) = (a-b,0,0,\ldots) = a-b+0X+0X^2+\ldots$, d'autre part $\varphi(a)-\varphi(b) = a+0X+0X^2+\ldots-(b+0X+0X^2+\ldots) = (a-b)+0X+0X^2+\ldots$; en particulier $\varphi(a-b) = \varphi(a)-\varphi(b)$.

Soient a et b dans A, alors d'une part $\varphi(ab) = (ab,0,0,\ldots) = ab+0X+0X^2+\ldots$, d'autre part
$$\varphi(a)\varphi(b) = (a+0X+0X^2+\ldots)(b+0X+0X^2+\ldots) = ab+0X+0X^2+\ldots$$
Par suite φ est un morphisme d'anneaux.

Enfin φ est injectif car par définition de φ le seul élément s'envoyant sur le polynôme nul est l'élément nul.

Exercice 872

1. Effectuer la division de X^2+3 par $X+1$.
2. Effectuer la division de X^5+X^2+3 par $-X^3+1$.
3. Effectuer la division de X^2+3 par X^3+1.
4. Effectuer dans $\mathbb{Z}[X]$ la division de X^2+3 par $2X+1$.

Éléments de réponse 872

1. Effectuons la division de X^2+3 par $X+1$:
$$X^2+3 = (X+1)(X-1)+4.$$
2. Effectuons la division de X^5+X^2+3 par $-X^3+1$:
$$X^5+X^2+3 = (-X^2)\cdot(-X^3+1)+(2X^2+3).$$

3. Effectuons la division de X^2+3 par X^3+1 :
$$X^2+3 = 0\cdot(X^3+1)+(X^2+3).$$
4. Nous ne pouvons pas effectuer dans $\mathbb{Z}[X]$ la division de X^2+3 par $2X+1$ car 2 n'est pas inversible dans $\mathbb{Z}$.

Exercice 873

1. Soient A un anneau intègre, $P\in A[X]$ et a_1, a_2, …, $a_k\in A$ des éléments distincts. Si $P(a_i)=0$ pour tout i, alors le produit $(X-a_1)(X-a_2)\dots(X-a_k)$ divise P.
2. Un polynôme non nul de degré n sur un anneau intègre A admet au plus n racines.
3. Donner un polynôme de degré n sur un anneau non intègre ayant plus de n racines.

Éléments de réponse 873

1. Soient A un anneau intègre, $P\in A[X]$ et a_1, a_2, …, $a_k\in A$ des éléments distincts. Supposons que $P(a_i)=0$ pour tout i, montrons par récurrence sur $k\geq 1$ que le produit $(X-a_1)(X-a_2)\dots(X-a_k)$ divise P.

   ◇ Pour $k=1$ effectuons la division euclidienne de P par $X-a_1$: $P=Q(X-a_1)+R$ où R est un polynôme de degré au plus 0 c'est-à-dire une constante. En évaluant cette expression au point $X=a_1$ nous obtenons $0=P(a_1)=R$; nous avons donc bien : $X-a_1$ divise P.

   ◇ Supposons maintenant l'hypothèse vraie au rang $k-1$ et supposons que $P(a_i)=0$ pour tout $i\leq k$. Par hypothèse de récurrence
   $$P=(X-a_1)(X-a_2)\dots(X-a_{k-1})Q.$$
   En évaluant cette expression au point $X=a_k$ nous obtenons $0=P(a_k)=(a_k-a_1)(a_k-a_2)\dots(a_k-a_{k-1})Q(a_k)$. Étant donnés que A est un anneau intègre et que les a_k-a_i sont non nuls (car les a_i sont tous distincts) nous obtenons que $Q(a_k)=0$; autrement dit $X-a_k$ divise Q, c'est-à-dire $Q=(X-a_k)R$. Finalement P s'écrit
   $$P=(X-a_1)(X-a_2)\dots(X-a_{k-1})(X-a_k)R.$$

2. Un polynôme non nul de degré n sur un anneau intègre A admet au plus n racines.

   Raisonnons par l'absurde : supposons qu'il existe un polynôme P de degré n admettant $n+1$ racines distinctes a_1, a_2, …, a_{n+1}. D'après la question qui précède nous avons l'égalité
   $$P=(X-a_1)(X-a_2)\dots(X-a_n)(X-a_{n+1})R. \tag{3.4.1}$$
   Le terme de gauche dans (3.6.2) est de degré n, alors que le terme de droite dans (3.6.2) est de degré $\geq n+1$: contradiction.

3. Donnons un polynôme de degré n sur un anneau non intègre ayant plus de n racines. Considérons l'anneau $A = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}[X]$ et le polynôme non nul $P = \overline{2}X$. Remarquons que P est de degré 1 et que P admet les deux racines distinctes suivantes :

$$P(\overline{2}) = \overline{2}\,\overline{2} = \overline{4} = \overline{0}, \qquad P(\overline{0}) = \overline{0}.$$

Exercice 874

1. Quels sont les polynômes inversibles dans la liste suivante sur $\mathbb{Q}[X]$: $1+3X+X^2$, $5+X$, 4 ?
2. Quels sont les polynômes inversibles dans la liste suivante sur $\mathbb{Z}[X]$: $1+3X+X^2$, $5+X$, 4 ?

Éléments de réponse 874

1. Dans la liste de polynômes sur $\mathbb{Q}[X]$: $1+3X+X^2$, $5+X$, 4, seul 4 est inversible (d'inverse $\frac{1}{4}$).
2. Dans la liste de polynômes sur $\mathbb{Z}[X]$: $1+3X+X^2$, $5+X$, 4, aucun n'est inversible. En effet, les éléments inversibles de $\mathbb{Z}[X]$ sont les constantes 1 et -1.

Exercice 875

1. La conjugaison complexe $\mathbb{C} \to \mathbb{C}$, $z = a+\mathbf{i}b \mapsto \overline{z} = a-\mathbf{i}b$ est-elle un morphisme d'anneaux ?
2. Montrer que si $P \in \mathbb{R}[X]$ admet une racine a, alors le conjugué $\overline{a}$ de a est aussi une racine de P.
3. Montrer que $P = (X-a)(X-\overline{a})$ est un polynôme réel.

Éléments de réponse 875

1. La conjugaison complexe $\mathbb{C} \to \mathbb{C}$, $z = a+\mathbf{i}b \mapsto \overline{z} = a-\mathbf{i}b$ est un morphisme d'anneaux ; en effet $\overline{1} = 1$ et pour tous z_1, z_2 nous avons

$$\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}, \qquad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$

2. Montrons que si $P \in \mathbb{R}[X]$ admet une racine a, alors le conjugué $\overline{a}$ vérifie lui aussi $P(\overline{a}) = 0$.

   Soit $P = \sum a_i X^i$. Nous avons

$$0 = P(a) = \overline{P(a)} = \overline{\sum a_i a^i} \overset{cf1.}{=} \sum \overline{a_i}\,\overline{a}^i \overset{a_i \in \mathbb{R}}{=} \sum a_i\,\overline{a}^i = P(\overline{a})$$

3. Montrons que $P = (X-a)(X-\overline{a})$ est un polynôme réel.

   Le polynôme conjugué de P est $\overline{P} = (X-\overline{a})(X-a)$; en effet $\overline{P}$ est obtenu à partir de P en changeant tous les coefficients par leur conjugué. Puisque $P = \overline{P}$ nous obtenons que P est réel.

   Autre rédaction possible : $P = (X-a)(X-\overline{a}) = X^2 - 2\mathrm{Re}(a)X + |a|^2$; les coefficients de P sont réels donc P est un polynôme réel et $P = \overline{P}$.

Exercice 876

1. Calculer une décomposition du polynôme $P = X+X^2+X^3+X^4$ en produit d'irréductibles sur $\mathbb{C}$.
2. Calculer une décomposition du polynôme $P = X+X^2+X^3+X^4$ en produit d'irréductibles sur $\mathbb{R}$.

Éléments de réponse 876

1. Calculons une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{C}$.

   Si nous multiplions P par $X-1$, nous trouvons $(X-1)P = X^5 - X = X(X^4-1)$. Les racines de ce polynôme sont 0 et les racines 4ièmes de l'unité, *i.e.* les racines de ce polynôme sont 0, 1, -1, $\mathbf{i}$ et $-\mathbf{i}$. Ainsi

   $$(X-1)P = X(X-1)(X+1)(X-\mathbf{i})(X+\mathbf{i})$$

   Comme nous sommes dans un anneau intègre, nous pouvons simplifier par $X-1$; nous obtenons alors

   $$P = X(X+1)(X-\mathbf{i})(X+\mathbf{i})$$

   qui est la décomposition voulue.

2. Calculons une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{R}$.

   Pour obtenir la décomposition dans $\mathbb{R}$ il faut regrouper les termes deux par deux avec leur conjugué, ici $X-\mathbf{i}$ et $X+\mathbf{i}$ dont le produit vaut X^2+1. La décomposition sur $\mathbb{R}$ est donc $P = X(X+1)(X^2+1)$.

Exercice 877

Soit $P \in \mathbb{Z}[X]$ un polynôme de degré au plus un. Discuter l'irréductibilité de ce polynôme.

Éléments de réponse 877

Si P est nul, alors il n'est pas irréductible.

Si P est une constante non nulle, alors P est irréductible si et seulement si p est un nombre premier.

Il ne reste qu'à considérer le cas où $P = aX + b$ est de degré 1. Si a et b ne sont pas premiers entre eux et ont un pgcd non trivial d, la décomposition $P = d\left(\frac{a}{d}X + \frac{b}{d}\right)$ montre que P n'est pas irréductible. Si a et b sont premiers entre eux, montrons que P est irréductible. Soit $P = QR$ une décomposition. Puisque P est de degré 1, il faut que Q et R soient de degré 0 et 1, par exemple par symétrie Q est de degré 0 et R est de degré 1. Par suite Q est une constante c. Nous obtenons donc $aX + b = c(dX + e)$ ce qui montre que c divise à la fois a et b ; il en résulte que c vaut ± 1 (rappelons que $\text{pgcd}(a, b) = 1$). Par conséquent Q est inversible dans $\mathbb{Z}[X]$; toute décomposition de P contient donc un facteur inversible ce qui prouve que Q est irréductible.

Exercice 878

1. Soit $P \in \mathbb{Z}[X]$. Vérifier que P est divisible dans $\mathbb{Z}[X]$ par le contenu $\text{ct}(P)$.
2. Montrer que si l'on écrit $P = \text{ct}(P)Q$, alors $\text{ct}(Q) = 1$.

Éléments de réponse 878

1. Soit $P \in \mathbb{Z}[X]$. Vérifions que P est divisible dans $\mathbb{Z}[X]$ par le contenu $\text{ct}(P)$. Écrivons P sous la forme $P = \sum_i a_i X^i$. Rappelons que le contenu $\text{ct}(P)$ est $\text{ct}(P) = \text{pgcd}(a_i)$. Nous avons
$$P = \text{ct}(P)\frac{a_i}{\text{ct}(P)}X^i$$
autrement dit P est divisible par $\text{ct}(P)$ puisque les $\frac{a_i}{\text{ct}(P)}$ sont des entiers.
2. Montrons que si l'on écrit $P = \text{ct}(P)Q$, alors $\text{ct}(Q) = 1$.

   Raisonnons par l'absurde, *i.e.* supposons que $\text{ct}(Q) \neq 1$. D'après 1. nous pouvons écrire Q sous la forme $\text{ct}(Q)\sum b_i X^i$. En reportant cette expression dans P nous obtenons
$$P = \text{ct}(P)\text{ct}(Q)\sum b_i X^i = \sum(\text{ct}(P)\text{ct}(Q)b_i)X^i$$
   ce qui montre que tous les coefficients de P sont divisibles par $\text{ct}(P)\text{ct}(Q)$: contradiction avec le fait que le plus grand diviseur commun des coefficients de P est $\text{ct}(P)$.

Exercice 879

Montrer que si $Q \in \mathbb{Z}[X]$ est tel que $\text{ct}(Q) = 1$, et si $Q = RS$ est une décomposition en produit de non inversibles, alors ni R, ni S ne sont des constantes.

Éléments de réponse 879

Soit $Q \in \mathbb{Z}[X]$ tel que $\text{ct}(Q) = 1$, Montrons que si $Q = RS$ est une décomposition en produit de non inversibles, alors R et S ne sont pas des constantes. Raisonnons par l'absurde : supposons que R soit une constante : $R = r$. Écrivons S sous la forme $\sum_i s_i X^i$. Alors $Q = RS$ s'écrit aussi $\sum_i (rs_i)X^i$; ainsi r divise tous les coefficients de Q donc leur pgcd qui est 1. Par

conséquent r vaut ± 1 et R est inversible : contradiction. De même si S est une constante, nous obtenons que S est inversible : contradiction. Finalement ni R, ni S ne sont des constantes.

Exercice 880

Considérons le polynôme P de degré 4 donné par $P = 5X^4 + 10X^3 - 5X^2 - 10X + 5 \in \mathbb{Z}[X]$.

1. Écrire P sous la forme $a_1 a_2 \dots a_n Q$ où les a_i sont des entiers irréductibles et où Q est de contenu 1.
2. Soit R un polynôme de $\mathbb{Z}[X]$ divisant Q. Donner la liste des valeurs possibles pour $R(0)$.
3. Donner de même la liste des valeurs possibles pour $R(1)$ et $R(-1)$.
4. Établir la liste des polynômes de degré 1 susceptibles de diviser Q.
5. Établir la liste des polynômes de degré 2 susceptibles de diviser Q.
6. Trouver la décomposition de Q en produit d'irréductibles.
7. Trouver la décomposition de P en produit d'irréductibles.

Éléments de réponse 880

1. Écrivons P sous la forme $a_1 a_2 \dots a_n Q$ où les a_i sont des entiers irréductibles et où Q est de contenu 1. On constate que
$$P = 5 \underbrace{(X^4 + 2X^3 - X^2 - 2X + 1)}_{Q};$$
de plus 5 est premier donc irréductible et $\mathrm{ct}(Q) = \mathrm{pgcd}(1, 2, -1, -2, 1) = 1$.
2. Soit R un polynôme de $\mathbb{Z}[X]$ divisant Q. Puisque $Q(0) = 1$ et $R(0)$ divise $Q(0)$ nous obtenons que $R(0)$ vaut ± 1.
3. Comme $Q(1) = 1$ et $R(1)$ divise $Q(1)$ nous obtenons que $R(1)$ vaut ± 1.
Puisque $Q(-1) = 1$ et $R(-1)$ divise $Q(-1)$ nous obtenons que $R(-1)$ vaut ± 1.
4. Faisons la liste des polynômes de degré 1 susceptibles de diviser Q. Les polynômes $aX + b$ de degré au plus 1 pouvant diviser Q doivent avoir pour valeur en 0 et 1 les valeurs 1 et -1 ce qui donne les quatre possibilités
$$1, \qquad -2X + 1, \qquad -1, \qquad 2X - 1.$$
Mais aucun des polynômes de degré 1 de cette liste prend la valeur 1 ou -1 en -1. Il en résulte que Q n'est pas divisible par un polynôme de degré 1.
5. Faisons la liste des polynômes de degré 2 susceptibles de diviser Q. On cherche les polynômes de la forme $a + bX + cX^2$ qui valent
   - ◇ 1 ou -1 en 0 ;
   - ◇ 1 ou -1 en 1 ;
   - ◇ 1 ou -1 en -1.

