

Éléments de théorie des groupes
Solutions des exercices

Éric Guirbal

Éléments de théorie des groupes
Solutions des exercices

Éric GUIRBAL

Version : 78f12ee (2024-09-28)

Compilé le 28 septembre 2024



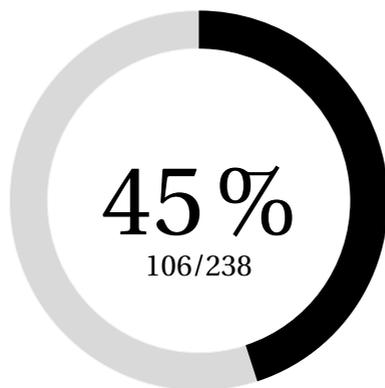
Ce document est distribué selon les termes de la licence Creative Commons
Attribution - Pas d'utilisation commerciale - Partage à l'identique 3.0 France.

<https://creativecommons.org/licenses/by-nc-sa/3.0/fr/>

Sommaire

ÉTAT D'AVANCEMENT DU PROJET	v
CHAPITRE PREMIER / <i>Structure de groupe</i>	1
CHAPITRE II / <i>Classes modulo un sous-groupe</i>	25
CHAPITRE III / <i>Groupes monogènes, symétriques et diédraux</i>	35
CHAPITRE IV / <i>Sous-groupes normaux</i>	55
CHAPITRE V / <i>Groupe opérant sur un ensemble</i>	63
CHAPITRE VI / <i>Groupes finis. Théorèmes de Sylow</i>	81
CHAPITRE VII / <i>Suites de composition</i>	83
CHAPITRE VIII / <i>Groupes abéliens</i>	85
CHAPITRE IX / <i>Groupes libres. Générateurs et relations. Produit libre de groupes</i>	87

État d'avancement du projet



I. Structure de groupe	32/34	
II. Classes modulo un sous-groupe	8/10	
III. Groupes monogènes, symétriques et diédraux	28/33	
IV. Sous-groupes normaux	15/38	
V. Groupe opérant sur un ensemble	15/27	
VI. Groupes finis. Théorèmes de Sylow	7/26	
VII. Suites de composition	1/35	
VIII. Groupes abéliens	0/23	
IX. Groupes libres. Générateurs et relations. Produit libre de groupes	0/12	

CHAPITRE PREMIER

Structure de groupe

1. a) On a $(0 * 0) * 1 = (0 - 0) - 1 = -1$ et $0 * (0 * 1) = 0 - (0 - 1) = 1$ donc $*$ n'est pas associative. De plus $0 * 1 = 0 - 1 = -1$ et $1 * 0 = 1 - 0 = 1$ donc $*$ n'est pas non plus commutative.
- b) Soit $a \in \mathbf{Z}$. $a * e = a$, soit $a - e = a$ implique $e = 0$. De plus $a * 0 = a - 0 = a$ pour tout $a \in \mathbf{Z}$. Donc 0 est l'unique élément neutre à droite pour $*$. Si $a \neq 0$, on a $0 * a = -a \neq a$ donc 0 n'est pas un élément neutre.
- c) Pour tout $a \in \mathbf{Z}$, on a $a * a = a - a = 0$, donc a est un symétrique à droite de a .

2. La loi $*$ admet 0 comme élément neutre. En effet, pour tout $a \in \mathbf{Q}$ on a $a * 0 = a + 0 + a \times 0 = a$ et de même $0 * a = a$. En revanche, on a $a * (-1) = a - 1 - a = -1 \neq 0$, donc -1 n'est pas symétrisable. En conclusion, $(\mathbf{Q}, *)$ n'est pas un groupe.

Remarque. Posons $A = \mathbf{Q} \setminus \{-1\}$. Nous allons montrer que $(A, *)$ est un groupe abélien.

- Soit $a, b \in A$. On a $1 + a \neq 0$ et $1 + b \neq 0$. En remarquant que $a * b = (1 + a)(1 + b) - 1$ on voit que $a * b \neq -1$ et donc que la restriction de $*$ à $A \times A$ définit bien une loi interne.
- On sait déjà que 0 est l'élément neutre de la loi $*$.

— Soit $a, b, c \in A$, on a

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

donc la loi $*$ est associative.

— La loi $*$ est clairement commutative.

— Soit $a \in A$, on a

$$a * \left(-\frac{a}{1+a} \right) = a - \frac{a}{1+a} - \frac{a^2}{1+a} = 0.$$

donc tout élément de A est symétrisable.

