Feuille d'exercices n° 3

Exercice 1

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) $a_{11} = a_{22} = 1$.

Solution 1

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 :

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} \tag{1}$$

(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) 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 G/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)) 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) 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) 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 2 Soient $n \geqslant 2$ un entier et $d \geqslant 1$ 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 $n = 6$, $d = 3$)

Solution 2

◇ Si $d = 1$, le seul sous-groupe d'ordre 1 de $\mathbb{Z}/n\mathbb{Z}$ est $\{\overline{0}\}$.

◇ Supposons maintenant $d \geqslant 2$.
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 :

$$\langle q \rangle = \left\{\overline{0}, \overline{q}, \overline{2q}, \ldots, \overline{(d-1)q}\right\}.$$

Unicité : Soit $\mathrm{H} \subset \mathbb{Z}/n\mathbb{Z}$ un sous-groupe d'ordre $d \geqslant 2$. 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 k : $a = qk + r$, $0 \leqslant r \leqslant k-1$, 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 3 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 leur cardinaux.
(3) Conclure.

Solution 3

(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 $g\mathrm{H} = \mathrm{H}g = \mathrm{G} \smallsetminus \mathrm{H}$; 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 $\mathcal{S}_4$ la réponse serait différente : les 3-cycles forment une seule classe de conjugaison dans $\mathcal{S}_4$, 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 4
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 $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

Solution 4

1. Les éléments de $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$. En voici la liste

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$$

Il en résulte que G est un groupe d'ordre 6.

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 $g \in \mathrm{G}$ et $u \in E$ on définit $g * u \in E$ comme l'image du vecteur u par l'application linéaire de matrice g dans la base (v, w).

3. Montrons que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

   Fixons une base de E et considérons l'action correspondante de G sur E. Pour tout $g \in \mathrm{G}$ l'application $\varphi_g \colon u \mapsto g * u$ est définie par les images des vecteurs non nuls de E ; en effet le vecteur nul a toujours pour image lui-même.

   Ainsi à tout élément de G est associée une permutation de $E \smallsetminus \{0\}$. Or E compte $2^2 = 4$ éléments. Soient v_1, v_2 et v_3 les trois vecteurs non nuls de E. Alors

$$g \mapsto \big((v_1, v_2, v_3) \mapsto (g * v_1, g * v_2, g * v_3)\big)$$

   définit un homomorphisme de groupes de G dans $\mathcal{S}_3$. Cet homomorphisme est injectif. Par suite G est isomorphe à un sous-groupe de $\mathcal{S}_3$. Puisque G et $\mathcal{S}_3$ ont même ordre, G est isomorphe à $\mathcal{S}_3$.

Exercice 5

Soit p un nombre premier. Soit $n \geqslant 1$ 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 $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$.
2. Montrer que l'ordre de $Z(\mathrm{G})$ est > 1 (sans utiliser 1.)

Indication : faire agir G par conjugaison sur H.

Solution 5

Soit p un nombre premier. Soit $n \geqslant 1$ 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 $\forall\, g \in \mathrm{G}$, $g\mathrm{H}g^{-1} \subset \mathrm{H}$.

   L'ordre de H est une puissance de p soit p^β car $|\mathrm{H}|$ divise $|\mathrm{G}|$ qui est une puissance de p. L'ordre de H est aussi somme des cardinaux des orbites pour cette action ; chacune de ces orbites a pour cardinal un diviseur de $|\mathrm{G}|$, 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. Nous avons alors

$$|\mathrm{H}| = p^\beta = 1 + \text{ somme de puissances de } p$$

   contradiction. Par suite $Z(\mathrm{G}) \cap \mathrm{H} \neq \{e\}$.

2. Montrons que l'ordre de $Z(\mathrm{G})$ est > 1. Nous allons encore appliquer la formule des classes. 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

$$p^n = |\mathrm{G}| = 1 + \text{ somme de puissances de } p$$

   contradiction. Il en résulte que $|Z(\mathrm{G})| > 1$.