On obtient les polynômes Q_0, $-Q_0$, Q_1, $-Q_1$, Q_2, $-Q_2$, Q_3 et $-Q_3$ où

$$Q_0 = -X^2 + X + 1, \qquad Q_1 = X^2 + X - 1, \qquad Q_2 = -2X^2 + 1, \qquad Q_3 = 1.$$

6. Seul Q_1 (et $-Q_1$) divise Q. La décomposition de Q en produit d'irréductibles est $Q = Q_1 Q_1 = Q_1^2$.
7. La décomposition de P en produit d'irréductibles est $P = 5Q_1^2$.

Exercice 881

Soit $P = \sum \frac{a_i}{b_i} X^i \in \mathbb{Q}[X]$ un polynôme non inversible.

1. Montrer qu'il existe une constante $q \in \mathbb{Q}$ tel que $R = qP$ soit dans $\mathbb{Z}[X]$ de contenu 1.
2. Soit $R = R_1 R_2 \dots R_s$ une décomposition de R en irréductibles dans $\mathbb{Q}[X]$. Donner une décomposition de P.

Éléments de réponse 881

1. Montrons qu'il existe une constante $q \in \mathbb{Q}$ tel que $R = qP$ soit dans $\mathbb{Z}[X]$ de contenu 1.

   Choisissons une constante q_1 (par exemple q_1 le produit des dénominateurs b_i) telle que $Q_1 = q_1 P = \sum a_i \frac{q_1}{b_i} X^i$ appartienne à $\mathbb{Z}[X]$. Soit c le contenu de Q_1. D'après l'exercice relatif (Exercice 9.2) à la factorisation du contenu d'un polynôme nous avons $Q_1 = cR$ où $R = \sum \frac{a_i q_1}{c b_i} X^i$ est un polynôme de contenu égal à 1. Nous avons donc le résultat voulu pour $q = \frac{q_1}{c}$.
2. Soit $R = R_1 R_2 \dots R_s$ une décomposition de R en irréductibles dans $\mathbb{Q}[X]$. La décomposition de P se déduit de celle de R. Puisque la multiplication par un inversible ne change pas l'irréductibilité, $\frac{1}{q} R_1$ est irréductible dans $\mathbb{Q}[X]$ et

   $$\left(\frac{1}{q} R_1\right) R_2 R_3 \dots R_s$$

   est la décomposition de P sur $\mathbb{Q}[X]$.

Exercice 882

Décomposer en irréductibles le polynôme $P = 5X^4 + 10X^3 - 5X^2 - 10X + 5 \in \mathbb{Q}[X]$ (on pourra se ramener à une décomposition sur $\mathbb{Z}$ faite dans un exercice précédent).

Éléments de réponse 882

Rappelons que P s'écrit $5(X^4 + 2X^3 - X^2 - 2X + 1)$ avec $\mathrm{ct}(X^4 + 2X^3 - X^2 - 2X + 1) = 1$ et que $(X^2 + X - 1)^2$ est une décomposition en produit d'irréductibles dans $\mathbb{Z}[X]$ de $X^4 + 2X^3 - X^2 - 2X + 1$. Il en résulte que la décomposition en produit d'irréductibles dans $\mathbb{Q}[X]$ est $(X^2 + X - 1)^2$. La multiplication par 5 qui est un inversible de $\mathbb{Q}[X]$ ne change pas l'irréductibilité. Ainsi la décomposition de P dans $\mathbb{Q}[X]$ est :

$$P = (5X^2 + 5X - 5)(X^2 + X - 1).$$

Exercice 883

Soient P, $Q \in \mathbb{Z}[X]$ et $\lambda \in \mathbb{Z}$. Montrer que l'application contenu ct vérifie :

1. $\mathrm{ct}(\lambda P) = \lambda \mathrm{ct}(P)$;
2. montrer que si $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ sont de contenu 1, alors $\mathrm{ct}(PQ) = 1$;
3. $\mathrm{ct}(P)\mathrm{ct}(Q) = \mathrm{ct}(PQ)$.

Éléments de réponse 883

1. Désignons par a_1, a_2, …, a_n les coefficients de P ; alors les coefficients de λP sont λa_1, λa_2, …, λa_n. L'égalité $\mathrm{ct}(\lambda P) = \lambda \mathrm{ct}(P)$ se réécrit donc $\mathrm{pgcd}(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda \mathrm{pgcd}(a_1, a_2, \ldots, a_n)$, égalité claire si on pense au pgcd comme les facteurs communs apparaissant dans la décomposition en facteurs premiers.
2. Soient $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ deux éléments de $\mathbb{Z}[X]$ de contenu 1. Raisonnons par l'absurde : supposons qu'un nombre premier d divise $\mathrm{ct}(PQ)$. Puisque $\mathrm{ct}(P) = 1$ il existe un entier n tel que d ne divise pas a_n ; on choisit un tel n minimum. De même choisissons m minimum tel que d ne divise pas b_m. Le coefficient c_{n+m} de X^{n+m} dans le produit PQ est $\sum_{i=0}^{m+n} a_i b_{m+n-i}$. Si $i < n$, alors d divise a_i et si $i > n$, alors $m+n-i < m$ donc d divise b_{m+n-i}. Finalement tous les termes de la somme sont divisibles par d sauf $a_n b_m$. Ainsi c_{n+m} n'est pas divisible par d : contradiction avec d divise $\mathrm{ct}(PQ)$.
3. Écrivons P sous la forme $P = \mathrm{ct}(P)P_1$ et écrivons Q sous la forme $Q = \mathrm{ct}(Q)Q_1$ où P_1 et Q_1 sont de contenu 1 (cf Exercice 9.2.). Alors $PQ = \mathrm{ct}(P)\mathrm{ct}(Q)P_1Q_1$. Le contenu du membre de gauche de cette dernière égalité est $\mathrm{ct}(PQ)$ tandis que le contenu du terme de droite est
$$\mathrm{ct}(\underbrace{\mathrm{ct}(P)\mathrm{ct}(Q)}_{\in\mathbb{Z}} P_1Q_1) \overset{1.}{=} \mathrm{ct}(P)\mathrm{ct}(Q)\mathrm{ct}(P_1Q_1) \overset{2.}{=} \mathrm{ct}(P)\mathrm{ct}(Q).$$
d'où l'égalité voulue.

Exercice 884

1. **Critère d'Eisenstein**. Soient $S = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ un polynôme de degré n de contenu 1 et p un nombre premier. Supposons que p divise a_0, a_1, …, a_{n-1} mais pas a_n et que p^2 ne divise pas a_0. Montrer que S est irréductible.
2. Montrer qu'il existe dans $\mathbb{Z}[X]$ des polynômes irréductibles de tout degré strictement positif.

Éléments de réponse 884

1. Soient $S = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ un polynôme de degré n de contenu 1 et p un nombre premier. Supposons que p divise a_0, a_1, …, a_{n-1} mais pas a_n et que p^2 ne divise pas a_0. Raisonnons par l'absurde, c'est-à-dire supposons que S ne soit pas irréductible ; écrivons alors une décomposition de S en produit de non inversibles
$$S = QR, \qquad Q = \sum q_iX^i, \qquad R = \sum r_iX^i.$$
Tous les q_i ne sont pas divisibles par p sinon S (et donc a_n) serait divisible par p. Ainsi il existe un plus petit entier k tel que q_k ne soit pas divisible par p. De même il existe un plus petit entier m tel que r_m ne soit pas divisible par p. Le coefficient c_{m+k} de X^{m+k} n'est donc pas divisible par p [3]. Par conséquent
$$m + k = \deg S = \deg Q + \deg R.$$
Puisque $m \leq \deg R$ et $k \leq \deg Q$ la seule possibilité est la suivante : $m = \deg R$ et $k = \deg Q$. Par ailleurs Q et R étant de degré au moins 1 car non inversibles, $m > 0$ et $k > 0$. Par minimalité de m et k, les coefficients q_0 et r_0 sont donc divisibles par p ; il en résulte que $a_0 = q_0r_0$ est divisible par p^2 : contradiction.
2. Considérons le polynôme $S = X^n + 2$; le point 1. assure que, pour tout n, le polynôme S est irréductible.

Exercice 885

Montrer que $\mathbb{Z}$ et $\Bbbk[X]$ sont des anneaux euclidiens en donnant l'application δ correspondante.

Éléments de réponse 885

Rappel. Un anneau euclidien A est un anneau intègre muni d'une application $\delta\colon A\setminus\{0\} \to \mathbb{N}$ vérifiant la propriété suivante : pour tout couple (a, b) d'éléments de A avec $b \neq 0$, il existe une division $a = bq + r$ avec $\delta(r) < \delta(b)$ ou $r = b$.

Pour $\mathbb{Z}$ l'application δ est l'application valeur absolue. Pour $\Bbbk[X]$ l'application δ est le degré des polynômes.

Exercice 886

Démontrer le corollaire qui dit que tout idéal de $\Bbbk[X]$ est principal en reprenant mot par mot la démonstration faite sur $\mathbb{Z}$ et en faisant les adaptations là où elles sont nécessaires.

Éléments de réponse 886

Soit $\mathcal{I}$ un idéal de $\Bbbk[X]$.

---

3. Le coefficient c_{m+k} de X^{m+k} dans le produit $S = QR$ est $\sum_{i=0}^{m+k} q_ir_{m+k-i}$. Si $i < k$, alors p divise q_i et si $i > k$, alors $m + k - i < m$ donc p divise r_{m+k-i}. Finalement tous les termes de la somme sont divisibles par p sauf q_kr_m.

Si $\mathcal{I} = \{0\}$, alors l'idéal $\mathcal{I}$ est principal engendré par 0.

Sinon $\mathcal{I}$ contient un élément b non nul. Soit a un élément non nul de $\mathcal{I}$ de degré minimum. Nous allons montrer que $\mathcal{I}$ est principal, plus précisément nous allons montrer que $\mathcal{I} = (a)$. Puisque $\mathcal{I}$ contient a et puisque (a) est le plus petit idéal de $\Bbbk[X]$ contenant b, nous avons $(a) \subset \mathcal{I}$. Montrons réciproquement l'inclusion $\mathcal{I} \subset (a)$. Soit b un élément de $\mathcal{I}$. La division de b par a s'écrit : $b = aq + r$ avec $\deg r < \deg a$. Remarquons que $r = b - aq$ appartient à $\mathcal{I}$ (car $a \in \mathcal{I}$, $b \in \mathcal{I}$ et $\mathcal{I}$ est un idéal de $\Bbbk[X]$). Puisque $\deg r < \deg a$ et que a est un élément non nul de $\mathcal{I}$ de degré minimum, $r = 0$. Il en résulte que $b = aq$, en particulier b appartient à (a) et $\mathcal{I} \subset (a)$.

Exercice 887

1. Soit $\Bbbk$ un corps. Si P est un pgcd des P_i, dans $\Bbbk[X]$, quels sont les autres pgcd des P_i ?
2. Calculer $\operatorname{pgcd}(5X^2 + 3, X^3 + X)$.

Éléments de réponse 887

1. Soit $\Bbbk$ un corps. Soit P est un pgcd des P_i dans $\Bbbk[X]$. Un pgcd est défini à inversible près et les inversibles de $\Bbbk[X]$ sont les constantes non nulles. Les pgcd possibles sont donc les polynômes cP où $c \in \Bbbk$ est une constante non nulle.
2. Déterminons $\operatorname{pgcd}(5X^2+3, X^3+X)$. Nous procédons comme avec les entiers. Nous faisons une suite de divisions donnée par l'algorithme d'Euclide et le pgcd est le dernier reste non nul. Ici :
$$X^3 + X = \frac{1}{5}X(5X^2 + 3) + \frac{2}{5}X, \qquad 5X^2 + 3 = \frac{25}{2}X\left(\frac{2}{5}X\right) + 3, \qquad \frac{2}{5}X = 3\,\frac{2}{15}X + 0$$
Le pgcd de $5X^2+3$ et X^3+X est donc 3 ou encore 1 à inversible près. Les deux polynômes $5X^2 + 3$ et $X^3 + X$ sont donc premiers entre eux.

Exercice 888

Montrer que $\mathbb{Z}[X]$ n'est pas euclidien en montrant que $(2, X)$ n'est pas principal.

Éléments de réponse 888

Montrons que $(2, X)$ n'est pas principal. Raisonnons par l'absurde : supposons qu'il existe un polynôme P tel que $(2, X) = (P)$. En particulier 2 appartient à (P), c'est-à-dire P divise 2. Notons que les diviseurs de 2 dans $\mathbb{Z}[X]$ sont 1, 2, -1 et -2.

- ◇ Si $P = 2$ ou -2, alors les multiples de P sont des polynômes dont tous les coefficients sont divisibles par 2. En particulier $X \in (P)$ a des coefficients divisibles par 2 : contradiction.
- ◇ Si $P = 1$ ou -1, alors $(P) = \mathbb{Z}[X]$. Un polynôme de $(2, X)$ s'écrit par définition $2A + XB$ avec A, B dans $\mathbb{Z}[X]$; le terme constant d'un tel polynôme est divisible par 2 ce qui n'est pas le cas du polynôme constant égal à 1. Il en résulte que 1 n'appartient pas à $(2, X)$. Mais 1 appartient à $(P) = \mathbb{Z}[X]$. Ainsi $(2, X) \neq P$.

Puisque $(2, X)$ n'est pas principal, $\mathbb{Z}[X]$ n'est pas euclidien.

Exercice 889

Montrer en vous ramenant à un travail sur $\mathbb{Q}$ que la décomposition en facteurs irréductibles dans $\mathbb{Z}[X]$ est essentiellement unique.