3. Soit $x \in G$, x' un symétrique à droite de x et e un élément neutre à droite. On a

$$\begin{aligned} xx' &= e \\ x'(xx') &= x'e \\ (x'x)x' &= x'. \end{aligned}$$

En multipliant à droite par l'inverse de x' , il reste $x'x = e$, donc x' est aussi un symétrique à gauche. De plus $ex = (xx')x = x(x'x) = xe = x$ donc e est aussi un élément neutre à gauche. On a démontré que (G, \cdot) est un groupe.

4. Du fait que tout élément de G est simplifiable à gauche et à droite, les applications translation à gauche et translation à droite sont injectives. Comme en plus G est fini, elles sont bijectives. Autrement dit, pour tout $(a, b) \in G^2$, chacune des équations $ax = b$ et $xa = b$ d'inconnue x possède une unique solution.

Montrons l'existence d'un élément neutre. Soit $a \in G$. Il existe $g \in G$ tel que $ga = a$. Vérifions que g est un neutre à gauche. Soit $x \in G$. Il

existe $h \in G$ tel que $x = ah$. On a alors $gx = g(ah) = (ga)h = ah = x$, ce qui prouve que g est un neutre à gauche. De même, on montre l'existence d'un neutre à droite g' . Enfin on a $gg' = g'$ car g est un neutre à gauche, et $gg' = g$ car g' est un neutre à droite, d'où $g = g'$. Notons e l'élément neutre.

Il reste à montrer que tout élément de G est inversible. Soit $x \in G$. Il existe $y \in G$ tel que $xy = e$. Donc $y(xy) = y$ soit $(yx)y = y$. Multiplions membre à membre par l'inverse à droite de y . Nous obtenons $yx = e$. Donc x est inversible.

Finalement (G, \cdot) est un groupe.

5. a) Soit H le sous-groupe de S_4 engendré par les transpositions τ_{12} et τ_{34} : $H = \langle \tau_{12}, \tau_{34} \rangle = \{e, \tau_{12}, \tau_{34}, \tau_{12}\tau_{34}\}$. Il est clair que pour tout $x \in H$, $x^2 = e$.
- b) Soit $(x, y) \in G^2$. Alors $x^2 = e$ et $y^2 = e$ impliquent $x^{-1} = x$ et $y^{-1} = y$. D'où $xyx^{-1}y^{-1} = xyxy = (xy)^2 = e$ donc $xy = yx$, et le groupe G est abélien.
6. L'application f vérifie $f \circ f = \text{id}_G$, c'est donc une permutation. Supposons que G soit abélien. Alors pour tout $(x, y) \in G^2$, on a

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$$

donc f est un automorphisme (Proposition 1.66).

Réciproquement, si f est un automorphisme, alors pour tout $(x, y) \in G^2$, on a $f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1})$ d'où $(x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$ puis $yx = xy$ donc G est abélien.

7. Soit G un groupe d'ordre $2n$. On définit sur G une relation d'équivalence \mathcal{R} ainsi :

$$x, y \in G, \quad x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = y^{-1}.$$

La classe d'équivalence d'un élément $x \in G$ est $\bar{x} = \{x, x^{-1}\}$. Soit $\{x_i\}_{i \in I}$ une famille de représentants des classes distinctes modulo \mathcal{R} . On a $1 \leq |\bar{x}_i| \leq 2$. On note k le nombre de classes de cardinal 1 et l le nombre de classes de cardinal 2. De $\sum_{i \in I} |\bar{x}_i| = 2n$ on tire $k + 2l = 2n$

puis $k = 2(n - l)$, c'est-à-dire que le nombre d'éléments $x \in G$ tel que $x^2 = e$ est nécessairement pair. Comme e est l'un d'eux, il existe au moins un $x \in G$ distinct de e tel que $x^2 = e$.