Exercice 6

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 $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrer que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (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 $|\mathrm{G}|$ 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 $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Solution 6

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 $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrons que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
   L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{Stab}(g)$ est claire.
   Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{Stab}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{Stab}(g)$.
   Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (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 $\mathrm{Stab}(g)$. Il en résulte que $\mathrm{Stab}(g)$ 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 $\mathrm{G} \setminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{Stab}(g)|$. Mais $|\mathrm{G} : \mathrm{Stab}(g)| \geqslant p$ car $|\mathrm{G} : \mathrm{Stab}(g)|$ 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 $|Z(\mathrm{G})| \geqslant p$. Finalement lorsque G n'est pas abélien, nous avons
   $$|Z(\mathrm{G})| \in \left\{p, p^2, \ldots, p^{n-2}\right\}$$
   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 $\mathrm{G} \setminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \setminus \{e\}$ 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 7

Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite.

Montrer que les stabilisateurs Stab_g et Stab_h sont des sous-groupes conjugués de G.

En déduire que Stab_g et Stab_h ont même ordre.

Solution 7

Soient E un ensemble et G un groupe opérant 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 $y \in \mathrm{Stab}_g$. 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 Stab_h. Autrement dit $x\mathrm{Stab}_g x^{-1} \subset \mathrm{Stab}_h$.
Un raisonnement similaire conduit à $\mathrm{Stab}_h \subset x\mathrm{Stab}_g x^{-1}$.
Il s'en suit que $\mathrm{Stab}_h = x\mathrm{Stab}_g x^{-1}$.

L'application $y \mapsto xyx^{-1}$ est un automorphisme de G. C'est donc une bijection et l'image de Stab_g par cet automorphisme est Stab_h. Ces deux ensembles ont donc même cardinal.

Exercice 8

Soit E un ensemble fini. Soit G un groupe fini qui opère sur E. Pour tout g dans G on définit

$$E^g = \big\{ s \in E \,|\, gs = s \big\}.$$

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

   $$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

   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. En déduire la formule de Burnside

   $$|\mathrm{G}| \times \text{ le nombre d'orbites } = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g).$$

Solution 8

1. Construisons la table de l'opération

   $$\varphi \colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$

   définie par

   $$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

   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 $\displaystyle\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.

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

$$\begin{aligned}\varphi^{-1}(V) &= \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ &= \big\{(g,s) \in \mathrm{G}\times E \,|\, s \in E^g\big\}\\ &= \{g_1\}\times E^{g_1} \cup \{g_2\}\times E^{g_2} \cup \ldots \cup \{g_p\}\times E^{g_p}\end{aligned}$$

ce qui conduit à

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$$

D'autre part

$$\begin{aligned}\varphi^{-1}(V) &= \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ &= \big\{(g,s) \in \mathrm{G}\times E \,|\, g \in \mathrm{G}_s\big\}\\ &= \mathrm{G}_{s_1}\times\{s_1\} \cup \mathrm{G}_{s_2}\times\{s_2\} \cup \ldots \cup \mathrm{G}_{s_q}\times\{s_q\}\end{aligned}$$

ce qui entraîne

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{s\in E} |\mathrm{G}_s|.$$

Il en résulte que

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = \sum_{s\in E} |\mathrm{G}_s|.$$

3. Si s est un élément de E, on désigne par $\mathcal{O}_s$ l'orbite de s sous l'action de G. On sait que $|\mathrm{G}_s| = \frac{|\mathrm{G}|}{\mathrm{card}(\mathcal{O}_s)}$. Par suite

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = |\mathrm{G}| \left(\frac{1}{\mathrm{card}(\mathcal{O}_{s_1})} + \frac{1}{\mathrm{card}(\mathcal{O}_{s_2})} + \ldots + \frac{1}{\mathrm{card}(\mathcal{O}_{s_q})}\right)$$

Soient σ_1, σ_2, …, σ_r des éléments de E tels que E est la réunion disjointe des $\mathcal{O}_{\sigma_i}$ pour $1 \leqslant i \leqslant r$. Nous avons

$$\sum_{s\in\mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_s)} = \sum_{s\in\mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \sum_{s\in\mathcal{O}_{\sigma_i}} 1 = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \times \mathrm{card}(\mathcal{O}_{\sigma_i}) = 1$$

d'où la formule de Burnside.