Éléments de réponse 889

Soit $P \in \mathbb{Z}[X]$ un polynôme. Soit

$$P = a_1 a_2 \dots a_r P_1 P_2 \dots P_s = b_1 b_2 \dots b_t Q_1 Q_2 \dots Q_u$$

deux décompositions de P dans $\mathbb{Z}[X]$ où a_i et b_i sont dans $\mathbb{Z}$ tandis que les autres termes sont des polynômes non constants de contenu égal à 1. Nous voulons démontrer l'unicité à permutation et au signe près, c'est-à-dire nous voulons démontrer que $r = t$, $s = u$ et $a_i = \varepsilon_i b_i$, $P_i = \varepsilon_i Q_i$ où $\varepsilon_i \in \{\pm 1\}$. Le contenu de P est $a_1 a_2 \dots a_r = b_1 b_2 \dots b_t$. Le polynôme $\frac{P}{\mathrm{ct}(P)} \in \mathbb{Z}[X]$ admet les deux décompositions $P_1 P_2 \dots P_s$ et $Q_1 Q_2 \dots Q_u$. Ce sont aussi des décompositions sur $\mathbb{Q}[X]$ donc par unicité de la décomposition sur les rationnels, nous avons $s = u$ et quitte à réordonner les facteurs $P_i = \varepsilon_i Q_i$. Enfin $a_1 a_2 \dots a_r$ et $b_1 b_2 \dots b_t$ sont deux décompositions dans $\mathbb{Z}$ de l'entier $\mathrm{ct}(P)$ (défini au signe près) ; par unicité de la décomposition sur $\mathbb{Z}$, nous obtenons $r = s$ et $a_i = \varepsilon_i b_i$ à permutation des a_i près.

Exercice 890

1. Si A est un corps contenant un nombre infini d'éléments. La fonction $A[X] \to A^A$, définie par $P \mapsto \widetilde{P}$ est un morphisme d'anneaux injectifs (en particulier, on peut assimiler polynômes et fonctions polynômiales).
2. Peut-on généraliser l'identification entre polynômes et fonctions polynômiales sans les hypothèses sur A ?

Éléments de réponse 890

1. Soit A est un corps contenant un nombre infini d'éléments. La fonction $\varphi\colon A[X] \to A^A$, définie par $P \mapsto \widetilde{P}$ où $\widetilde{P}$ est un morphisme d'anneaux injectifs (en particulier, on peut assimiler polynômes et fonctions polynômiales). En effet c'est clairement un morphisme. D'après un exercice précédent si A est un anneau intègre et P un polynôme non nul, alors $\widetilde{P}$ est une fonction ayant un nombre de zéros inférieur ou égal au degré de P. La fonction nulle ayant un nombre infini de zéros, $\widetilde{P}$ n'est pas la fonction nulle dès que P est non nul. Il s'en suit que le noyau de φ est réduit au polynôme nul : φ est injectif.
2. Nous ne pouvons pas généraliser l'identification entre polynômes et fonctions polynômiales sans les hypothèses sur A ; comme nous l'avons vu en cours le polynôme $P = X^2 + X$ dans $\mathbb{Z}/2\mathbb{Z}$ satisfait les propriétés suivantes :
   - ◇ le polynôme P est non nulle,

◇ la fonction polynomiale associée à P est nulle.

Exercice 891

Soit $P = \sum a_i X^i \in \mathbb{Z}[X]$, p un nombre premier et $\overline{P} = \sum \overline{a_i} X^i$ l'image $\overline{P}$ de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.

1. Comparer le degré de P et celui de P. À quelle condition a-t-on égalité ?
2. Si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et a même degré que P, montrer que $P \in \mathbb{Z}[X]$ est irréductible
3. Décomposer $\overline{P} = X^3 + X^2 + X + \overline{1}$ sur $\mathbb{Z}/3\mathbb{Z}$.
4. Montrer que $P = X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Z}$.

Éléments de réponse 891

Soient $P = \sum a_i X^i \in \mathbb{Z}[X]$, p un nombre premier et $\overline{P} = \sum \overline{a_i} X^i$ l'image de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.

1. Nous avons $\deg \widetilde{P} \leq \deg P$ avec égalité si et seulement si p ne divise pas le coefficient dominant a_n de P.
2. Montrons que si $P \in \mathbb{Z}[X]$ est réductible, alors $\overline{P}$ est réductible. Supposons que $P \in \mathbb{Z}[X]$ soit réductible, c'est-à-dire que $P = QR$. Nous avons $\overline{P} = \overline{Q}\,\overline{R}$. Pour montrer que $\overline{P}$ est réductible il suffit donc de montrer que $\overline{Q}$ et $\overline{R}$ sont non inversibles, *i.e.* non constants. Nous avons d'une part
$$\deg \overline{P} = \deg \overline{Q} + \deg \overline{R} \leq \deg Q + \deg R = \deg(QR) = \deg P$$
et d'autre part $\deg \overline{P} = \deg P$. Il en résulte que $\deg Q = \deg \overline{Q}$ et $\deg R = \deg \overline{R}$. Puisque par hypothèse Q et R sont des polynômes non constants nous obtenons que $\overline{Q}$ et $\overline{R}$ sont non constants.
3. Décomposons $\overline{P} = X^3 + X^2 + X + \overline{1}$ sur $\mathbb{Z}/3\mathbb{Z}$.
   Si P était réductible, nous aurions $P = QR$ avec Q de degré 2 et $R = aX + b$ de degré 1. En particulier P aurait une racine $-\frac{b}{a}$. Ainsi pour montrer que P est irréductible il suffit de voir que P n'a pas de racine. Remarquons que
$$P(\overline{0}) = \overline{1}, \qquad P(\overline{1}) = \overline{1}, \qquad P(\overline{2}) = \overline{2};$$
   autrement dit P est sans racine donc irréductible.
4. Montrons que $P = X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Z}$. L'image $\overline{P}$ de P est irréductible dans $\mathbb{Z}/3\mathbb{Z}[X]$ d'après 3. et a même degré que P. Le point 2. assure alors que P est irréductible.

Exercice 892

Soit $P = a_0 + a_1 X + \ldots + a_n X^n$ un polynôme de degré $n \geq 1$ à coefficients dans $\mathbb{Z}$.

1. Supposons que P ait une racine rationnelle $r \in \mathbb{Q}$. Posons $r = \frac{u}{v}$, où $u \in \mathbb{Z}$, $v \in \mathbb{Z} \setminus \{0\}$ et $\operatorname{pgcd}(u, v) = 1$.

a) Montrer que v divise a_n.

b) Montrer que u divise a_0.

2. En déduire que si P est unitaire, alors tout racine rationnelle de P est entière.
3. Soit $a \in \mathbb{Z}$. Posons $P = X^3 + aX + 2$. Montrer que P a (au moins) une racine dans $\mathbb{Q}$ si et seulement si a appartient à $\{-5, -3, 1\}$.

Éléments de réponse 892

1. Nous avons $0 = P(r) = a_0 + a_1\frac{u}{v} + a_2\frac{u^2}{v^2} + \ldots + a_n\frac{u^n}{v^n}$. En multiplicant par v^n il vient

$$a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \ldots + a_{n-1}u^{n-1}v + a_nu^n = 0. \tag{3.4.2}$$

a) L'égalité (3.4.2) se réécrit

$$a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \ldots + a_{n-1}u^{n-1}v = -a_nu^n.$$

Puisque v divise $a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \ldots + a_{n-1}u^{n-1}v$, v divise $-a_nu^n$. Comme v est premier à u, v divise a_n.

b) L'égalité (3.4.2) se réécrit

$$-a_0v^n = a_1uv^{n-1} + a_2u^2v^{n-2} + \ldots + a_{n-1}u^{n-1}v + a_nu^n.$$

Puisque u divise $a_1uv^{n-1} + a_2u^2v^{n-2} + \ldots + a_{n-1}u^{n-1}v + a_nu^n$, u divise $-a_0v^n$. Comme u est premier à v, u divise a_0.

2. Si P est unitaire, *i.e.* si $a_n = 1$, alors v divise 1 (d'après 1.a)) et $v = \pm 1$. Il en résulte que $r = \pm u$; en particulier r appartient à $\mathbb{Z}$.
3. Supposons que P possède une racine $r \in \mathbb{Q}$. Puisque P est unitaire, r appartient à $\mathbb{Z}$ d'après 2. De plus 1.b) assure que r divise le terme constant de P qui ici vaut 2. Il s'en suit que $r \in \{-2, -1, 1, 2\}$.

   ◇ Si $r = -2$, alors $0 = r^3 + ar + 2 = -8 - 2a + 2$ et $a = -3$.

   ◇ Si $r = -1$, alors $0 = r^3 + ar + 2 = -1 - a + 2$ et $a = 1$.

   ◇ De même si $r = 1$, alors $a = -3$ et si $r = 2$, alors $a = -5$.

   Finalement a appartient à $\{-5, -3, 1\}$.

   Cela montre aussi que, réciproquement, si a appartient à $\{-5, -3, 1\}$, alors P a une racine entière.

Exercice 893

Soit $\mathcal{I}$ l'ensemble des polynômes $P \in \mathbb{Z}[X]$ tels que $P(0)$ appartient à $2\mathbb{Z}$:

$$\mathcal{I} = \{P \in \mathbb{Z}[X] \,|\, P(0) \in 2\mathbb{Z}\}$$

1. Montrer que $\mathcal{I}$ est un idéal de $\mathbb{Z}[X]$.

2. Montrer que $\mathcal{I}$ n'est pas un idéal principal, *i.e.* qu'il n'existe aucun polynôme $Q \in \mathbb{Z}[X]$ tel que $\mathcal{I} = Q\mathbb{Z}[X]$.

Éléments de réponse 893

1. Soient P et Q deux éléments de $\mathcal{I}$. Les entiers $P(0)$ et $Q(0)$ sont pairs donc $(P+Q)(0) = P(0)+Q(0)$ est pair et $(P+Q)$ appartient à $\mathcal{I}$. L'entier $(-P)(0) = -P(0)$ est pair, ainsi $-P$ appartient à $\mathcal{I}$. Enfin le polynôme nul appartient à $\mathcal{I}$. Il en résulte que $\mathcal{I}$ est un sous-groupe de $\mathbb{Z}[X]$. De plus, pour tout $Q \in \mathbb{Z}[X]$, nous avons $(PQ)(0) = P(0)Q(0)$; il s'en suit que $(PQ)(0)$ est pair et que PQ appartient à $\mathcal{I}$. Finalement $\mathcal{I}$ est un idéal de $\mathbb{Z}[X]$.
2. Supposons qu'il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que $\mathcal{I} = Q\mathbb{Z}[X]$. Puisque le polynôme constant 2 appartient à $\mathcal{I}$, le polynôme Q divise 2. Par suite Q est l'un des polynômes constants 1, -1, 2 ou -2.
   - ◇ Si $Q = \pm 2$, alors $\mathcal{I} = 2\mathbb{Z}[X]$; par conséquent tous les coefficients des polynômes de $\mathcal{I}$ sont pairs : contradiction avec le fait que le polynôme X n'appartienne pas à $\mathcal{I}$.
   - ◇ Si $Q = \pm 1$, alors $\mathcal{I} = \mathbb{Z}[X]$: contradiction avec le fait que le polynôme 1 appartienne à $\mathcal{I}$.

   Nous en déduisons qu'il n'y a pas de polynôme $Q \in \mathbb{Z}[X]$ tel que $\mathcal{I} = Q\mathbb{Z}[X]$.

Exercice 894

Soit p un nombre premier. Pour tout entier k, désignons par $\overline{k}$ sa classe dans $\mathbb{F}_p$. Soit ρ le morphisme de réduction modulo p

$$\rho\colon \mathbb{Z}[X] \to \mathbb{F}_p, \qquad p_0 + p_1X + p_2X^2 + \ldots + p_nX^n \mapsto \overline{p_0} + \overline{p_1}X + \overline{p_2}X^2 + \ldots + \overline{p_n}X^n.$$

Notons $\pi\colon \mathbb{Z}[X] \to {}^{\mathbb{Z}[X]}\!/_{(X^2+1)\mathbb{Z}[X]}$ et $\pi_p\colon \mathbb{F}_p[X] \to {}^{\mathbb{F}_p[X]}\!/_{(X^2+1)\mathbb{F}_p[X]}$ les projections canoniques.

1. Montrer que la composée $\pi_p \circ \rho$ passe au quotient et définit un morphisme d'anneaux surjectif
$$\overline{\rho}\colon {}^{\mathbb{Z}[X]}\!/_{(X^2+1)\mathbb{Z}[X]} \to {}^{\mathbb{F}_p[X]}\!/_{(X^2+1)\mathbb{F}_p[X]}$$
et que pour tout $P \in \mathbb{Z}[X]$ nous avons $\overline{\rho}(\pi(P)) = \pi_p(\rho(P))$.
2. Soit $f\colon \mathbb{Z}[\mathbf{i}] \to {}^{\mathbb{Z}[X]}\!/_{(X^2+1)\mathbb{Z}[X]}$ l'isomorphisme d'anneaux défini par
$$\forall\, a,\, b \in \mathbb{Z} \quad f(a + \mathbf{i}b) = \pi(a + bX).$$
Montrer que la composée $\overline{\rho} \circ g$ se factorise par le quotient ${}^{\mathbb{Z}[\mathbf{i}]}\!/_{p\mathbb{Z}[\mathbf{i}]}$ et définit un isomorphisme d'anneaux
$$F\colon {}^{\mathbb{Z}[\mathbf{i}]}\!/_{p\mathbb{Z}[\mathbf{i}]} \xrightarrow{\simeq} {}^{\mathbb{F}_p[X]}\!/_{(X^2+1)\mathbb{F}_p[X]}$$

Éléments de réponse 894

1. Pour tout polynôme $P = p_0 + p_1X + p_2X^2 + \ldots + p_nX^n \in \mathbb{Z}[X]$, nous avons

$$\pi_p \circ \rho(P) = \pi_p(\overline{p_0} + \overline{p_1}X + \overline{p_2}X^2 + \ldots + \overline{p_n}X^n)$$

Soit P un élément de $(X^2+1)\mathbb{Z}[X]$, autrement dit supposons que P s'écrive $(X^2+1)Q$. Puisque ρ est un morphisme d'anneaux, $\rho(P) = \rho(X^2+1)\rho(Q)$. Comme $\rho(X^2+1) = X^2+1 \in \mathbb{F}_p[X]$ nous obtenons que $\rho(P)$ appartient à $(X^2+1)\mathbb{F}_p[X]$. Nous en déduisons que $\pi_p(\rho(P)) = 0$. Ainsi l'idéal $(X^2+1)\mathbb{Z}[X]$ est inclus dans $\ker(\pi_p \circ \rho)$. Le théorème de passage au quotient assure l'existence d'un morphisme d'anneaux

$$\overline{\rho}\colon {}^{\mathbb{Z}[X]}\!\diagup_{(X^2+1)\mathbb{Z}[X]} \to {}^{\mathbb{F}_p[X]}\!\diagup_{(X^2+1)\mathbb{F}_p[X]}$$

tel que pour tout $P \in \mathbb{Z}[X]$ nous avons $\overline{\rho}(\pi(P)) = \pi_p(\rho(P))$.