8. a) L'ensemble \mathbf{U} est une partie de \mathbf{Q}^* . De plus, si $x \in \mathbf{U}$ et $y \in \mathbf{U}$, on a $xy \in \mathbf{U}$ et $x^{-1} = x \in \mathbf{U}$, donc (\mathbf{U}, \times) est un sous-groupe de (\mathbf{Q}^*, \times) .
- b) L'application $\varphi: \mathbf{U} \rightarrow \frac{\mathbf{Z}}{(2)}$ définie par $\varphi(1) = \bar{0}$ et $\varphi(-1) = \bar{1}$ est un homomorphisme de groupes; en effet,

$$\varphi(1 \times 1) = \varphi(1) = \bar{0} = \bar{0} + \bar{0} = \varphi(1) + \varphi(1),$$

$$\varphi(1 \times (-1)) = \varphi(-1) = \bar{1} = \bar{0} + \bar{1} = \varphi(1) + \varphi(-1)$$

et

$$\varphi((-1) \times (-1)) = \varphi(1) = \bar{0} = \bar{1} + \bar{1} = \varphi(-1) + \varphi(-1).$$

De plus, l'application φ est clairement bijective, donc les groupes (\mathbf{U}, \times) et $(\frac{\mathbf{Z}}{(2)}, +)$ sont isomorphes.

9. Soit $\frac{a}{10^n}, \frac{b}{10^m} \in (\mathbf{D}, +) \subset (\mathbf{Q}, +)$. On a

$$\frac{a}{10^n} - \frac{b}{10^m} = \frac{a10^m - b10^n}{10^{n+m}}$$

avec $a10^m - b10^n \in \mathbf{Z}$ et $n + m \in \mathbf{N}$ donc $\frac{a}{10^n} - \frac{b}{10^m} \in \mathbf{D}$. Ainsi $(\mathbf{D}, +)$ est un sous-groupe de $(\mathbf{Q}, +)$.

10. a) \mathbf{Q}_p est un sous-groupe de $(\mathbf{Q}, +)$, en effet pour tout $(a, n) \in \mathbf{Z} \times \mathbf{N}$, on a

$$\frac{a}{p^n} - \frac{b}{p^m} = \frac{ap^m - bp^n}{p^{n+m}}$$

avec $ap^m - bp^n \in \mathbf{Z}$ et $n + m \in \mathbf{N}$ donc $\frac{a}{p^n} - \frac{b}{p^m} \in \mathbf{Q}_p$.

Ensuite

$$\mathbf{Q}_p = \bigcup_{n \in \mathbf{N}} \left\{ \frac{a}{p^n}; a \in \mathbf{Z} \right\} = \bigcup_{n \in \mathbf{N}} \left\langle \frac{1}{p^n} \right\rangle$$

b) φ est clairement injective, et de l'égalité $\frac{a}{p^n} = p \frac{a}{p^{n+1}}$ on déduit qu'elle est également surjective et donc que φ est une permutation de \mathbf{Q}_p .

Pour tout $(x, y) \in \mathbf{Q}_p^2$, on a $\varphi(x+y) = p(x+y) = px+py = \varphi(x)+\varphi(y)$. Or un homomorphisme bijectif est un isomorphisme (Proposition 1.66) donc φ est un automorphisme du groupe $(\mathbf{Q}_p, +)$.

11. Rappelons que la racine carrée d'un entier naturel qui n'est pas un carré parfait est irrationnel.¹ En particulier, la racine carrée d'un nombre premier est irrationnel.

— $G_1 = \{a + b\sqrt{p}; (a, b) \in \mathbf{Z} \times \mathbf{Z}\}$ est un sous-groupe de $(\mathbf{R}, +)$.

On a $G_1 \subset \mathbf{R}$. Soient $a + b\sqrt{p} \in G_1$, $a' + b'\sqrt{p} \in G_1$. On a

$$(a + b\sqrt{p}) - (a' + b'\sqrt{p}) = (a - a') + (b - b')\sqrt{p} \in G_1$$

— $G_2 = \{a + b\sqrt{p}; (a, b) \in (\mathbf{Q}^2)^*\}$ est un sous-groupe de (\mathbf{R}^*, \times) .

Puisque \sqrt{p} est irrationnel, $G_2 \subset \mathbf{R}^*$. Soient $a + b\sqrt{p} \in G_2$ et $a' + b'\sqrt{p} \in G_2$. En multipliant le dénominateur et le numérateur par le conjugué $a' - b'\sqrt{p}$ de $a' + b'\sqrt{p}$, nous obtenons

$$(a + b\sqrt{p}) \times (a' + b'\sqrt{p})^{-1} = \frac{aa' - pbb'}{a'^2 - pb'^2} + \frac{a'b - ab'}{a'^2 - pb'^2} \sqrt{p} \in G_2.$$

— $G_3 = \{a + ib\sqrt{p}; \mathbf{Z} \times \mathbf{Z}\}$ est un sous-groupe de $(\mathbf{C}, +)$.