Exercice 9

Combien $(\mathbb{F}_2)^n$ admet-il de sous-espaces vectoriels de dimension k ?

Solution 9

Soit $0 \leqslant k \leqslant n$. 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 [1]

$$\underbrace{(2^k-1)(2^k-2)\dots(2^k-2^{k-1})}_{|\mathrm{GL}(k,\mathbb{F}_2)|} \times (2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1}).$$

Simplifions cette expression :

$$\begin{aligned}
&(2^k-1)(2^k-2)\dots(2^k-2^{k-1})(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1}) \\
&\quad = \Big((2^k-1)(2^k-2)\dots(2^k-2^{k-1})\Big)\Big((2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\Big) \\
&\quad = \Big((2^k-1)\times 2\times(2^{k-1}-1)\times\dots\times 2^{k-1}\times(2-1)\Big) \\
&\qquad\qquad \Big(2^k\times(2^{n-k}-1)\times 2^{k+1}\times(2^{n-k-1}-1)\times\dots\times 2^{n-1}\times(2-1)\Big) \\
&\quad = 2\times 2^2\times\dots 2^k\times 2^{k+1}\times\dots\times 2^{n-1}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1) \\
&\qquad\qquad \times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times(2-1) \\
&\quad = 2^{1+2+\dots+(n-1)}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1) \\
&\qquad\qquad \times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1) \\
&\quad = 2^{\frac{n(n-1)}{2}}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1) \\
&\qquad\qquad \times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)
\end{aligned}$$

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 10

Montrer que dans un groupe tout sous-groupe d'indice 2 est distingué.

Solution 10

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

$$ghg^{-1} = xh_0hh_0^{-1}x^{-1} = xh'x^{-1}$$

où $h' = h_0hh_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à xH, *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 11

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 $\mathrm{G} = \{\tau_{a,b} \,|\, a \neq 0\}$.
   Montrer que G est un groupe pour la composition des applications.
2. Soit $\mathrm{H} = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.
   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.

1. 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...

5. Soit $\mathrm{N} = \{\tau_{a,b} \,|\, a = 1\}$.
   Montrer que N est un sous-groupe distingué de G.

Solution 11

1. Soit $\mathrm{G} = \{\tau_{a,b} \,|\, a \neq 0\}$.
   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 12

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 ?

Solution 12

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 13

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.

Solution 13

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 ${}^{\mathrm{G}}\!/_{\mathrm{N}}$.

Soit q l'ordre de $h\mathrm{N}$ dans ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. 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 $(h\mathrm{N})^{|\mathrm{H}|} = \mathrm{H}$. 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 14

Soit G un groupe qui ne contient qu'un seul sous-groupe H d'ordre n.

Montrer que H est distingué dans G.

Solution 14

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 15

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 ?

Solution 15

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 16

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.

Solution 16

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 $0 \leqslant r < p_0$. 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 17

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 ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ des classes à gauche modulo H.

(b) Montrer que cette action est transitive.
Déterminer le stabilisateur de $a\mathrm{H}$.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Solution 17

(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

$$[\mathrm{G} : \mathrm{H}] = \mathrm{card}\Big({}^{\mathrm{G}}\!/_{\mathrm{H}}\Big) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[\mathrm{G} : 1]}{[\mathrm{G}_x : 1]} = \frac{[\mathrm{G} : 1]}{[\mathrm{H} : 1]}.$$

Exercice 18

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 $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

Solution 18

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

$$\mathbb{H}_8 = \big\{ \pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k} \big\}$$

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 $\mathrm{G} = \mathcal{S}_4$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ 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 $\langle g_1 \rangle$, …, $\langle g_n \rangle$. 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 $\mathrm{G} = \mathcal{S}_3$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ 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 19