Étant donné que π_p et ρ sont surjectifs, la composée $\pi_p \circ \rho$ est surjective ; il s'en suit que $\overline{\rho}$ est surjectif.

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\quad\rho\quad} & \mathbb{F}_p[X] \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi_p} \\ {}^{\mathbb{Z}[X]}\!\diagup_{(X^2+1)\mathbb{Z}[X]} & \xrightarrow{\quad\overline{\rho}\quad} & {}^{\mathbb{F}_p[X]}\!\diagup_{(X^2+1)\mathbb{F}_p[X]} \end{array}$$

2. La composée $\overline{\rho} \circ f$ est surjective car $\overline{\rho}$ et f le sont. Pour tous entiers a, b dans $\mathbb{Z}$ nous avons

$$\overline{\rho}(f(a+\mathbf{i}b)) = \overline{\rho}(\pi(a+bX)) = \pi_p(\rho(a+bX)) = \pi(\overline{a} + \overline{b}X).$$

Étudions le noyau de $\overline{\rho} \circ f$. Pour tous a, b dans $\mathbb{Z}$ nous avons

$$\overline{\rho} \circ f(a+\mathbf{i}b) = 0 \iff \pi_p(\overline{a} + \overline{b}X) = 0 \iff (\overline{a} + \overline{b}X) \in (X^2+1)\mathbb{F}_p[X].$$

Les multiples non nuls de X^2+1 sont de degré au moins 2 ; par conséquent

$$(\overline{a} + \overline{b}X) \in (X^2+1)\mathbb{F}_p[X] \iff \overline{a} + \overline{b}X = 0.$$

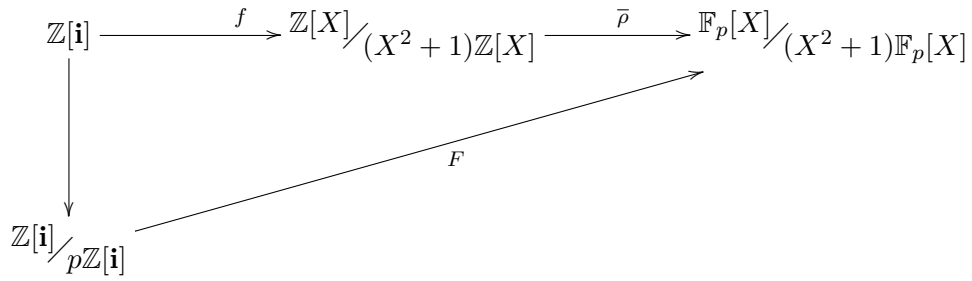
De plus,

$$\overline{a} + \overline{b}X = 0 \iff \overline{a} = \overline{b} = 0 \iff \text{ } a \text{ et } b \text{ sont multiples de } p \iff a + \mathbf{i}b \in p\mathbb{Z}[\mathbf{i}].$$

Ainsi $\ker \overline{\rho} \circ f = p\mathbb{Z}[\mathbf{i}]$ et le théorème de passage au quotient assure que $\overline{\rho} \circ f$ définit un morphisme d'anneaux injectif

$$F\colon {}^{\mathbb{Z}[\mathbf{i}]}\!\diagup_{p\mathbb{Z}[\mathbf{i}]} \xrightarrow{\simeq} {}^{\mathbb{F}_p[X]}\!\diagup_{(X^2+1)\mathbb{F}_p[X]}.$$

Enfin $\overline{\rho}$ et f étant surjectifs, $\overline{\rho} \circ f$ est surjectif et finalement F aussi.



Exercice 895

1. Calculer $\begin{pmatrix} 509 \\ 108 \end{pmatrix} \bmod 7$.
2. Soient k, n des entiers tels que $0 < k \leq n$. Calculer $\begin{pmatrix} p^n - 1 \\ p^k \end{pmatrix} \bmod p$.

Éléments de réponse 895

1. Nous avons

   $$509 = 5 + 2 \times 7 + 3 \times 7^2 + 1 \times 7^3 \qquad \text{et} \qquad 108 = 3 + 1 \times 7 + 2 \times 7^2 + 0 \times 7^3$$

   Par suite

   $$\begin{pmatrix} 509 \\ 108 \end{pmatrix} \equiv_7 \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv_7 \frac{5 \times 4}{2} \times 2 \times 3 \times 1 \equiv_7 3 \times 2 \times 3 \bmod 7 \equiv_7 4$$

2. Nous avons

   $$p^n - 1 = (p-1)(1 + p + p^2 + \ldots + p^{n-1}) = (p-1) + (p-1)p + \ldots + (p-1)p^{n-1}.$$

   Par suite les chiffres de $p^n - 1$ en base p sont donc tous égaux à $p - 1$. Les chiffres de p^r en base p sont tous nuls sauf celui relatif à p^r qui vaut 1. Nous avons $\begin{pmatrix} p-1 \\ 0 \end{pmatrix} = 1$ et comme $r \leq n$ nous en déduisons

   $$\begin{pmatrix} p^n - 1 \\ p^r \end{pmatrix} \equiv_p \begin{pmatrix} p-1 \\ 1 \end{pmatrix} \equiv_p p - 1 \equiv_p -1.$$

Exercice 896

Soit a un entier au moins égal à 2. Soit n un entier strictement positif. Montrer que pour tout diviseur d de n, $a^d - 1$ divise $a^n - 1$.

Éléments de réponse 896

Posons $n = dm$. Nous avons

$$X^m - 1 = (X-1)(X^{m-1} + X^{m-2} + \ldots + X + 1) = (X-1)Q(X)$$

où Q désigne un élément de $\mathbb{Z}[X]$. Remplaçons X par X^d. Nous obtenons alors l'égalité

$$(X^d - 1)Q(X^d) = (X^d)^m - 1 = X^{dm} - 1 = X^n - 1.$$

En évaluant en a, il vient $(a^d - 1)Q(a^d) = a^n - 1$. Puisque $Q(a^d)$ est un entier, $a^d - 1$ divise $a^n - 1$.

3.5. Anneaux et corps

Exercice 897

Soient n et m des entiers au moins égaux à 2.

1. Montrer que si n n'est pas multiple de m, il n'existe pas de morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.
2. Montrer qu'il existe un unique morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si n est multiple de m.

Éléments de réponse 897

1. Supposons qu'il existe un morphisme d'anneaux $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Nous avons $f(\overline{1}_{[n]}) = \overline{1}_{[m]}$. Nous en déduisons pour tout $k \in \mathbb{Z}$

   $$f(\overline{k}_{[n]}) = f(k\overline{1}_{[n]}) = kf(\overline{1}_{[n]}) = k\overline{1}_{[m]} = \overline{k}_{[m]}.$$

   Il s'en suit que le morphisme f est unique. Puisque $\overline{n}_{[n]} = \overline{0}_{[n]}$, nous obtenons

   $$\overline{0}_{[m]} = f(\overline{0}_{[n]}) = f(\overline{n}_{[n]}) = \overline{n}_{[m]}$$

   dont nous déduisons que n est multiple de m.
2. Réciproquement, supposons que n soit un multiple de m. Alors, dans le groupe $\mathbb{Z}/m\mathbb{Z}$ nous avons $n\overline{1}_{[m]} = \overline{0}_{[m]}$; par suite il existe un morphisme de groupes $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ tel que $f(\overline{1}_{[n]}) = \overline{1}_{[m]}$. Pour tous $\overline{k}_{[n]}$ et $\overline{\ell}_{[n]}$ dans $\mathbb{Z}/n\mathbb{Z}$ nous avons

   $$f(\overline{k}_{[n]}\overline{\ell}_{[n]}) = f(k\ell\overline{1}_{[n]}) = k\ell f(\overline{1}_{[n]}) = k\ell\overline{1}_{[m]} = \overline{k}_{[m]}\overline{\ell}_{[m]}$$

   Il en résulte que f est un morphisme d'anneaux.

Exercice 898

Expliciter un isomorphisme d'anneaux entre $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ et $\mathbb{Z}/65\mathbb{Z}$ et l'isomorphisme réciproque.

Éléments de réponse 898

L'isomorphisme entre $\mathbb{Z}/65\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ des restes chinois est défini par

$$f\colon \mathbb{Z}/65\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}, \qquad \overline{x}_{[65]} \mapsto (\overline{x}_{[5]}, \overline{x}_{[13]})$$

La relation de Bézout $2 \times 13 - 5 \times 5 = 1$ indique que

$$2 \times 13 \equiv \begin{cases} 1 \bmod 5 \\ 0 \bmod 13 \end{cases} \qquad \text{et} \qquad -5 \times 5 \equiv \begin{cases} 0 \bmod 5 \\ 1 \bmod 13 \end{cases}$$

Pour tous entiers a et b, nous avons $26a - 25b \equiv \begin{cases} a \bmod 5 \\ b \bmod 13 \end{cases}$. Considérons

$$g\colon \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \to \mathbb{Z}/65\mathbb{Z}, \qquad (\overline{x}_{[5]}, \overline{y}_{[13]}) \mapsto \overline{26x - 25y}_{[65]}.$$

On constate que $g \circ f = \mathrm{id}$ et $f \circ g = \mathrm{id}$.

Exercice 899

1. Quel est l'ordre du groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$?
2. Montrer que le groupe $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$ est cyclique.
3. En déduire que le groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est cyclique.
4. Déterminer un générateur de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$.
5. Combien y a-t-il de générateurs du groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$?
6. Déterminer tous les générateurs de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$.
7. Le groupe $\left(\mathbb{Z}/33\mathbb{Z}\right)^\times$ est-il cyclique ?

Éléments de réponse 899

1. L'ordre de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est
$$\varphi(22) = \varphi(2 \times 11) = (2-1)(11-1) = 10.$$
2. Comme 11 est un nombre premier, le groupe $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$ est d'ordre 10. Ainsi tout $x \in \left(\mathbb{Z}/11\mathbb{Z}\right)^\times \setminus \{\overline{1}\}$ est d'ordre 2, 5 ou 10.

   Nous avons $2^2 \equiv_{11} 4$ et $2^5 = 32 \equiv_{11} -1$. Autrement dit $\overline{2}^2 = \overline{4} \neq \overline{1}$ et $\overline{2}^5 = -\overline{1} \neq \overline{1}$; il en résulte que l'ordre de $\overline{2}$ dans $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$ est 10. En particulier $\overline{2}$ est un générateur de $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$.

3. L'isomorphisme d'anneaux $f\colon \mathbb{Z}/22\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ des restes chinois induit un isomorphisme de groupes $f^\times\colon \left(\mathbb{Z}/22\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/2\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/11\mathbb{Z}\right)^\times$. Puisque $\left(\mathbb{Z}/2\mathbb{Z}\right)^\times = \{1\}$ le groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est isomorphe à $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$. En particulier $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est cyclique.
4. Puisque $\overline{2}$ engendre $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$, l'élément $b \in \left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ tel que $f^\times(b) = (\overline{1}_{[2]}, \overline{2})$ est un générateur de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$. Pour calculer b il suffit de prendre la classe modulo 22 d'un entier $x \in \mathbb{Z}$ tel que $x \equiv_2 1$ et $x \equiv_{11} 2$. La relation de Bézout $11 - 2 \times 5 = 1$ montre que $x = 11 \times 1 - 10 \times 2 = -9$ convient. Ainsi $b = -\overline{9}_{[22]} = \overline{13}_{[22]}$ est un générateur du groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$.
5. Le groupe $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est un groupe cyclique d'ordre 10 ; par conséquent le nombre de générateur de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ est $\varphi(10) = \varphi(2 \times 5) = 1 \times 4 = 4$.
6. Étant donné que b est un générateur, les générateurs sont les éléments b^k où k est premier à 10 et $1 \leq k \leq 10$, c'est-à-dire $k \in \{1, 3, 7, 9\}$. Les générateurs de $\left(\mathbb{Z}/22\mathbb{Z}\right)^\times$ sont donc $\overline{13}$, $\overline{13}^3 = \overline{19}$, $\overline{13}^7 = \overline{7}$ et $\overline{13}^9 = \overline{17}$.
7. Rappelons l'énoncé suivant :

Soient C_p un groupe cyclique à p éléments et C_q un groupe cyclique à q éléments. Le groupe $\mathrm{C}_p \times \mathrm{C}_q$ est cyclique si et seulement si p et q sont premiers entre eux.

Le groupe $\left(\mathbb{Z}/33\mathbb{Z}\right)^\times$ est isomorphe à $\left(\mathbb{Z}/3\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/11\mathbb{Z}\right)^\times$. D'une part $\left(\mathbb{Z}/3\mathbb{Z}\right)^\times = \{1, -1\}$ est cyclique d'ordre 2 et d'autre part $\left(\mathbb{Z}/11\mathbb{Z}\right)^\times$ est cyclique d'ordre 10. Étant donné que 2 et 10 ne sont pas premiers entre eux, $\left(\mathbb{Z}/3\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/11\mathbb{Z}\right)^\times$ n'est pas cyclique.

Exercice 900

Expliciter un isomorphisme d'anneaux entre $\left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/12\mathbb{Z}\right)$ et $\left(\mathbb{Z}/4\mathbb{Z}\right) \times \left(\mathbb{Z}/6\mathbb{Z}\right)$.

Éléments de réponse 900

Le théorème des restes chinois assure l'existence des isomorphismes d'anneaux

$$f\colon \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/12\mathbb{Z}\right) \to \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z}\right) \times \left(\mathbb{Z}/4\mathbb{Z}\right)$$
$$g\colon \left(\mathbb{Z}/4\mathbb{Z}\right) \times \left(\mathbb{Z}/6\mathbb{Z}\right) \to \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z}\right) \times \left(\mathbb{Z}/4\mathbb{Z}\right)$$

définis par

$$f(\overline{x}_{[2]}, \overline{y}_{[12]}) = (\overline{x}_{[2]}, \overline{y}_{[3]}, \overline{y}_{[4]}) \qquad g(\overline{x}_{[6]}, \overline{y}_{[4]}) = (\overline{x}_{[2]}, \overline{x}_{[3]}, \overline{y}_{[4]})$$

L'application $h = g^{-1} \circ f \colon \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/12\mathbb{Z}\right) \to \left(\mathbb{Z}/4\mathbb{Z}\right) \times \left(\mathbb{Z}/6\mathbb{Z}\right)$ est donc un isomorphisme d'anneaux.