Clairement $G_3 \subset \mathbf{C}$. Soient $a + ib\sqrt{p} \in G_3$ et $a' + ib'\sqrt{p} \in G_3$. On a

$$(a + ib\sqrt{p}) - (a' + ib'\sqrt{p}) = (a - a') + i(b - b')\sqrt{p} \in G_3.$$

— $G_4 = \{a + ib\sqrt{p}; (a, b) \in (\mathbf{Q}^2)^*\}$ est un sous-groupe de (\mathbf{C}^*, \times) .

1. Soit d un entier naturel qui n'est pas un carré parfait. Supposons que \sqrt{d} soit rationnel, alors l'ensemble $S = \{k \in \mathbf{N}^*; k\sqrt{d} \in \mathbf{N}\}$ est une partie non vide de \mathbf{N}^* . Notons m son plus petit élément. Le nombre $l = (\sqrt{d} - [\sqrt{d}])m$ est un entier non nul tel que $l\sqrt{d} = md - [\sqrt{d}]m\sqrt{d} \in \mathbf{N}$, donc $l \in S$. Or $l < m$, ce qui contredit la définition de m , donc \sqrt{d} est irrationnel.

Puisque \sqrt{p} est irrationnel, $G_4 \subset \mathbf{C}^*$. Soient $a + ib\sqrt{p} \in G_4$ et $a' + ib'\sqrt{p}$. On vérifie que

$$(a + ib\sqrt{p}) \times (a' + ib'\sqrt{p})^{-1} = \frac{aa' - bb'p}{a'^2 + b'^2p} + i \frac{a'b - ab'}{a'^2 + b'^2p} \sqrt{p} \in G_4.$$

12. L'énoncé comporte une petite erreur de frappe. La définition correcte de l'ensemble Γ_∞ est

$$\Gamma_\infty = \{z \in \mathbf{C}; \exists n \in \mathbf{N}^*, z^n = 1\}.$$

Il est clair que Γ_∞ est une partie non vide ($1 \in \Gamma_\infty$) de \mathbf{C}^* . Soit $(z, w) \in \Gamma_\infty^2$. Il existe $(n, m) \in \mathbf{N}^{*2}$ tel que $z^n = 1$ et $w^m = 1$. On a alors $nm \neq 0$ et $(zw^{-1})^{nm} = (z^n)^m (w^m)^{-n} = 1$, donc $zw^{-1} \in \Gamma_\infty$. Le théorème 1.24 permet de conclure que Γ_∞ est un sous-groupe de (\mathbf{C}^*, \times) .

Remarque. Notons que $\Gamma_\infty = \bigcup_{n \geq 1} U_n$ où U_n est le sous-groupe des racines n -ième de l'unité (exemple 1.30). Or nous savons que l'union d'une famille de sous-groupes n'est, en général, pas un sous-groupe (exemple 1.26). La famille $\{U_n\}_{n \geq 1}$ n'étant pas totalement ordonnée pour l'inclusion (par exemple, U_2 et U_3 ne sont pas comparables), la proposition 1.27 n'est pas applicable. En revanche, on vérifie facilement que pour tous entiers $n \geq 1$ et $m \geq 1$, on a $U_n \subseteq U_{mn}$ et $U_m \subseteq U_{mn}$. On dit que l'ensemble ordonné $(\{U_n\}_{n \geq 1}, \subseteq)$ est *filtrant à droite*. Cet exemple suggère une extension de la proposition 1.27 :

PROPOSITION. Soient G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G ordonnée par l'inclusion. Si pour tout $(i, j) \in I^2$, il existe $k \in I$ tel que $H_i \subseteq H_k$ et $H_j \subseteq H_k$, alors $\bigcup_{i \in I} H_i$ est un sous-groupe de G .

13. C'est un cas particulier du lemme 1.77 appliqué au groupe $(\mathbf{R}, +)$.

14. Pour tout $(x, y) \in \mathbf{R}^*$, on a

$$f(xy) = |xy| = |x||y| = f(x)f(y)$$

donc f est un homomorphisme de groupes. De plus

$$f(x) = 1 \iff |x| = 1 \iff x = 1 \text{ ou } x = -1$$

donc $\text{Ker}(f) = \{-1; +1\}$.

Pour tout $(z, w) \in \mathbf{C}^*$, on a

$$g(zw) = |zw| = |z||w| = g(z)g(w)$$

donc g est homomorphisme de groupes. De plus

$$g(z) = 1 \iff |z| = 1$$

donc $\text{Ker}(f) = \mathbf{U}$.