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 homomorphisme 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 $\mathrm{Int(G)} \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Solution 19

a) Il faut montrer que $\varphi(a)$ est un homomorphisme 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 $g \in \ker\varphi(a)$, autrement dit $aga^{-1} = e$ d'où $g = a^{-1}a = e$. Ainsi $\varphi(a)$ est un homomorphisme 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 homomorphisme de groupes de G dans Aut(G).

c) Int(G) est l'image de G par l'homomorphisme 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 $\mathrm{Im}\,\varphi$. Le groupe Int(G) est distingué dans Aut(G).

d) D'une part $\ker\varphi$ est le centre $Z(\mathrm{G})$ de G, d'autre part $\mathrm{Im}\,\varphi = \mathrm{Int(G)}$. Le théorème d'isomorphisme assure que $\mathrm{Int(G)} \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Exercice 20

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.

Solution 20

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 21 [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 $F = \{(g, x) \in \mathrm{G} \times X \,|\, g \cdot x = x\}$ 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 $\pm\frac{2\pi}{3}$.

   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.

Solution 21

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 suite $\left|\mathrm{G}/\mathrm{G}_x\right| = |\mathcal{O}_x|$, *i.e.* $|\mathrm{G}| = |\mathcal{O}_x|\,|\mathrm{G}_x|$. Ainsi $\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.
   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.

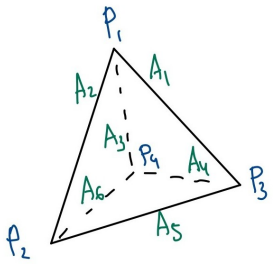
   a) Soit X l'ensemble des coloriages où on interdit cette identification. Quel est le cardinal de X ?
   Un tétraèdre régulier a quatre faces S_1, S_2, S_3, S_4 et six arêtes A_1, A_2, …, A_6. En particulier il y a dix objets à colorier. On a donc $|X| = k^{10}$.

   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 $|\mathrm{Fix}(g)| = k^6$.

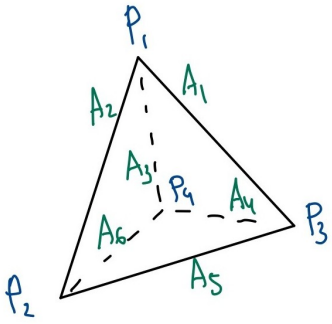


Par exemple si g est la rotation d'axe passant par le milieu de l'arête A_2 et le milieu de l'arête A_4 alors

- ◇ g envoie P_1 sur P_2 et P_2 sur P_1 donc une fois A_1, A_2 et A_3 fixés, A_1, A_4 et A_5 le sont $\rightsquigarrow k^3$ choix,
- ◇ g envoie P_3 sur P_4 et P_4 sur P_3, il n'y a donc aucune contrainte sur A_6 $\rightsquigarrow k$ choix,
- ◇ g envoie $P_1P_2P_3$ sur $P_1P_2P_4$ et $P_1P_2P_4$ sur $P_1P_2P_3$, autrement dit les faces $P_1P_2P_4$ et $P_1P_2P_3$ ont même couleur $\rightsquigarrow k$ choix,
- ◇ g envoie $P_2P_3P_4$ sur $P_1P_3P_4$ et $P_1P_3P_4$ sur $P_2P_3P_4$, autrement dit les faces $P_1P_3P_4$ et $P_2P_3P_4$ ont même couleur $\rightsquigarrow k$ choix

soit au total k^6 choix.

- 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 $|\mathrm{Fix}(g)| = k^4$.