Explicitons g^{-1}. Puisque $3-2=1$, pour tous entiers a et b, nous avons $3a-2b \equiv \begin{cases} a \bmod 2 \\ b \bmod 3 \end{cases}$

Il en résulte que

$$g(\overline{3a-2b}_{[6]}, \overline{y}_{[4]}) = (\overline{a}_{[2]}, \overline{b}_{[3]}, \overline{y}_{[4]}), \qquad g^{-1}(\overline{a}_{[2]}, \overline{b}_{[3]}, \overline{y}_{[4]}) = (\overline{3a-2b}_{[6]}, \overline{y}_{[4]}).$$

Il vient pour tous x et y dans $\mathbb{Z}$

$$h(\overline{x}_{[2]}, \overline{y}_{[12]}) = g^{-1} \circ f(\overline{x}_{[2]}, \overline{y}_{[12]}) = g^{-1}(\overline{x}_{[2]}, \overline{y}_{[3]}, \overline{y}_{[4]}) = (\overline{3x-2y}_{[6]}, \overline{y}_{[4]}).$$

Exercice 901

1. Montrer que le groupe $\left(\mathbb{Z}/455\mathbb{Z}\right)^\times$ est isomorphe au groupe produit $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/7\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/13\mathbb{Z}\right)^\times$.
2. En déduire que si un entier $a \in \mathbb{Z}$ n'est multiple ni de 5, ni de 7, ni de 13, alors $a^{12} \equiv_{455} 1$.
3. Le groupe $\left(\mathbb{Z}/455\mathbb{Z}\right)^\times$ possède-t-il des éléments d'ordre 12 ? Indication : calculer l'ordre de $\overline{2}$ dans $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$.

Éléments de réponse 901

1. Remarquons que $455 = 5 \times 7 \times 13$. Le théorème des restes chinois assure l'existence d'un isomorphisme d'anneaux
$$\varphi\colon \mathbb{Z}/455\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$$
entre $\mathbb{Z}/455\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. L'isomorphisme φ définit un isomorphisme de groupes multiplicatifs
$$\varphi^\times\colon \left(\mathbb{Z}/455\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/5\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/7\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/13\mathbb{Z}\right)^\times$$
2. Le groupe $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times$ est d'ordre 4 ; ainsi pour tout $x \in \left(\mathbb{Z}/5\mathbb{Z}\right)^\times$ nous avons $x^4 = 1$ et $x^{12} = 1$. De même le groupe $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ est d'ordre 6 ; par suite pour tout $y \in \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ nous avons $y^6 = 1$ et $y^{12} = 1$. Enfin, pour tout $z \in \left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ nous avons $z^{12} = 1$ car $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ est d'ordre 12. Il en résulte que $(x, y, z)^{12} = 1$ pour tout $(x, y, z) \in \left(\mathbb{Z}/5\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/7\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/13\mathbb{Z}\right)^\times$. Par l'isomorphisme $\varphi^\times$ nous en déduisons que $\overline{a}^{12} = 1$ pour tout $\overline{a} \in \left(\mathbb{Z}/455\mathbb{Z}\right)^\times$.
3. La classe $\overline{2}$ de 2 dans $\mathbb{Z}/13\mathbb{Z}$ appartient à $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$; de plus, $\overline{2}$ est d'ordre 12. Par conséquent l'élément $(1, 1, g)$ du groupe $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/7\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ est d'ordre 12. Nous en déduisons que $(\varphi^\times)^{-1}(1, 1, g)$ est un élément d'ordre 12 du groupe $\left(\mathbb{Z}/455\mathbb{Z}\right)^\times$.

Exercice 902

1. Soit A un anneau. Soient x et y deux éléments de A. Montrer que si le produit xy est inversible, alors x et y sont inversibles.
2. Trouver les entiers $a \in \mathbb{Z}$ tels que $3a^5 \equiv_7 1$.
3. Trouver les entiers $a \in \mathbb{Z}$ tels que $a^3 \equiv_{85} 1$.

Éléments de réponse 902

1. Supposons que xy soit inversible, *i.e.* qu'il existe $b \in A$ tel que $(xy)b = 1$. Nous avons alors $x(yb) = 1 = (xb)y$. Ainsi x est inversible d'inverse yb et y est inversible d'inverse xb.
2. Posons $x = \overline{a}_{[7]}$. L'équation $3a^5 \equiv_7 1$ se réécrit alors $3x^5 = 1$ dans le corps $\mathbb{Z}/7\mathbb{Z}$. Si x est solution de $3x^5 = 1$ dans le corps $\mathbb{Z}/7\mathbb{Z}$, alors $x \neq 0$ et $x^6 = 1$ (en effet $\mathbb{Z}/7\mathbb{Z}$ est d'ordre 6). En multipliant par x nous avons donc l'équivalence
$$3x^5 = 1 \quad \Longleftrightarrow \quad 3 = 3x^6 = x.$$
Les solutions de l'équation $3a^5 \equiv_7 1$ sont donc les entiers de la forme $3 + 7k$ avec $k \in \mathbb{Z}$:
$$\{a \,|\, 3a^5 \equiv_7 1\} = \{3 + 7k \,|\, k \in \mathbb{Z}\}.$$
3. Posons $x = \overline{a}_{[85]}$. L'équation $a^3 \equiv_{85} 1$ se réécrit alors $x^3 = 1$ dans l'anneau $\mathbb{Z}/85\mathbb{Z}$. Si x est solution de cette équation, alors la question précédente assure que x est inversible dans $\mathbb{Z}/85\mathbb{Z}$, *i.e.* x appartient à $\left(\mathbb{Z}/85\mathbb{Z}\right)^\times$. Par ailleurs, d'une part $85 = 5 \times 17$ et d'autre part $\operatorname{pgcd}(5, 17) = 1$; il en résulte que l'application
$$\left(\mathbb{Z}/85\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/5\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/17\mathbb{Z}\right)^\times, \qquad \overline{q} \mapsto (\overline{q}_{[5]}, \overline{q}_{[17]})$$
est un isomorphisme de groupes. Pour tout $a \in \mathbb{Z}$ nous avons donc
$$a^3 \equiv_{85} 1 \quad \Longleftrightarrow \quad (\overline{a}_{[5]}, \overline{a}_{[17]})^3 = (\overline{1}_{[5]}, \overline{1}_{[17]}).$$
Autrement dit $a^3 \equiv_{85} 1$ si et seulement si $\overline{a}_{[5]}$ est d'ordre 1 ou 3 dans $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times$ et $\overline{a}_{[17]}$ est d'ordre 1 ou 3 dans $\left(\mathbb{Z}/17\mathbb{Z}\right)^\times$.

Remarquons que $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times$ est d'ordre 4 et $\left(\mathbb{Z}/17\mathbb{Z}\right)^\times$ est d'ordre 16. Par conséquent dans ces deux groupes tout élément est d'ordre une puissance de 2 ; en particulier ces deux groupes ne contiennent pas d'élément d'ordre 3. Nous en déduisons que
$$a^3 \equiv_{85} 1 \quad \Longleftrightarrow \quad a \equiv_5 1 \text{ et } a \equiv_{17} 1$$
puis que
$$a^3 \equiv_{85} 1 \quad \Longleftrightarrow \quad a \equiv_{85} 1.$$
Finalement les solutions de l'équation $a^3 \equiv_{85} 1$ sont les entiers $a = 1 + 85k$ où $k \in \mathbb{Z}$:
$$\{a \,|\, a^3 \equiv_{85} 1\} = \{1 + 85k \,|\, k \in \mathbb{Z}\}.$$

Exercice 903

Soit n un entier au moins égal à 2.

1. Soit d un diviseur positif de n.

   Désignons par H_d l'unique sous-groupe à d éléments de $\mathbb{Z}/n\mathbb{Z}$.

1.a) Montrer que H_d contient les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

1.b) Montrer que H_d possède $\varphi(d)$ éléments d'ordre d.

2. En déduire l'égalité $n = \sum_{\substack{d|n \\ d>0}} \varphi(d)$.

Éléments de réponse 903

1.a) Posons $n = dd'$. Alors $\mathrm{H}_d = \langle \overline{d'} \rangle = \{\overline{0}, \overline{d'}, \ldots, \overline{(d-1)d'}\}$. Soit $\overline{k}$ un élément de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{k}$ est donc d'ordre d ; par unicité nous avons $\langle \overline{k} \rangle = \mathrm{H}_d$. En particulier $\overline{k}$ appartient à H_d.

Nous avons donc $d\overline{k} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$; autrement dit dk est multiple de $n = dd'$. Il en résulte que k est multiple de d' ; ainsi $\overline{k}$ appartient à H_d.

1.b) Le groupe H_d est cyclique ; il est d'ordre d donc possède $\varphi(d)$ générateurs. Les générateurs de H_d étant les éléments d'ordre d, H_d possède $\varphi(d)$ éléments d'ordre d.

2. D'après 1. les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont les $\varphi(d)$ éléments d'ordre d de H_d. Le groupe $\mathbb{Z}/n\mathbb{Z}$ compte donc $\varphi(d)$ éléments d'ordre d. En dénombrant les éléments ordre par ordre nous obtenons que $\mathbb{Z}/n\mathbb{Z}$ compte $\sum_{\substack{d|n \\ d>0}} \varphi(d)$, c'est-à-dire $n = \sum_{\substack{d|n \\ d>0}} \varphi(d)$.

Exercice 904

Considérons l'anneau quotient $A = \mathbb{Z}[\mathbf{i}]/3\mathbb{Z}[\mathbf{i}]$.

1. Montrer que A possède 9 éléments.
2. Soit α la classe de $1 + \mathbf{i}$ dans A.
   a) Calculer α^4.
   b) En déduire que α appartient à $A^\times$.
   c) Quel est l'ordre de α dans le groupe $A^\times$?
3. Montrer que A est un corps.
4. Montrer que pour tout élément a de A nous avons $a^9 = a$.
5. Posons $B = \{\overline{0}, \overline{1}, \overline{-1}\} \subset A$. Montrer que B est un sous-corps de A isomorphe à $\mathbb{F}_3$.

Éléments de réponse 904

1. Pour tous $z = a + \mathbf{i}b$ et $z' = a' + \mathbf{i}b'$ appartenant à $\mathbb{Z}[\mathbf{i}]$ nous avons

$$\begin{aligned} z = z' &\iff z - z' \text{ est multiple de 3 dans } \mathbb{Z}[\mathbf{i}] \\ &\iff \exists\, u, v \in \mathbb{Z} \text{ tels que } (a - a') = 3u \text{ et } (b - b') = 3v \\ &\iff a \equiv_3 a' \text{ et } b \equiv_3 b' \end{aligned}$$

Par suite les éléments de A sont les classes des $a+\mathbf{i}b$ où a et b appartiennent à $\{0,\,1,\,-1\}$, c'est-à-dire

$$A=\{\overline{0},\,\overline{1},\,\overline{-1},\,\overline{\mathbf{i}},\,\overline{-\mathbf{i}},\,\overline{1+\mathbf{i}},\,\overline{1-\mathbf{i}},\,\overline{-1+\mathbf{i}},\,\overline{-1-\mathbf{i}}\}$$

2.a) À partir de $(1+\mathbf{i})^2=2\mathbf{i}$ nous obtenons $\alpha^2=\overline{2\mathbf{i}}$ et $\alpha^4=\overline{-4}=\overline{-1}$.

2.b) L'égalité $\alpha^4=\overline{-1}$ implique $\alpha^8=\overline{1}$ c'est-à-dire $\alpha\alpha^7=\alpha^7\alpha=\overline{1}$. Il en résulte que α et α^7 sont inverses l'un de l'autre dans l'anneau A ; en particulier α appartient à $A^\times$.

2.c) L'égalité $\alpha^8=\overline{1}$ assure que l'ordre de α dans $A^\times$ divise 8. Puisque les éléments α, $\alpha^2=\overline{2\mathbf{i}}=\overline{-\mathbf{i}}$ et $\alpha^4=\overline{-1}$ sont différents de $\overline{1}$, α est d'ordre 8.

3. Le sous-groupe de $A^\times$ engendré par α est d'ordre 8 et l'ensemble $A\smallsetminus\{0\}$ compte huit éléments. Il en résulte que $A^\times=A\smallsetminus\{0\}$. Autrement dit l'anneau A est un corps.

4. Pour tout $x\in A^\times$, nous avons $x^8=1$ d'où $x^9=x$. De plus $0^9=0$. Il en résulte que $x^9=x$ quel que soit x dans A.

5. Comme $\overline{3}=\overline{0}$, le sous-groupe additif de A engendré par $\overline{1}$ est

$$\{\overline{0},\,\overline{1},\,\overline{-1}\}$$

Notons que le produit de deux éléments de B est dans B et que $\overline{1}$ appartient à B ; il s'en suit que B est un sous-anneau de A. Les éléments $\overline{1}$ et $\overline{-1}$ étant leur propre inverse, B est un sous-corps de A.

Pour tout $k\in\mathbb{Z}$, notons $\widehat{k}$ la classe de k dans le corps $\mathbb{F}_3$; l'application

$$\varphi\colon\{\widehat{0},\,\widehat{1},\,\widehat{2}\}=\mathbb{F}_3\to B$$

définie par $\varphi(\widehat{k})=\overline{k}$ est un isomorphisme de corps.

3.6. Anneaux principaux, anneaux euclidiens

Exercice 905

1. Le polynôme X^2+X-1 est-il irréductible dans $\mathbb{F}_3[X]$?
2. Le polynôme X^4+2X^2+X+1 est-il irréductible dans $\mathbb{F}_3[X]$?
3. Considérons dans $\mathbb{F}_3[X]$ le polynôme $P=X^4+X-1$. Montrer que P n'a pas de diviseur de degré 2. En déduire que P est irréductible dans $\mathbb{F}_3[X]$.
4. Le polynôme X^4-2X+5 est-il irréductible dans $\mathbb{Q}[X]$?

Éléments de réponse 905

1. Le polynôme X^2+X-1 est de degré 2. Notons qu'aucun élément de $\mathbb{F}_3=\{0,\,1,\,-1\}$ n'est racine de P. Il en résulte que P est un polynôme irréductible de $\mathbb{F}_3[X]$.
2. Le polynôme $X^4+2X^2+X+1\in\mathbb{F}_3[X]$ a pour racine -1 ; il n'est donc pas irréductible dans $\mathbb{F}_3[X]$.