15. — Montrons que λ est un homomorphisme. Pour tout $(x, y) \in \mathbf{R}^2$,

$$\lambda(x + y) = 10^{x+y} = 10^x \times 10^y = \lambda(x)\lambda(y).$$

— λ est injective; en effet,

$$\lambda(x) = 1 \implies 10^x = 1 \implies x = 0.$$

— λ est surjective, car pour tout $y \in \mathbf{R}_+^*$,

$$\lambda(\log_{10} y) = y.$$

En conclusion, λ est un isomorphisme de groupes.

16. a) Tout élément de H qui commute avec tous ceux de G commute à fortiori avec tous ceux de H d'où $Z(G) \cap H \subset Z(H)$. De plus $Z(G) \cap H$ est un sous-groupe de G donc $Z(G) \cap H \leq Z(H)$.

b) Soit $y \in f(Z(G))$. Il existe $x \in Z(G)$ tel que $y = f(x)$. Comme f est surjective, pour tout $z \in G'$, il existe $w \in G$ tel que $z = f(w)$, et on a

$$zy = f(w)f(x) = f(wx) = f(xw) = f(x)f(w) = yz$$

d'où $y \in Z(G')$. Comme $f(Z(G))$ est un sous-groupe de G' inclus dans $Z(G')$, on conclut que $f(Z(G)) \leq Z(G')$.

17. a) Soit $g, h \in C_G(S)$. Pour tout $x \in S$, on a

$$(gh^{-1})x(gh^{-1})^{-1} = (gh^{-1})x(hg^{-1}) = g(h^{-1}xh)g^{-1} = gxg^{-1} = x.$$

Donc $gh^{-1} \in C_G(S)$ et $C_G(S)$ est un sous-groupe de G .

$$b) \quad g \in Z(G) \Leftrightarrow \forall x \in G, gx = xg \Leftrightarrow \forall x \in G, g \in C_G(x) \Leftrightarrow g \in \bigcap_{x \in G} C_G(x).$$

$$c) \quad H = C_G(x) \Leftrightarrow \forall h \in H, hx = xh \Leftrightarrow x \in Z(H).$$

18. Pour toute partie non vide S du groupe G , on note \mathcal{H}_S l'ensemble des sous-groupes de G contenant S . Nous savons que

$$H = \bigcap_{L \in \mathcal{H}_{A \cup B \cup C}} L \quad \text{et} \quad K = \bigcap_{L \in \mathcal{H}_{H \cup C}} L.$$

Montrons que $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$. Soit $L \in \mathcal{H}_{A \cup B \cup C}$. Comme $A \cup B \subseteq L$, nécessairement $H \subseteq L$ donc $L \in \mathcal{H}_{H \cup C}$. Réciproquement, soit $L \in \mathcal{H}_{H \cup C}$. On a $A \cup B \subseteq H \subseteq L$, donc $L \in \mathcal{H}_{A \cup B \cup C}$. Nous avons montré que $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$, ce qui nous permet de conclure que $K = \langle H, C \rangle$.

19. Rappelons que le groupe des quaternions Q_8 est l'ensemble des 8 matrices

$$\begin{aligned} q_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & q_2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, & q_3 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & q_4 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ q_5 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, & q_6 &= \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, & q_7 &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, & q_8 &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \end{aligned}$$

muni de la multiplication des matrices.

Montrons que $Q_8 = \langle A, B \rangle$. Comme $A \in Q_8$ et $B \in Q_8$, on a $\langle A, B \rangle \subseteq Q_8$. De plus, on vérifie que $q_1 = A^4$, $q_2 = A^2$, $q_3 = A$, $q_4 = A^3$, $q_5 = B$, $q_6 = B^3$, $q_7 = BA$ et $q_8 = AB$, donc $Q_8 \subseteq \langle A, B \rangle$.

20. Quel que soit $x \in \mathbf{R}^*$, notons M_x la matrice $\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}$. La multiplication des matrices s'écrit

$$M_x M_y = M_{xy} = M_{yx} = M_y M_x$$

pour tout $(x, y) \in \mathbf{R}^{*2}$. Il s'ensuit que la multiplication des matrices définit une loi interne commutative sur l'ensemble Γ . Nous savons déjà que cette loi est associative. Elle admet pour élément neutre la matrice M_1 , de plus toute matrice M_x est inversible d'inverse $M_{x^{-1}}$, en effet $M_x M_{x^{-1}} = M_{x x^{-1}} = M_1$. Nous avons montré que l'ensemble Γ muni de la multiplication des matrices est un groupe abélien.