Par exemple si g est une rotation d'axe passant par P_1 et le centre de la face $P_2P_3P_4$, alors

- ◇ g envoie A_1 sur A_2, A_2 sur A_3 et A_3 sur A_1 donc les arêtes A_1, A_2 et A_3 sont de même couleur $\rightsquigarrow k$ choix,
- ◇ g envoie A_4 sur A_6, A_6 sur A_5 et A_5 sur A_4 donc les arêtes A_4, A_5 et A_6 sont de même couleur $\rightsquigarrow k$ choix,
- ◇ g laisse fixe la face $A_4A_5A_6$ $\rightsquigarrow k$ choix,
- ◇ g envoie la face $A_1A_2A_5$ sur la face $A_1A_3A_4$, la face $A_1A_3A_4$ sur la face $A_2A_3A_6$ et la face $A_2A_3A_6$ sur la face $A_1A_2A_5$ donc les faces $A_1A_2A_5$, $A_1A_3A_4$ et $A_2A_3A_6$ sont de même couleur $\rightsquigarrow k$ choix

soit au total k^4 choix

Finalement

$$n = \frac{1}{12}\left(k^{10} + 3 \cdot k^6 + 8 \cdot k^4\right)$$

Exercice 22

1. Soit G un groupe fini de cardinal p^m avec p premier et $m \in \mathbb{N}^*$ qui opère sur un ensemble fini non vide E. Posons
$$E^{\mathrm{G}} = \left\{x \in E \,|\, \forall\, g \in \mathrm{G},\, g \cdot x = x\right\}.$$
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 : faire agir $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des $(x_1, x_2, \ldots, x_p)$ de H^p tels que $x_1x_2\ldots x_p = e$.

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.

Solution 22

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. Si x_i est un élément de ω_i, alors $|\omega_i| = [\mathrm{G} : \mathrm{Stab}_{\mathrm{G}}(x_i)]$, c'est donc une puissance de p. 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. 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 $\mathcal{S}_p$. 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 H^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. Appliquons alors le résultat de la question précédente à l'opération induite sur E. 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 E^{K} 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 $x \in \mathrm{H}$ d'ordre p. Or par hypothèse $x^m = e$ donc p divise m.

Exercice 23

a) Combien y a-t-il d'opérations 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 opération $(g, x) \mapsto g \cdot x$ de G sur X telle que pour tout $g \in \mathrm{G}$ l'application $x \mapsto g \cdot x$ soit un automorphisme de X.
L'opération de G sur lui-même par translation est-elle une opération par automorphismes ?
L'opération de G sur lui-même par conjugaison est-elle une opération par automorphismes ?

c) Si $\mathrm{G} = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathbb{Z}/13\mathbb{Z}, +\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

d) Si $\mathrm{G} = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathcal{S}_3, \circ\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

Solution 23

a) On cherche le nombre de morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans le groupe des permutations $\mathcal{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\overline{1})$) dans $\mathcal{S}_5$. Or $\mathcal{S}_5$ 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'opération de G sur lui-même par translation n'est pas une opération par automorphismes.
L'opération de G sur lui-même par conjugaison est une opération 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 $\mathcal{S}_3$ sont intérieurs. Le groupe des automorphismes de $\mathcal{S}_3$ est donc isomorphe à $\mathcal{S}_3$ quotienté par son centre, c'est-à-dire à $\mathcal{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathcal{S}_3$ et il y a 3 possibilités.

Exercice 24

Soit E un espace euclidien. On fait opérer 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 ?

Solution 24

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 25

1. Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E = \big\{(g, x) \in \mathrm{G} \times X \,|\, g \cdot x = x\big\},$$

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 ?

Solution 25

1. Désignons par $\mathrm{Fix}(g) = \big\{x \in X \,|\, g \cdot x = x\big\}$ 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 $\sum_{y \in \mathcal{O}_x} |\mathrm{G}_y| = |\mathrm{G}|$.