3. Supposons que $U \in \mathbb{F}_3[X]$ soit un diviseur de degré 2 de P. Nous pouvons supposer U unitaire, écrivons donc U sous la forme $X^2 + aX + b$ où a, b désignent deux éléments de $\mathbb{F}_3$. Comme P est unitaire, il existe un polynôme unitaire $V = X^2 + cX + d$ où c, $d \in \mathbb{F}_3$, tel que $P = UV$. Cette égalité se traduit par

$$\begin{cases} a + c = 0 \\ b + d + ac = 0 \\ ad + bc = 1 \\ bd = -1 \end{cases} \tag{3.6.1}$$

Puisque les éléments b et d de $\mathbb{F}_3$ satisfont $bd = -1$ nous obtenons $(b, d) = (1, -1)$ ou $(b, d) = (-1, 1)$. En particulier, $b + d = 0$; la seconde équation de (3.6.1) se réécrit donc $ac = 0$, ce qui conduit à $a = 0$ ou $c = 0$. Mais alors la première équation de (3.6.1) entraîne $a = c = 0$ et la troisième équation de (3.6.1) se réécrit $0 = 1$: contradiction. Il en résulte que P n'a pas de diviseur de degré 2. Étant donné que P n'a pas de racine dans $\mathbb{F}_3$ il n'a pas non plus de diviseur de degré 1. Finalement P est irréductible dans $\mathbb{F}_3[X]$.

4. Le polynôme $X^4 - 2X + 5$ est unitaire et à coefficients entiers. Sa réduction modulo 3 est le polynôme $X^4 + X - 1 \in \mathbb{F}_3[X]$ qui est irréductible d'après 3. Il en résulte que $X^4 - 2X + 5$ est un polynôme irréductible de $\mathbb{Q}[X]$.

Exercice 906

1. Quelle est la décomposition de $X^3 - 2X + 1$ en produit d'irréductibles dans $\mathbb{F}_5[X]$?
2. Quelle est la décomposition de $X^{15} - 2X^5 + 1$ en produit d'irréductibles dans $\mathbb{F}_5[X]$?
3. Quelle est la décomposition de $3X^5 - 1$ en produit d'irréductibles dans $\mathbb{F}_5[X]$?

Éléments de réponse 906

1. Le polynôme $P = X^3 - 2X + 1 \in \mathbb{F}_5[X]$ a pour racine 1. Ainsi $P = (X - 1)(X^2 + X - 1)$; remarquons que 2 est racine de $X^2 + X - 1$. Il en résulte que $X^2 + X - 1 = (X - 2)R$ où $R \in \mathbb{F}_5[X]$ est de degré 1. Écrivons R sous la forme $aX + b$. Alors

$$X^2 + X - 1 = (X - 2)(aX + b) \iff X^2 + X - 1 = aX^2 + (b - 2a)X - 2b$$
$$\iff a \equiv_5 1,\ b - 2a \equiv_5 1,\ -2b \equiv_5 -1 \iff a \equiv_5 1,\ b - 2a \equiv_5 1,\ -2b \equiv_5 4 \iff a \equiv_5 1,\ b \equiv_5 -2.$$

Finalement la décomposition de P en facteurs irréductibles dans $\mathbb{F}_5[X]$ est

$$P = (X - 1)(X - 2)(X - 2) = (X - 1)(X - 2)^2.$$

2. La décomposition de $X^{15} - 2X^5 + 1$ en facteurs irréductibles dans $\mathbb{F}_5[X]$ est :

$$X^{15} - 2X^5 + 1 = (X^3 - 2X + 1)^5 = \left((X - 1)(X - 2)^2\right)^5 = (X - 1)^5(X - 2)^{10}.$$

3. Puisque $3X^5 - 1 = 3X^5 - 6 = 3(X^5 - 2) = 3(X - 2)^5$ la décomposition de $3X^5 - 1$ dans $\mathbb{F}_5[X]$ est $3(X - 2)^5$.

Exercice 907

Soit z dans $\mathbb{Z}[\mathbf{i}]$. Montrer que si z et $\overline{z}$ sont associés, alors

- ◇ ou bien z appartient à $\mathbb{Z}$,
- ◇ ou bien z appartient à $\mathbf{i}\mathbb{Z}$,
- ◇ ou bien z s'écrit $n(1 \pm \mathbf{i})$ où n désigne un élément de $\mathbb{Z}$.

Éléments de réponse 907

Les inversibles de $\mathbb{Z}[\mathbf{i}]$ sont ± 1 et $\pm\mathbf{i}$. Par suite z et $\overline{z}$ sont associés si et seulement si $z = \overline{z}$ ou $z = -\overline{z}$ ou $z = \mathbf{i}z$ ou $z = -\mathbf{i}z$. Or

- ◇ $z = \overline{z}$ veut dire que z est réel donc z appartient à $\mathbb{Z}$;
- ◇ $z = -\overline{z}$ signifie que z est imaginaire, donc que z appartient à $\mathbf{i}\mathbb{Z}$;
- ◇ posons $z = a + \mathbf{i}b$, alors

$$z = \mathbf{i}\overline{z} \Longleftrightarrow a + \mathbf{i}b = \mathbf{i}(a - \mathbf{i}b) \Longleftrightarrow b = a \Longleftrightarrow z = a(1 + \mathbf{i}).$$

- ◇ posons $z = a + \mathbf{i}b$, alors

$$z = -\mathbf{i}\overline{z} \Longleftrightarrow a + \mathbf{i}b = -\mathbf{i}(a - \mathbf{i}b) \Longleftrightarrow b = -a \Longleftrightarrow z = a(1 - \mathbf{i}).$$

Exercice 908

1. Dans l'anneau $\mathbb{Z}[\mathbf{i}]$ posons $a = 1 + \mathbf{i}$ et $b = 2$. Montrer que nous pouvons choisir $q = 0$, 1 ou $\mathbf{i}$ comme quotient dans la division euclidienne de a par b.
2. Calculer $\operatorname{pgcd}(7 - \mathbf{i}, 10)$ dans $\mathbb{Z}[\mathbf{i}]$.

Éléments de réponse 908

1. Nous désignons par N la norme sur $\mathbb{Z}[\mathbf{i}]$, *i.e.* $N(a+\mathbf{i}b) = a^2 + b^2$. Nous avons les divisions euclidiennes

$$\begin{aligned} &1 + \mathbf{i} = 2 \times 0 + (1 + \mathbf{i}), && N(1 + \mathbf{i}) = 2 < N(2) = 4, \\ &1 + \mathbf{i} = 2 \times 1 + (-1 + \mathbf{i}), && N(-1 + \mathbf{i}) = 2 < N(2) = 4 \\ &1 + \mathbf{i} = 2 \times \mathbf{i} + (1 - \mathbf{i}), && N(1 - \mathbf{i}) = 2 < N(2) = 4. \end{aligned}$$

2. Nous avons les divisions euclidiennes

$$7 - \mathbf{i} = 10 \times -3 - \mathbf{i}, \qquad 10 = (-3 - \mathbf{i})(-3 + \mathbf{i}) + 0;$$

par conséquent $\operatorname{pgcd}(7 - \mathbf{i}, 10) = 3 + \mathbf{i}$.

Exercice 909 Considérons l'anneau $A = \mathbb{Z}[\mathbf{i}\sqrt{5}]$.

1. Montrer que 2, 3 et $\sqrt{5}$ sont irréductibles dans A.

2. Montrer que dans A nous avons $2 \times 3 = (1 + \mathbf{i}\sqrt{5})(1 - \mathbf{i}\sqrt{5})$. En déduire que l'anneau A n'est pas principal.
3. Soit $x = a + b\mathbf{i}\sqrt{5}$ un élément de A. Montrer que x est multiple de $\mathbf{i}\sqrt{5}$ si et seulement si a est multiple de 5.
4. Soient x et y dans A. Montrer que si $\mathbf{i}\sqrt{5}$ divise xy, alors $\mathbf{i}\sqrt{5}$ divise x ou y.

Éléments de réponse 909

1. Commençons par rappeler

Soit A un anneau intègre. Un élément $a \neq 0$ appartenant à A est *irréductible* si a n'est pas inversible et si pour tous u, $v \in A$ nous avons l'implication $a = uv \Longrightarrow u$ ou v est inversible

Nous désignons par N la norme sur $\mathbb{Z}[\mathbf{i}\sqrt{5}]$, *i.e.* $N(a + \mathbf{i}\sqrt{5}b) = a^2 + 5b^2$.

Supposons que 2 s'écrive uv où u et v désignent deux éléments de A. Alors $4 = N(2) = N(uv) = N(u)N(v)$. Puisque $N(u)$ et $N(v)$ sont des entiers positifs, ou bien l'un des entiers $N(u)$ ou $N(v)$ vaut 1, ou bien $N(u) = N(v) = 2$. Mais il n'existe pas d'entiers a et b tels que $a^2 + 5b^2 = 2$, autrement dit il n'y a pas d'élément de norme 2 dans A. Ainsi u ou v est de norme 1 et u ou v est inversible. De plus, 2 n'est pas inversible dans A. Finalement 2 est irréductible dans A.

Supposons 3 s'écrive uv où u et v désignent deux éléments de A. Alors $9 = N(3) = N(uv) = N(u)N(v)$. Puisque $N(u)$ et $N(v)$ sont des entiers positifs, ou bien l'un des entiers $N(u)$ ou $N(v)$ vaut 1, ou bien $N(u) = N(v) = 3$. Mais il n'existe pas d'entiers a et b tels que $a^2 + 5b^2 = 3$, autrement dit il n'y a pas d'élément de norme 3 dans A. Ainsi u ou v est de norme 1 et u ou v est inversible. De plus, 3 n'est pas inversible dans A. Finalement 3 est irréductible dans A.

Comme $N(\sqrt{5}) = 5$ est un nombre premier, $\sqrt{5}$ est irréductible dans A.

2. Dans A nous avons $2 \times 3 = (1 + \mathbf{i}\sqrt{5})(1 - \mathbf{i}\sqrt{5})$. Si A était principal, l'élément irréductible 2 diviserait $(1 + \mathbf{i}\sqrt{5})$ ou $(1 - \mathbf{i}\sqrt{5})$ ce qui est impossible car dans A, les multiples de 2 sont les éléments $a + \mathbf{i}\sqrt{5}$ tels que a et b sont pairs.
3. Nous avons : x est multiple de $\mathbf{i}\sqrt{5}$ si et seulement s'il existe n, $m \in \mathbb{Z}$ tels que
$$a + b\mathbf{i}\sqrt{5} = \mathbf{i}\sqrt{5}(n + m\mathbf{i}\sqrt{5}) = -5m + n\mathbf{i}\sqrt{5},$$
i.e. si et seulement si a est multiple de 5.
4. Écrivons x sous la forme $a + b\mathbf{i}\sqrt{5}$ et y sous la forme $c + d\mathbf{i}\sqrt{5}$. Alors $xy = (ac - 5bd) + (ad + bc)\mathbf{i}\sqrt{5}$. D'après 3. xy s'écrit aussi $-5m + n\mathbf{i}\sqrt{5}$. En particulier 5 divise $ac - 5bd$; il s'en suit que 5 divise ac. Puisque 5 est un nombre premier, le Théorème de Gauss assure que 5 divise a ou c. Si par exemple 5 divise a alors 3. assure que $\mathbf{i}\sqrt{5}$ divise x.

Exercice 910

Soit $\mathbf{j}$ le nombre complexe $-\frac{1}{2}+\frac{\mathbf{i}\sqrt{3}}{2}$. Soit $\mathbb{Z}[\mathbf{j}]=\{x+\mathbf{j}y \,|\, x,\, y\in\mathbb{Z}\}$. Pour tout $z\in\mathbb{Z}[\mathbf{j}]$, nous posons $N(z)=z\overline{z}$.

1. Montrer que pour tous entiers x, x', y, y' nous avons
$$x+\mathbf{j}y=x'+\mathbf{j}y' \quad\Longleftrightarrow\quad (x=x' \text{ et } y=y').$$

2.a) Montrer que $\mathbf{Z}[\mathbf{j}]$ est un sous-anneau de $\mathbb{C}$.

2.b) Montrer que $\mathbb{Z}[\mathbf{i}\sqrt{3}]$ est un sous-anneau de $\mathbb{C}$.

3.a) Montrer que pour tous z, z' dans $\mathbb{Z}[\mathbf{j}]$ nous avons $N(zz')=N(z)N(z')$.

3.b) Calculer $N(a+\mathbf{j}b)$ pour tous a, $b\in\mathbb{Z}$.

4. Montrer que l'anneau $\mathbb{Z}[\mathbf{j}]$ est euclidien (utiliser $N\colon \mathbb{Z}[\mathbf{j}]\to\mathbb{N}$ et raisonner comme pour l'anneau $\mathbb{Z}[\mathbf{i}]$).

5. Trouver deux irréductibles dans $\mathbb{Z}[\mathbf{j}]$ de normes différentes.

6. Déterminer les éléments inversibles de $\mathbb{Z}[\mathbf{j}]$.

7. Posons $\alpha=1-\mathbf{j}$ et $A={}^{\mathbb{Z}[\mathbf{j}]}\!/_{\alpha\mathbb{Z}[\mathbf{j}]}$. Soit $p\colon \mathbb{Z}[\mathbf{j}]\to A$ la projection canonique.

7.a) Montrer que 3 et α^2 sont associés et que pour tous a, $b\in\mathbb{Z}$ nous avons $p(a+b)=p(a+\mathbf{j}b)$.

7.b) Montrer qu'il existe un isomorphisme d'anneaux ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\to A$. En déduire que A est un corps isomorphe à $\mathbb{F}_3$.

Éléments de réponse 910

1. Comme $(1,\mathbf{j})$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$, pour tous entiers x, x', y, y' nous avons
$$x+\mathbf{j}y=x'+\mathbf{j}y' \quad\Longleftrightarrow\quad (x=x' \text{ et } y=y').$$

2.a) Soient $z=a+\mathbf{j}b$ et $z'=a'+\mathbf{j}b'$ des éléments de $\mathbb{Z}[\mathbf{j}]$. Nous avons :
$$z+z'\in\mathbb{Z}[\mathbf{j}], \qquad -z\in\mathbb{Z}[\mathbf{j}], \qquad 0\in\mathbb{Z}[\mathbf{j}].$$
Par suite $\mathbb{Z}[\mathbf{j}]$ est un sous-groupe additif de $\mathbb{C}$. De plus 1 appartient à $\mathbb{Z}[\mathbf{j}]$ et
$$zz'=(a+\mathbf{j}b)(a'+\mathbf{j}b')=aa'+bb'\mathbf{j}^2+(ab'+a'b)\mathbf{j}=aa'+bb'(-1-\mathbf{j})+(ab'+a'b)\mathbf{j}=(aa'-bb')+\mathbf{j}(ab'+a'b-bb')$$
car $\mathbf{j}^2=-1-\mathbf{j}$. Ainsi zz' appartient à $\mathbb{Z}[\mathbf{j}]$. Finalement $\mathbb{Z}[\mathbf{j}]$ est un sous-anneau de $\mathbb{C}$.