Le groupe Γ n'est pas un sous-groupe de $GL(2, \mathbf{R})$; en effet, les matrices M_x ont un déterminant nul et donc ne sont pas inversibles dans $GL(2, \mathbf{R})$.

Montrons que les groupes Γ et (\mathbf{R}^*, \times) sont isomorphes. Soit l'application $\varphi: \Gamma \rightarrow \mathbf{R}^*$ définie par $\varphi(M_x) = x$. L'application φ est un morphisme de groupes. En effet, pour tout $(M_x, M_y) \in \Gamma^2$, on a

$$\varphi(M_x M_y) = \varphi(M_{xy}) = xy = \varphi(M_x)\varphi(M_y).$$

Le morphisme φ est injectif, car $\varphi(M_x) = 1$ implique $x = 1$ c'est-à-dire $M_x = M_1$. Enfin, le morphisme φ est surjectif, car pour tout $x \in \mathbf{R}^*$, on a $\varphi(M_x) = x$. On conclut que φ est un isomorphisme de groupes, donc que les groupes Γ et (\mathbf{R}^*, \times) sont isomorphes.

21. a) *La correspondance μ est une application.*

Soient $(x, x', y, y') \in \mathbf{Z}^4$. L'identité

$$x'y' - xy = x'(y' - y) + y(x' - x)$$

montre que si n divise $x' - x$ et $y' - y$, alors n divise $x'y' - xy$. Autrement dit, si $\bar{x} = x'$ et $\bar{y} = y'$, alors $\overline{x'y'} = \overline{xy}$.

$\frac{\mathbf{Z}}{(n)}$ est un anneau unitaire commutatif.

La multiplication dans $\frac{\mathbf{Z}}{(n)}$ est associative: quels que soient $\bar{x}, \bar{y}, \bar{z}$ dans $\frac{\mathbf{Z}}{(n)}$, on a

$$(\bar{x} \bar{y}) \bar{z} = \overline{xy} \bar{z} = \overline{(xy)z} = \overline{x(yz)} = \bar{x} \overline{yz} = \bar{x} (\bar{y} \bar{z}).$$

La multiplication est commutative: quels que soient \bar{x}, \bar{y} dans $\frac{\mathbf{Z}}{(n)}$, on a

$$\bar{x} \bar{y} = \overline{xy} = \overline{yx} = \bar{y} \bar{x}.$$

La multiplication est distributive par rapport à l'addition: quels que soient $\bar{x}, \bar{y}, \bar{z}$ dans $\frac{\mathbf{Z}}{(n)}$, on a

$$\bar{x} (\bar{y} + \bar{z}) = \bar{x} \overline{y+z} = \overline{x(y+z)} = \overline{xy+xz} = \overline{xy} + \overline{xz} = \bar{x} \bar{y} + \bar{x} \bar{z}.$$

La multiplication admet un élément neutre: quel que soit \bar{x} dans $\frac{\mathbf{Z}}{(n)}$, on a

$$\bar{x} \bar{1} = \overline{x \times 1} = \bar{x}.$$

- b) L'ensemble G_p est fini et nous avons déjà démontré que la multiplication est associative. Soient \bar{a} , \bar{x} et \bar{y} trois éléments de G_p tels que $\bar{a} \bar{x} = \bar{a} \bar{y}$. Alors $\overline{ax} = \overline{ay}$, donc p divise $a(x - y)$. Or p ne divise pas a puisque $\bar{a} \neq \bar{0}$, donc p divise $x - y$ ce qui signifie que $\bar{x} = \bar{y}$. Nous en déduisons que la multiplication est simplifiable à gauche. Elle est commutative, donc elle est également simplifiable à droite. D'après le résultat de l'exercice 4, l'ensemble G_p muni de la multiplication définie dans $\frac{\mathbf{Z}}{(p)}$ est un groupe. Par conséquent tout élément non nul de $\frac{\mathbf{Z}}{(p)}$ est inversible, d'où nous concluons que $\frac{\mathbf{Z}}{(p)}$ est un corps.
- c) Supposons n non premier. Il existe deux entiers $k > 1$ et $l > 1$ tels que $n = kl$. Alors $\bar{k} \bar{l} = \bar{n} = \bar{0}$ avec $\bar{k} \neq \bar{0}$ et $\bar{l} \neq \bar{0}$, donc \bar{k} n'est pas inversible: $\frac{\mathbf{Z}}{(n)}$ n'est pas un corps.