◇ 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 $|E| = \displaystyle\sum_{x\in X}|\mathrm{G}_x|$. Par conséquent $\displaystyle\sum_{g\in\mathrm{G}}|\mathrm{Fix}(g)| = \sum_{x\in X}|\mathrm{G}_x|$. Mais d'après ce qui précède $|\Omega|\,|\mathrm{G}| = \displaystyle\sum_{x\in X}|\mathrm{G}_x|$. 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 $\mathrm{G} = \mathcal{S}_n$ agit (via l'action évidente) sur $X = \big\{1, 2, \ldots, n\big\}$, 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

$$\mathrm{G} = \big\{\mathrm{id},\, r,\, r^2,\, r^3,\, r^4,\, r^5,\, r^6,\, r^7,\, r^8,\, s,\, r\circ s,\, r^2\circ s,\, r^3\circ s,\, r^4\circ s,\, r^5\circ s,\, r^6\circ s,\, r^7\circ s,\, r^8\circ s\big\}$$

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 26

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 $\mathcal{S}_{\mathbb{P}(E)}$.
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 $\mathcal{S}_{q+1}$.

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 $\mathcal{S}_3$.

f) Supposons que $q = 3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2, \mathbb{F}_3)$ sur $\mathcal{S}_4$ 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 $\mathcal{S}_5$ et de $\mathrm{PSL}(2, \mathbb{F}_5)$ sur $\mathcal{A}_5$ (rappelons une conséquence non trviale de la simplicité des groupes alternés : tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ pour $n \geqslant 5$).

Solution 26

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 $Z(\mathrm{SL}(n,\Bbbk)) = \{\lambda \mathrm{Id} \,|\, \lambda^n = 1\}$. Or il y a $\mathrm{pgcd}(n, q-1)$ racines $n$ièmes de l'unité dans un corps $\Bbbk$ de cardinal q [2] donc

$$|\mathrm{PSL}(n,\Bbbk)| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}}{\mathrm{pgcd}(n,q-1)}.$$

c) Faisons opérer $\mathrm{PGL}(n,\Bbbk)$ 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'opération 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 $\mathcal{S}_{\mathbb{P}(E)}$.

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.* $|\mathbb{P}(E)| = q+1$.

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 $\mathcal{S}_3$ 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 $|\mathcal{S}_4| = 24$. Ainsi Φ réalise un isomorphisme entre entre $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathcal{S}_4$. 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 $\mathcal{S}_4$ est $\mathcal{A}_4$ [3] 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 $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathcal{S}_4$ 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 $\mathcal{S}_5$ qui ne peut être que $\mathcal{A}_5$ [4].

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 $\mathcal{S}_6$ lequel est isomorphe à $\mathcal{S}_5$ 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 $\mathrm{PGL}(2,\mathbb{F}_5) \simeq \mathcal{S}_5$ et est donc isomorphe, via Φ, à $\mathcal{A}_5$.

Exercice 27

Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Solution 27

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 faisons agir G sur lui-même par conjugaison

$$\mathrm{G}\times\mathrm{G}\to\mathrm{G}, \qquad\qquad (g,h)\mapsto hgh^{-1}.$$

Notons que g appartient à $Z(\mathrm{G})$ si et seulement si l'orbite $\mathcal{O}_g$ de g sous cette action est réduite à $\{g\}$. L'équation aux classes assure que

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|.$$

D'après le théorème de Lagrange $|\mathcal{O}_{g_i}|$ divise p donc

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

conduit à

$$|\mathrm{G}| \equiv |Z(\mathrm{G})| \bmod p$$

2. 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.
3. En effet, dès que $m \geqslant 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.
4. En effet, dès que $m \geqslant 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Mais e_G appartient à $Z(\mathrm{G})$ donc $|Z(\mathrm{G})| \geqslant p$. Par suite $Z(\mathrm{G})$ est de cardinal 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 de cardinal p premier, $\mathrm{G}/Z(\mathrm{G})$ est cyclique et G est, d'après a), abélien.

Exercice 28

Soit G un groupe fini d'ordre 21 opérant 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.

Solution 28

1. L'équation aux classes s'écrit
$$n = a_1 + 3a_2 + 7a_3 + 21a_4$$
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 $n \geqslant 12$ peut s'écrire $3a + 7b$ avec a, $b \geqslant 0$. Or c'est vrai pour 12, 13 et 14 donc pour tout entier plus grand en ajoutant un multiple de 3.