Feuille d'exercices n° 1

Exercice 1

Donner un exemple de groupe non abélien.

Solution 1

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 $\mathcal{S}_3$, c'est-à-dire le groupe contenant les six bijections de l'ensemble $\{1, 2, 3\}$.

Exercice 2

Donner un exemple de groupe contenant exactement 3 éléments.

Solution 2

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

$$\mu_3 = \left\{1, \exp\left(\frac{2\mathbf{i}\pi}{3}\right), \exp\left(-\frac{2\mathbf{i}\pi}{3}\right)\right\}$$

des racines cubiques de l'unité.

Exercice 3

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 ?

Solution 3

La multiplication permet de munir $\mathbb{C}^*$ d'une structure de groupe et

$$\mathrm{ordre}(\mathbf{i}) = 4, \qquad \mathrm{ordre}(2) = \infty.$$

Exercice 4

Si R est un rectangle (non carré), donner la liste des isométries du plan préservant ce rectangle. Cet ensemble est-il un groupe ?

Solution 4

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 5

Donner un exemple de groupe d'ordre fini, abélien et non cyclique.

Solution 5

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 6

Soit $\sigma \in \mathcal{S}_8$ 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.

Solution 6

La décomposition canonique de σ est

$$\sigma = (1\ 7\ 6) \circ (3\ 8) \circ (4\ 5).$$

Exercice 7

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.

Expliciter un isomorphisme du groupe $\mathrm{Isom}(T)$ vers le groupe symétrique $\mathcal{S}_3$.

Solution 7

Si A_1, A_2 et A_3 sont les sommets du triangle T, alors l'isomorphisme souhaité est donné par $f \in \mathrm{Isom}(T) \mapsto \sigma \in \mathcal{S}_3$ où σ est définie par $f(A_i) = A_{\sigma(i)}$.

Exercice 8

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 $\mathrm{H} = \{\mathrm{id},\ s_A\}$, 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.* $g\mathrm{H} \neq \mathrm{H}g$.

Solution 8

Par exemple $g = S_B$ convient car

$$s_B\mathrm{H} = \{s_B,\ s_B \circ s_A\}, \qquad \mathrm{H}s_B = \{s_B,\ s_A \circ s_B\}$$

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 9

Calculer l'ordre de la permutation $\sigma \in \mathcal{S}_{10}$ suivante

$$\sigma = (1\ 2\ 3\ 4\ 5) \circ (6\ 7\ 8) \circ (9\ 10)$$

Solution 9

La permutation σ est du type 2, 3, 5. Son ordre est donc $\mathrm{ppcm}(2, 3, 5) = 30$.

Exercice 10

Donner une permutation $\sigma \in \mathcal{S}_6$ telle que $\sigma \circ (1\ 3\ 5) \circ \sigma^{-1} = (2\ 4\ 6)$.

Solution 10

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 11

Donner la liste des classes de conjugaison avec leur cardinal pour le groupe alterné $\mathcal{A}_5$.

Solution 11

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 $\mathcal{S}_5$ la réponse serait différente, il n'y aurait qu'une seule classe de 5-cycles, de cardinal 24.

Exercice 12

Donner un exemple de deux groupes d'ordre 8 non abéliens et non isomorphes.

Solution 12

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
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{bmatrix}, \qquad \begin{bmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{bmatrix}$$
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 13

Parmi les ensembles suivants lesquels sont des groupes pour l'opération donnée ?

1. $\mathbb{Q}^*$, $+$;
2. $\mathbb{Q}^*$, $\cdot$;
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. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 0\}$, $+$.

Solution 13

2. $\mathbb{Q}^*$, $\cdot$;
5. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\}$, $\cdot$

sont des groupes.

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 $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ 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 14

Parmi les groupes suivants lesquels sont abéliens ?

1. $\mathbb{R}[x]_{\leqslant 8}$, $+$ (les polynômes de degré $d \leqslant 8$ 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. $\mathcal{S}_4$, $\circ$.

Solution 14

$\mathbb{R}[x]_{\leqslant 8}$, $+$ (les polynômes de degré $d \leqslant 8$ dans une variable x à coefficients réels) est un groupe abélien.

Exercice 15

Lesquels des ensembles A sont des sous-groupes du groupe G donné ?

1. $A = \mathbb{R}[x]_8$, $+$ (les polynômes de degré 8) et $\mathrm{G} = \mathbb{R}[x]_{\leqslant 8}$, $+$;
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 $\mathrm{G} = \mathbb{Z}$.

Solution 15

$A = 100\mathbb{Z}$ est un sous-groupe de $\mathrm{G} = 10\mathbb{Z}$.

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 16

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. $\overline{3}, \overline{5}, \overline{7}, \overline{9}$.