22. L'ensemble Γ est un sous-groupe de $GL(2, \mathbf{R})$. Soient I la matrice identité de dimension 2 et A la matrice

$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Notons A_x la matrice obtenue en permutant les colonnes de A , A_y la matrice obtenue en permutant les lignes de A et A_{xy} la matrice obtenue en permutant les colonnes et les lignes de A , ainsi

$$\Gamma = \{I, A, I_x, A_x, A_y, A_{xy}\}.$$

Comme $\det(A) \neq 0$, et que permuter les lignes ou les colonnes d'une matrice conserve le déterminant au signe près, nous en déduisons que $\Gamma \subset GL(2, \mathbf{R})$. Posons $H = \langle A \rangle = \{I, A, A_{xy}\}$ et $K = \langle A_y \rangle = \{I, A_y\}$. Ce sont deux sous-groupes de $GL(2, \mathbf{R})$. On vérifie que $AA_y = I_x$, $A_yA = A_x$, $A_{xy}A_y = A_x$ et $A_yA_{xy} = I_x$, d'où $HK = KH = \Gamma$. La proposition 1.47 nous permet alors de conclure que Γ est un sous-groupe de $GL(2, \mathbf{R})$.

Les groupes Γ et $\text{GL}\left(2, \frac{\mathbf{Z}}{(2)}\right)$ sont isomorphes. Pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, notons \bar{M} la matrice $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$. On vérifie que

$$\det(\bar{M}) = \bar{a}\bar{d} - \bar{b}\bar{c} = \overline{ad - bc} = \overline{\det(M)} = \bar{1} \neq \bar{0},$$

nous pouvons donc définir l'application

$$\begin{aligned} \varphi: \Gamma &\rightarrow \text{GL}\left(2, \frac{\mathbf{Z}}{(2)}\right) \\ M &\mapsto \bar{M}. \end{aligned}$$

L'application φ est un homomorphisme de groupes : soient

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad N = \begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

alors

$$\begin{aligned} \varphi(MN) &= \varphi\left(\begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}\right) \\ &= \begin{pmatrix} \overline{ae + bg} & \overline{af + bh} \\ \overline{ce + dg} & \overline{cf + dh} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a}\bar{e} + \bar{b}\bar{g} & \bar{a}\bar{f} + \bar{b}\bar{h} \\ \bar{c}\bar{e} + \bar{d}\bar{g} & \bar{c}\bar{f} + \bar{d}\bar{h} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{e} & \bar{f} \\ \bar{g} & \bar{h} \end{pmatrix} \\ &= \varphi(M)\varphi(N). \end{aligned}$$

L'application φ est injective : soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, alors $M \in \text{Ker}(\varphi)$ si et seulement si $a \in \{-1, 1\}$, $b = 0$, $c = 0$ et $d \in \{-1, 1\}$, d'où $\text{Ker}(\varphi) = I$.

L'application φ est surjective : les matrices de $\text{GL}\left(2, \frac{\mathbf{Z}}{(2)}\right)$ sont celles dont les vecteurs colonnes sont $\frac{\mathbf{Z}}{(2)}$ -linéairement indépendants. Nous trouvons

$$\text{GL}\left(2, \frac{\mathbf{Z}}{(2)}\right) = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\}.$$

L'application φ est une injection entre deux groupes de même cardinal, donc elle est bijective.

À l'aide de la proposition 1.66 nous concluons que φ est un isomorphisme.

Les groupes Γ et S_3 sont isomorphes. Les tables de multiplication des groupes Γ et S_3 sont écrites ci-dessous :

\times	I	A	A_{xy}	A_x	I_x	A_y
I	I	A	A_{xy}	A_x	I_x	A_y
A	A	A_{xy}	I	A_y	A_x	I_x
A_{xy}	A_{xy}	I	A	I_x	A_y	A_x
A_x	A_x	I_x	A_y	I	A	A_{xy}
I_x	I_x	A_y	A_x	A_{xy}	I	A
A_y	A_y	A_x	I_x	A	A_{xy}	I

\times	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

Soit $g: \Gamma \rightarrow S_3$ la bijection définie par

$$\begin{aligned} g(I) &= e, & g(A) &= \sigma_1, & g(A_{xy}) &= \sigma_2, \\ g(A_x) &= \tau_1, & g(I_x) &= \tau_2, & g(A_y) &= \tau_3. \end{aligned}$$

Si nous identifions chaque élément de Γ avec son image dans S_3 par l'application g , alors nous constatons que les tables de multiplication des groupes Γ et S_3 sont identiques; cela signifie que les groupes Γ et S_3 sont isomorphes.