2.b) De même nous montrons que $\mathbb{Z}[\mathbf{i}\sqrt{3}]$ est un sous-anneau de $\mathbb{C}$.

3.a) Soient z, z' deux éléments de $\mathbb{Z}[\mathbf{j}]$; nous avons
$$N(zz')=(zz')(\overline{zz'})=z\,z'\,\overline{z}\,\overline{z'}=z\,\overline{z}\,z'\,\overline{z'}=N(z)N(z').$$

3.b) Pour tous a, b dans $\mathbb{Z}$ nous avons

$$N(a+b\mathbf{j}) = (a+b\mathbf{j})(a+b\bar{\mathbf{j}}) = a^2 + ab\mathbf{j} + ab\bar{\mathbf{j}} + b^2\mathbf{j}\bar{\mathbf{j}} = a^2 + ab(\mathbf{j}+\bar{\mathbf{j}}) + b^2|\mathbf{j}|^2 = a^2 - ab + b^2$$

car $\mathbf{j}+\bar{\mathbf{j}} = -1$ et $|\mathbf{j}| = 1$. Pour tout élément $a+b\mathbf{j} \in \mathbb{Z}[\mathbf{j}]$ nous avons donc

$$N(a+b\mathbf{j}) = a^2 - ab + b^2.$$

4. Commençons par remarquer que N est à valeurs dans $\mathbb{N}$. Soient a, b dans $\mathbb{Z}$, alors $(a-b)^2 \geq 0$, *i.e.* $-ab \geq -\frac{a^2+b^2}{2}$. Ainsi $N(a+b\mathbf{j}) = a^2 - ab + b^2 \geq a^2 + b^2 - \frac{a^2+b^2}{2} = \frac{a^2+b^2}{2} \geq 0$.

Soient γ et δ deux éléments de $\mathbb{Z}[\mathbf{j}]$. Supposons que δ soit non nul et posons $\frac{\gamma}{\delta} = \frac{\gamma\bar{\delta}}{\delta\bar{\delta}} = \frac{\gamma\bar{\delta}}{N(\delta)} = x + y\mathbf{j}$ où x et y désignent deux éléments de $\mathbb{Q}$. Soit n l'entier le plus proche de x et soit m l'entier le plus proche de y. Par conséquent $|x-n| \leq \frac{1}{2}$ et $|y-m| \leq \frac{1}{2}$. Posons $q = n + mj$. Nous avons $q \in \mathbb{Z}[\mathbf{j}]$ et $\gamma = \delta q + r$ où

$$r = \delta\left(\frac{\gamma}{\delta} - q\right) = \delta\Big(x - n + (y-m)\mathbf{j}\Big).$$

D'après le choix de n et m nous avons

$$\begin{aligned} |x-n+\mathbf{j}(y-m)|^2 &= (x-n)^2 - (x-n)(y-m) + (y-m)^2 \\ &= |x-n|^2 + |x-n|\,|y-m| + |y-m|^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1. \end{aligned}$$

Ainsi $N(r) = N(\delta)\Big|x - n + (y-m)\mathbf{j}\Big|^2 < N(\delta)$ car $N(\delta) > 0$. Cela définit une division euclidienne $a = bq + r$ dans l'anneau $\mathbb{Z}[\mathbf{j}]$.

5. Il suffit de trouver deux éléments de $\mathbb{Z}[\mathbf{j}]$ dont la norme est un nombre premier. Par exemple

$$2^2 - 2\times 3 + 3^2 = 7 \qquad \text{et} \qquad 6^2 - 6\times 1 + 1^2 = 31$$

d'où $2+3\mathbf{j}$ et $6+\mathbf{j}$ sont des éléments irréductibles de $\mathbb{Z}[\mathbf{j}]$.

6. Les inversibles de $\mathbb{Z}[\mathbf{j}]$ sont les éléments de norme ± 1. Mais ici la norme est à valeurs dans $\mathbb{N}$ (cf. 4.) ; les inversibles de $\mathbb{Z}[\mathbf{j}]$ sont donc les éléments de norme 1, c'est-à-dire les $a+\mathbf{j}b$, avec a, $b \in \mathbb{Z}$ et $a^2 - ab + b^2 = 1$. Puisque $(a-b)^2 \geq 0$, nous avons $ab \leq \frac{a^2+b^2}{2}$ et

$$1 = a^2 - ab + b^2 \geq a^2 - \frac{a^2+b^2}{2} + b^2 = \frac{a^2+b^2}{2}$$

donc $a^2 + b^2 \leq 2$. Il en résulte que a et b appartiennent à l'ensemble $\{-1, 0, 1\}$. Nous avons les solutions $(a = \pm 1,\ b = 0)$ et $(a = 0,\ b = \pm 1)$ qui donnent les inversibles 1, -1, $\mathbf{j}$ et $-\mathbf{j}$. Finalement le groupe des inversibles de $\mathbb{Z}[\mathbf{j}]$ est

$$\big(\mathbb{Z}[\mathbf{j}]\big)^\times = \{1, -1, \mathbf{j}, -\mathbf{j}, 1+\mathbf{j}, -1-\mathbf{j}\}.$$

7.a) Nous avons $\alpha^2 = (1 - 2\mathbf{j} + \mathbf{j}^2) = -3\mathbf{j}$. Comme $-\mathbf{j}$ est inversible, 3 et α^2 sont associés.

Pour tous a, $b \in \mathbb{Z}$ nous avons $(a+b)-(a+b\mathbf{j}) = b\alpha$ appartient à $\alpha\mathbb{Z}[\mathbf{j}]$, d'où $p(a+b) = p(a+\mathbf{j}b)$.

7.b) Considérons le morphisme d'anneaux restriction de p à $\mathbb{Z}$:

$$f = p_{|\mathbb{Z}} \colon \mathbb{Z} \to A.$$

D'après la question précédente α divise 3 dans $\mathbb{Z}[\mathbf{j}]$; ainsi $f(3) = 0$. Nous en déduisons que f définit un morphisme d'anneaux $\widetilde{f} \colon \mathbb{Z}/3\mathbb{Z} \to A$ tel que $\widetilde{f}(\overline{k}) = f(k)$ pour tout $\overline{k} \in \mathbb{Z}/3\mathbb{Z}$. Comme $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ est un corps, $\widetilde{f}$ est injectif [4].

Montrons que f est surjectif. En effet, si $\beta = p(a + \mathbf{j}b)$ est un élément de A, alors $p(a+b) = p(a+\mathbf{j}b)$ d'où $f(a+b) = p(a+b) = \beta$. Nous en déduisons que $\widetilde{f}$ est surjectif et donc que $\widetilde{f}$ est un isomorphisme d'anneaux. Étant donné que $\mathbb{F}_3$ est un corps, l'anneau A est un corps.

Exercice 911

Considérons l'équation $(\star)$ $y^2 + 2 = z^3$, $(y, z) \in \mathbb{Z} \times \mathbb{Z}$.
Posons $A = \mathbb{Z}[\mathbf{i}\sqrt{2}]$.

1. Soit (y, z) une solution de $(\star)$. Montrer que y est impair et que $\mathbf{i}\sqrt{2}$ est irréductible dans A.
2. Soit (y, z) une solution de $(\star)$. Soit $\alpha \in A$ un diviseur irréductible commun à $y + \mathbf{i}\sqrt{2}$ et $y - \mathbf{i}\sqrt{2}$.

2.a) Montrer que α divise $2\mathbf{i}\sqrt{2}$.

2.b) Montrer que α est associé à $\mathbf{i}\sqrt{2}$.

3. Soit (y, z) une solution de $(\star)$. Déduire de ce qui précède que $y + \mathbf{i}\sqrt{2}$ et $y - \mathbf{i}\sqrt{2}$ sont premiers entre eux.

4.a) Soit (y, z) une solution de $(\star)$. Montrer qu'il existe a, b dans $\mathbb{Z}$ tels que $y + \mathbf{i}\sqrt{2} = (a + b\mathbf{i}\sqrt{2})^3$.

4.b) Soit (y, z) une solution de $(\star)$. Montrer que $a = \pm 1$ et $b = 1$.

5. Résoudre l'équation $(\star)$.

Éléments de réponse 911

Rappelons que $A = \mathbb{Z}[\mathbf{i}\sqrt{2}]$ est un anneau principal.

---

4. Soient $\Bbbk$ un corps et A un anneau. Soit $f \colon \Bbbk \to A$ un morphisme d'anneaux ; alors f est injectif. En effet, soit x dans $\Bbbk$; nous avons l'alternative :

- ou bien $x = 0$ et $f(x) = 0$;
- ou bien $x \neq 0$ auquel cas $\Bbbk$ étant un corps x est inversible, *i.e.* il existe x^{-1} dans $\Bbbk$ tel que $xx^{-1} = 1$. Nous en déduisons que $f(xx^{-1}) = f(1)$ ou encore que $f(x)f(x^{-1}) = 1$; en particulier $f(x) = 0$.

Elle conduit à $\ker f = \{0\}$, c'est-à-dire f est injective.

1. Soit (y,z) une solution de $(\star)$. Supposons que y est pair. Alors z est pair, 4 divise y^2 et 4 divise z^3. Il s'en suit que 4 divise z^3-y^2 ce qui est impossible puisque $z^3-y^2=2$. Finalement y est impair.

   Nous constatons que $N(\mathbf{i}\sqrt{2})=2$; puisque 2 est premier nous en déduisons que $\mathbf{i}\sqrt{2}$ est irréductible dans A.

2. Soit (y,z) une solution de $(\star)$.

2.a) Puisque α divise $y+\mathbf{i}\sqrt{2}$ et $y-\mathbf{i}\sqrt{2}$, α divise $(y+\mathbf{i}\sqrt{2})-(y-\mathbf{i}\sqrt{2})=2\mathbf{i}\sqrt{2}$. Notons que $2\mathbf{i}\sqrt{2}=-(\mathbf{i}\sqrt{2})^3$; il s'en suit que l'irréductible α divise $\mathbf{i}\sqrt{2}$.

2.b) Étant donné que $\mathbf{i}\sqrt{2}$ est irréductible, nous obtenons que α est associé à $\mathbf{i}\sqrt{2}$.

3. Soit (y,z) une solution de $(\star)$. Supposons que $y+\mathbf{i}\sqrt{2}$ et $y-\mathbf{i}\sqrt{2}$ ne soient pas premiers entre eux. Il existe donc un irréductible α qui divise ces deux éléments. D'après 2. α est associé à $\mathbf{i}\sqrt{2}$. Il s'en suit que $\mathbf{i}\sqrt{2}$ divise $y+\mathbf{i}\sqrt{2}$ et que $\mathbf{i}\sqrt{2}$ divise y. Autrement dit il existe des entiers n et m tels que $y=\mathbf{i}\sqrt{2}(n+m\mathbf{i}\sqrt{2})$ ce qui se réécrit $y=-2m+n\mathbf{i}\sqrt{2}$. Nous en déduisons que $y=-2m$ (rappelons que y appartient à $\mathbb{Z}$) : contraction avec le fait que y est impair (d'après 1.)

4.a) Soit (y,z) une solution de $(\star)$. Rappelons l'énoncé suivant :

> Soit A un anneau principal. Soient a, b, $c\in A$ des éléments non nuls et non inversibles tels que $ab=c^n$ avec $n\geq 1$. Si a et b sont premiers entre eux, il existe α, β des éléments de A et ε, $\varepsilon'\in A^*$ des inversibles tels que $a=\varepsilon\alpha^n$ et $b=\varepsilon'\beta^n$.

   Nous avons : $(y+\mathbf{i}\sqrt{2})(y-\mathbf{i}\sqrt{2})=y^2+2=z^3$. Puisque $y+\mathbf{i}\sqrt{2}$ et $y-\mathbf{i}\sqrt{2}$ sont premiers entre eux, chacun de ces éléments est associé au cube d'un élément de A (cf Rappel). Les inversibles de A étant ± 1, ce sont des cubes ; ainsi il existe a, $b\in\mathbb{Z}$ tels que $y+\mathbf{i}\sqrt{2}=(a+b\mathbf{i}\sqrt{2})^3$.

4.b) Soit (y,z) une solution de $(\star)$. D'après 4.a) il vient

$$y+\mathbf{i}\sqrt{2}=a^3+3a^2b\mathbf{i}\sqrt{2}-6ab^2-2b^3\mathbf{i}\sqrt{2}=a(a^2-6b^2)+b(3a^2-2b^2)\mathbf{i}\sqrt{2}.$$

   Il en résulte que

$$y=a(a^2-6b^2),\qquad\qquad 1=b(3a^2-2b^2).$$

   Cette dernière égalité implique $b=\pm 1$ et $3a^2-2b^2=3a^2-2=\pm 1$. Comme $3a^2\neq 1$, nous en déduisons que $3a^2-2=1$, *i.e.* $a=\pm 1$ et $b=1$.

5. Si (y,z) est solution de $(\star)$, alors y s'écrit $a(a^2-6b^2)$ avec $a=\pm 1$ et $b=1$. Par conséquent $y=\pm 5$. Par suite $z^3=5^2+2$ et $z=3$. Les solutions de $(\star)$ sont les couples $(5,3)$ et $(-5,3)$.

Exercice 912

1. Effectuer la division de X^2+3 par $X+1$.
2. Effectuer la division de X^5+X^2+3 par $-X^3+1$.
3. Effectuer la division de X^2+3 par X^3+1.
4. Effectuer dans $\mathbb{Z}[X]$ la division de X^2+3 par $2X+1$.

Éléments de réponse 912

1. Effectuons la division de X^2+3 par $X+1$:
$$X^2+3=(X+1)(X-1)+4.$$
2. Effectuons la division de X^5+X^2+3 par $-X^3+1$:
$$X^5+X^2+3=(-X^2)\cdot(-X^3+1)+(2X^2+3).$$
3. Effectuons la division de X^2+3 par X^3+1 :
$$X^2+3=0\cdot(X^3+1)+(X^2+3).$$
4. Nous ne pouvons pas effectuer dans $\mathbb{Z}[X]$ la division de X^2+3 par $2X+1$ car 2 n'est pas inversible dans $\mathbb{Z}$.

Exercice 913

1. Soient A un anneau intègre, $P\in A[X]$ et a_1, a_2, …, $a_k\in A$ des éléments distincts. Si $P(a_i)=0$ pour tout i, alors le produit $(X-a_1)(X-a_2)\dots(X-a_k)$ divise P.
2. Un polynôme non nul de degré n sur un anneau intègre A admet au plus n racines.
3. Donner un polynôme de degré n sur un anneau non intègre ayant plus de n racines.