Solution 16

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 Bezout ; en effet on a les équivalences suivantes :

$$\begin{aligned} &\text{Il existe } b \in \mathbb{Z} \text{ tel que } ab \equiv 1 \bmod n \\ &\qquad \iff \text{il existe } b \in \mathbb{Z} \text{ et } k \in \mathbb{Z} \text{ tels que } ab = kn + 1 \\ &\qquad a \text{ est premier avec } n \end{aligned}$$

Exercice 17

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. $\{1, -1\}$.

Solution 17

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 18

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 $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?

Solution 18

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 19

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.

Solution 19

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 20

Compléter pour obtenir un énoncé correct : Si G est le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $g = ([1]_4, [4]_6)$, alors

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. $\langle g\rangle = \mathrm{G}$.

Solution 20

Si G est le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $g = ([1]_4, [4]_6)$, alors

$\langle g\rangle = \{([1]_4,\, [4]_6),\, ([2]_4,\, [2]_6),\, ([3]_4,\, [0]_6),\, ([0]_4,\, [4]_6),\, ([1]_4,\, [2]_6),\, ([2]_4,\, [0]_6),\, ([3]_4,\, [4]_6),\, ([0]_4,\, [2]_6),\, ([1]_4,\, [0]_6),\, ([2]_4,\, [4]_6),\, ([3]_4,$

Exercice 21

Quelles sont les implications 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.

Solution 21

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 $g \in \mathrm{G} \smallsetminus \{e\}$. 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 22

La décomposition de la permutation $(1\ 2\ 3\ 4)(2\ 3)(1\ 4\ 3)$ de $\mathcal{S}_4$ en cycles disjoints est :

1. $(3\ 2\ 4)$;
2. id ;

3. $(2\ 4\ 3)(1)$;
4. $(1)(2)(3)(4)$.

Solution 22

La décomposition de la permutation $(1\ 2\ 3\ 4)(2\ 3)(1\ 4\ 3)$ de $\mathcal{S}_4$ en cycles disjoints est :

1. $(3\ 2\ 4)$;
3. $(2\ 4\ 3)(1)$.

Exercice 23

L'ordre de l'élément $(1\ 3)(2\ 4\ 5)(6\ 9\ 8\ 7)$ dans $\mathcal{S}_{11}$ est

1. 9 ;
2. 11 ;
3. 12 ;
4. 24.

Solution 23

L'ordre de l'élément $(1\ 3)(2\ 4\ 5)(6\ 9\ 8\ 7)$ dans $\mathcal{S}_{11}$ 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 $\operatorname{ppcm}(2, 3, 4) = 12$.

Exercice 24

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.

Solution 24

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 25

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.

Solution 25

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 26

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. $\{\dots, -1, 3, 7, 11, \dots\}$;
4. $-5 * \mathrm{H}$.

Solution 26

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. $\{\dots, -1, 3, 7, 11, \dots\}$;
4. $-5 * \mathrm{H}$.

Exercice 27

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 $h^{-1}gh \in \mathrm{H}$.

Solution 27

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 28

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 $g\mathrm{H} = \mathrm{H}g$.

Solution 28

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 29

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 ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$ est cyclique ;
6. Si G n'est pas cyclique et H est un sous-groupe de G, alors ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$ n'est pas cyclique.

Solution 29

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 ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$ est abélien ; En effet soient $g_1\mathrm{H}$ et $g_2\mathrm{H}$ deux éléments de ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$, 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 ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$ est cyclique. En effet soit x un générateur de G. Soit $g\mathrm{H}$ un élément de ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$. 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 ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$.

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 ${}^{\mathrm{G}}\!/\!_{\mathrm{H}}$ 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 30

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.

Solution 30

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 31

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 $\mathrm{G} = \mathcal{S}_3$ sur $A = \{1, 2, 3, 4\}$;

4. l'élément $(1\ 2) \cdot (3\ 4)$ si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathcal{S}_4$ sur lui-même ($A = \mathrm{G}$).

Solution 31

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 $\mathrm{G} = \mathcal{S}_3$ sur $A = \{1, 2, 3, 4\}$, alors l'élément $(1\ 2) \cdot 2$ est 2 ;
4. si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathcal{S}_4$ 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 32

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 ?

Solution 32

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 33

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.

Solution 33

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 34

Soit G un groupe. Soient a, b deux éléments de G d'ordre fini. Le groupe engendré par a et b est-il fini ?

Solution 34

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 35

Dans le lemme chinois expliciter rapidement comment on construit l'isomorphisme.

Solution 35

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 $\dot{n}$ la classe de n modulo pq, respectivement p, respectivement q. Considérons le morphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$

Il est injectif car $\mathrm{pgcd}(p, q) = 1$. 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 36

Donner un exemple de groupe fini simple.

Solution 36

Le groupe des permutations $\mathcal{A}_n$ dès que $n \geqslant 5$.