Éléments de réponse 913

1. Soient A un anneau intègre, $P\in A[X]$ et a_1, a_2, …, $a_k\in A$ des éléments distincts. Supposons que $P(a_i)=0$ pour tout i, montrons par récurrence sur $k\geq 1$ que le produit $(X-a_1)(X-a_2)\dots(X-a_n)$ divise P.
   - ◇ Pour $k=1$ effectuons la division euclidienne de P par $X-a_1$: $P=Q(X-a_1)+R$ où R est un polynôme de degré au plus 0 c'est-à-dire une constante. En évaluant cette expression au point $X=a_1$ nous obtenons $0=P(a_1)=R$; nous avons donc bien : $X-a_1$ divise P.
   - ◇ Supposons maintenant l'hypothèse vraie au rang $k-1$ et supposons que $P(a_i)=0$ pour tout $i\leq k$. Par hypothèse de récurrence
   $$P=(X-a_1)(X-a_2)\dots(X-a_{k-1})Q.$$
   En évaluant cette expression au point $X=a_k$ nous obtenons $0=P(a_k)=(a_k-a_1)(a_k-a_2)\dots(a_k-a_{k-1})Q(a_k)$. Étant donnés que A est un anneau intègre et que

les $a_k - a_i$ sont non nuls (car les a_i sont tous distincts) nous obtenons que $Q(a_k) = 0$; autrement dit $X - a_k$ divise Q, c'est-à-dire $Q = (X - a_k)R$. Finalement P s'écrit

$$P = (X - a_1)(X - a_2)\dots(X - a_{k-1})(X - a_k)R.$$

2. Un polynôme non nul de degré n sur un anneau intègre A admet au plus n racines.

   Raisonnons par l'absurde : supposons qu'il existe un polynôme P de degré n admettant $n+1$ racines distinctes $a_1, a_2, \dots, a_{n+1}$. D'après la question qui précède nous avons l'égalité

$$P = (X - a_1)(X - a_2)\dots(X - a_n)(X - a_{n+1})R. \tag{3.6.2}$$

   Le terme de gauche dans (3.6.2) est de degré n, alors que le terme de droite dans (3.6.2) est de degré $\geq n + 1$: contradiction.

3. Donnons un polynôme de degré n sur un anneau non intègre ayant plus de n racines. Considérons l'anneau $A = \mathbb{Z}/4\mathbb{Z}[X]$ et le polynôme non nul $P = \overline{2}X$. Remarquons que P est de degré 1 et que P admet les deux racines distinctes suivantes :

$$P(\overline{2}) = \overline{2} \times \overline{2} = \overline{4} = \overline{0}, \qquad P(\overline{0}) = \overline{0}.$$

Exercice 914

1. Dans la liste suivante quels sont les polynômes inversibles sur $\mathbb{Q}[X]$: $1+3X+X^2$, $5+X$, 4 ?
2. Dans la liste suivante suels sont les polynômes inversibles sur $\mathbb{Z}[X]$: $1+3X+X^2$, $5+X$, 4 ?

Éléments de réponse 914

1. Dans la liste de polynômes sur $\mathbb{Q}[X]$: $1+3X+X^2$, $5+X$, 4, seul 4 est inversible (d'inverse $\frac{1}{4}$).
2. Dans la liste de polynômes sur $\mathbb{Z}[X]$: $1 + 3X + X^2$, $5 + X$, 4, aucun n'est inversible. En effet, les éléments inversibles de $\mathbb{Z}[X]$ sont les constantes 1 et -1.

Exercice 915

1. La conjugaison complexe $\mathbb{C} \to \mathbb{C}$, $z = a+\mathbf{i}b \mapsto \overline{z} = a-\mathbf{i}b$ est-elle un morphisme d'anneaux ?
2. Montrer que si $P \in \mathbb{R}[X]$ admet une racine a, alors le conjugué $\overline{a}$ de a est aussi une racine de P.
3. Montrer que $P = (X - a)(X - \overline{a})$ est un polynôme réel.

Éléments de réponse 915

1. La conjugaison complexe $\mathbb{C} \to \mathbb{C}$, $z = a + \mathbf{i}b \mapsto \overline{z} = a - \mathbf{i}b$ est un morphisme d'anneaux ; en effet $\overline{1} = 1$ et pour tous z_1, z_2 nous avons
$$\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}, \qquad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$
2. Montrons que si $P \in \mathbb{R}[X]$ admet une racine a, alors le conjugué $\overline{a}$ vérifie lui aussi $P(\overline{a}) = 0$.
   Soit $P = \sum a_i X^i$. Nous avons
$$0 = P(a) = \overline{P(a)} = \overline{\sum a_i a^i} \overset{cf1.}{=} \sum \overline{a_i}\,\overline{a}^i \overset{a_i \in \mathbb{R}}{=} \sum a_i\,\overline{a}^i = P(\overline{a})$$
3. Montrons que $P = (X - a)(X - \overline{a})$ est un polynôme réel.
   Le polynôme conjugué de P est $\overline{P} = (X - \overline{a})(X - a)$; en effet $\overline{P}$ est obtenu à partir de P en changeant tous les coefficients par leur conjugué. Puisque $P = \overline{P}$ nous obtenons que P est réel.
   Autre rédaction possible : $P = (X - a)(X - \overline{a}) = X^2 - 2\mathrm{Re}(a)X + |a|^2$; les coefficients de P sont réels donc P est un polynôme réel et $P = \overline{P}$.

Exercice 916

1. Calculer une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{C}$.
2. Calculer une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{R}$.

Éléments de réponse 916

1. Calculons une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{C}$.
   Si nous multiplions P par $X - 1$, nous trouvons $(X - 1)P = X^5 - X = X(X^4 - 1)$. Les racines de ce polynôme sont 0 et les racines 4ièmes de l'unité, *i.e.* les racines de ce polynôme sont 0, 1, -1, $\mathbf{i}$ et $-\mathbf{i}$. Ainsi
$$(X - 1)P = X(X - 1)(X + 1)(X - \mathbf{i})(X + \mathbf{i})$$
   Comme nous sommes dans un anneau intègre, nous pouvons simplifier par $X - 1$; nous obtenons alors
$$P = X(X + 1)(X - \mathbf{i})(X + \mathbf{i})$$
   qui est la décomposition voulue.
2. Calculons une décomposition du polynôme $P = X + X^2 + X^3 + X^4$ en produit d'irréductibles sur $\mathbb{R}$.
   Pour obtenir la décomposition dans $\mathbb{R}$ il faut regrouper les termes deux par deux avec leur conjugué, ici $X - \mathbf{i}$ et $X + \mathbf{i}$ dont le produit vaut $X^2 + 1$. La décomposition sur $\mathbb{R}$ est donc $P = X(X + 1)(X^2 + 1)$.

Exercice 917

Soit $P \in \mathbb{Z}[X]$ un polynôme de degré au plus un. Discuter l'irréductibilité de ce polynôme.

Éléments de réponse 917

Si P est nul, alors il n'est pas irréductible.

Si P est une constante non nulle, alors P est irréductible si et seulement si p est un nombre premier.

Il ne reste qu'à considérer le cas où $P = aX + b$ est de degré 1. Si a et b ne sont pas premiers entre eux et ont un pgcd non trivial d, la décomposition $P = d\left(\frac{a}{d}X + \frac{b}{d}\right)$ montre que P n'est pas irréductible. Si a et b sont premiers entre eux, montrons que P est irréductible. Soit $P = QR$ une décomposition. Puisque P est de degré 1, il faut que Q et R soient de degré 0 et 1, par exemple Q est de degré 0 et R est de degré 1. Par suite Q est une constante c. Nous obtenons donc $aX + b = c(dX + e)$ ce qui montre que c divise à la fois a et b ; il en résulte que c vaut ± 1 (rappelons que $\text{pgcd}(a, b) = 1$). Par conséquent Q est inversible dans $\mathbb{Z}[X]$; toute décomposition de P contient donc un facteur inversible ce qui prouve que Q est irréductible.

Exercice 918

1. Soit $\Bbbk$ un corps. Si P est un pgcd des P_i dans $\Bbbk[X]$, quels sont les autres pgcd des P_i ?
2. Calculer $\text{pgcd}(5X^2 + 3, X^3 + X)$.

Éléments de réponse 918

1. Soit $\Bbbk$ un corps. Soit P un pgcd des P_i dans $\Bbbk[X]$. Un pgcd est défini à inversible près et les inversibles de $\Bbbk[X]$ sont les constantes non nulles. Les pgcd possibles sont donc les polynômes cP où $c \in \Bbbk$ est une constante non nulle.
2. Déterminons $\text{pgcd}(5X^2+3, X^3+X)$. Nous procédons comme avec les entiers. Nous faisons une suite de divisions donnée par l'algorithme d'Euclide et le pgcd est le dernier reste non nul. Ici :
$$X^3 + X = \frac{1}{5}X(5X^2 + 3) + \frac{2}{5}X, \qquad 5X^2 + 3 = \frac{25}{2}X\left(\frac{2}{5}X\right) + 3, \qquad \frac{2}{5}X = 3\,\frac{2}{15}X + 0$$
Le pgcd de $5X^2+3$ et X^3+X est donc 3 ou encore 1 à inversible près. Les deux polynômes $5X^2 + 3$ et $X^3 + X$ sont donc premiers entre eux.

Exercice 919

Montrer que $\mathbb{Z}[X]$ n'est pas euclidien en montrant que $(2, X)$ n'est pas principal.

Éléments de réponse 919

Montrons que $(2, X)$ n'est pas principal. Raisonnons par l'absurde : supposons qu'il existe un polynôme P tel que $(2, X) = (P)$. En particulier 2 appartient à (P), c'est-à-dire P divise 2. Notons que les diviseurs de 2 dans $\mathbb{Z}[X]$ sont 1, 2, -1 et -2.

◇ Si $P = 2$ ou -2, alors les multiples de P sont des polynômes dont tous les coefficients sont divisibles par 2. En particulier $X \in (P)$ a des coefficients divisibles par 2 : contradiction.

◇ Si $P = 1$ ou -1, alors $(P) = \mathbb{Z}[X]$. Un polynôme de $(2, X)$ s'écrit par définition $2A + XB$ avec A, B dans $\mathbb{Z}[X]$; le terme constant d'un tel polynôme est divisible par 2 ce qui n'est pas le cas du polynôme constant égal à 1. Il en résulte que 1 n'appartient pas à $(2, X)$. Mais 1 appartient à $(P) = \mathbb{Z}[X]$. Ainsi $(2, X) \neq P$.

Puisque $(2, X)$ n'est pas principal, $\mathbb{Z}[X]$ n'est pas euclidien.

Exercice 920

1. Soit A est un corps contenant un nombre infini d'éléments. Montrer que la fonction $A[X] \to A^A$, définie par $P \mapsto \widetilde{P}$ est un morphisme d'anneaux injectifs (en particulier, on peut assimiler polynômes et fonctions polynômiales).
2. Peut-on généraliser l'identification entre polynômes et fonctions polynômiales sans les hypothèses sur A ?

Éléments de réponse 920

1. Soit A est un corps contenant un nombre infini d'éléments. La fonction $\varphi\colon A[X] \to A^A$, définie par $P \mapsto \widetilde{P}$ où $\widetilde{P}$ est clairement un morphisme. D'après un exercice précédent si A est un anneau intègre et P un polynôme non nul, alors $\widetilde{P}$ est une fonction ayant un nombre de zéros inférieur ou égal au degré de P. La fonction nulle ayant un nombre infini de zéros, $\widetilde{P}$ n'est pas la fonction nulle dès que P est non nul. Il s'en suit que le noyau de φ est réduit au polynôme nul : φ est injectif.
2. Nous ne pouvons pas généraliser l'identification entre polynômes et fonctions polynômiales sans les hypothèses sur A ; comme nous l'avons vu en cours le polynôme $P = X^2 + X$ dans $\mathbb{Z}/2\mathbb{Z}$ satisfait les propriétés suivantes :
   ◇ le polynôme P est non nulle,
   ◇ la fonction polynomiale associée à P est nulle.

Exercice 921

Soit $P = \sum a_i X^i \in \mathbb{Z}[X]$, p un nombre premier et $\overline{P} = \sum \overline{a_i} X^i$ l'image $\overline{P}$ de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.

1. Comparer le degré de P et celui de P. À quelle condition a-t-on égalité ?
2. Si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et a même degré que P, montrer que $P \in \mathbb{Z}[X]$ est irréductible.
3. Décomposer $\overline{P} = X^3 + X^2 + X + \overline{1}$ sur $\mathbb{Z}/3\mathbb{Z}$.
4. Montrer que $P = X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Z}$.

Éléments de réponse 921

Soient $P = \sum a_i X^i \in \mathbb{Z}[X]$, p un nombre premier et $\overline{P} = \sum \overline{a_i} X^i$ l'image de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.

1. Nous avons $\deg \widetilde{P} \leq \deg P$ avec égalité si et seulement si p ne divise pas le coefficient dominant a_n de P.
2. Montrons que si $P \in \mathbb{Z}[X]$ est réductible, alors $\overline{P}$ est réductible. Supposons que $P \in \mathbb{Z}[X]$ soit réductible, c'est-à-dire que $P = QR$. Nous avons $\overline{P} = \overline{Q}\,\overline{R}$. Pour montrer que $\overline{P}$ est réductible il suffit donc de montrer que $\overline{Q}$ et $\overline{R}$ sont non inversibles, *i.e.* non constants. Nous avons d'une part
$$\deg \overline{P} = \deg \overline{Q} + \deg \overline{R} \leq \deg Q + \deg R = \deg(QR) = \deg P$$
et d'autre part $\deg \overline{P} = \deg P$. Il en résulte que $\deg Q = \deg \overline{Q}$ et $\deg R = \deg \overline{R}$. Puisque par hypothèse Q et R sont des polynômes non constants nous obtenons que $\overline{Q}$ et $\overline{R}$ sont non constants.
3. Décomposons $\overline{P} = X^3 + X^2 + X + \overline{1}$ sur $\mathbb{Z}/3\mathbb{Z}$.

   Si P était réductible, nous aurions $P = QR$ avec Q de degré 2 et $R = aX + b$ de degré 1. En particulier P aurait une racine $-\frac{b}{a}$. Ainsi pour montrer que P est irréductible il suffit de voir que P n'a pas de racine. Remarquons que
$$P(\overline{0}) = \overline{1}, \qquad P(\overline{1}) = \overline{1}, \qquad P(\overline{2}) = \overline{2};$$
autrement dit P est sans racine donc irréductible.
4. Montrons que $P = X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Z}$. L'image $\overline{P}$ de P est irréductible dans $\mathbb{Z}/3\mathbb{Z}[X]$ d'après 3. et a même degré que P. Le point 2. assure alors que P est irréductible.

INDEX

circulaire (relation binaire), 9

représentant canonique, 16

BIBLIOGRAPHIE