23. a) Les ensembles Γ_1 , Γ_2 et Γ_3 sont non vides et $\Gamma_1 \subseteq GL(2, \mathbf{R})$, $\Gamma_2 \subset \mathbf{C}^*$ et $\Gamma_3 \subseteq \frac{\mathbf{Z}}{(5)}$. Pour vérifier la stabilité par rapport à la multiplication et à l'inverse, construisons leurs tables de Cayley.

Posons $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ et $C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ de sorte que $\Gamma_1 = \{I, A, B, C\}$. Sa table de Cayley est :

\times	I	A	B	C
I	I	A	B	C
A	A	B	C	I
B	B	C	I	A
C	C	I	A	B

Les tables de Cayley de Γ_2 et Γ_3 sont les suivantes :

\times	1	i	-1	-i	\times	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
1	1	i	-1	-i	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
i	i	-1	-i	1	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
-1	-1	-i	1	i	$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
-i	-i	1	i	-1	$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Nous en déduisons que Γ_1 est un sous-groupe de $GL(2, \mathbf{R})$, Γ_2 un sous-groupe de (\mathbf{C}^*, \times) et Γ_3 un sous-groupe de $\frac{\mathbf{Z}}{5}$.

- b) En identifiant chaque élément du groupe Γ_1 à son image dans le groupe Γ_2 par la bijection $f: \Gamma_1 \rightarrow \Gamma_2$ définie par $f(I) = 1$, $f(A) = i$, $f(B) = -1$ et $f(C) = -i$, nous constatons que la table de Cayley du groupe Γ_1 est la même que celle du groupe Γ_2 . Nous en déduisons que les groupes Γ_1 et Γ_2 sont isomorphes.

De même, on montre que les groupes Γ_1 et Γ_3 sont isomorphes à l'aide de la bijection $g: \Gamma_1 \rightarrow \Gamma_3$ définie par $g(I) = \bar{1}$, $g(A) = \bar{2}$, $g(B) = \bar{4}$ et $g(C) = \bar{3}$.

De ce qui précède, nous déduisons que Γ_1 est isomorphe à Γ_3 (remarque 1.71).

Remarquons que $\Gamma_1 = \langle A \rangle$, $\Gamma_2 = \langle i \rangle$ et $\Gamma_3 = \langle \bar{2} \rangle$, donc les groupes Γ_1 , Γ_2 et Γ_3 sont cycliques.

24. a) Démontrons que K_1 est un sous-groupe de $GL(2, \mathbf{R})$.

Pour tout $(a, b) \in \{-1, 1\}^2$, posons

$$M_{a,b} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

et notons I_2 la matrice unité $M_{1,1}$. Ainsi

$$K_1 = \{I_2, M_{1,-1}, M_{-1,1}, M_{-1,-1}\}.$$

Soit $(a, a', b, b') \in \{-1, 1\}^4$. On a

$$M_{a,b}M_{a',b'} = M_{aa',bb'} \quad \text{avec} \quad (aa', bb') \in \{-1, 1\}^2,$$

donc

$$M_{a,b}M_{a',b'} \in K_1.$$

On vérifie que $M_{a,b}^2 = I_2$, donc

$$M_{a,b}^{-1} = M_{a,b} \in K_1.$$

L'ensemble K_1 est donc un sous-groupe de $GL(2, \mathbf{R})$.

Démontrons que K_2 est un groupe.

Soit \bar{x} et \bar{y} deux éléments de K_2 avec $(x, y) \in \{1, 3, 5, 7\}^2$. Le produit xy est impair et 8 est pair, donc les représentants de \overline{xy} sont impairs. On en déduit que $\bar{x} \cdot \bar{y} = \overline{xy} \in K_2$, donc le produit définit une loi interne sur K_2 . On sait que $\frac{\mathbf{Z}}{(8)}$ est un anneau, donc le produit est associatif. L'élément unité est $\bar{1}$. De plus, pour tout $\bar{x} \in K_2$, on a $\bar{x}^2 = \bar{1}$, donc $\bar{x}^{-1} = \bar{x} \in K_2$. Nous avons ainsi démontré que K_2 est un groupe multiplicatif.

b) Démontrons que les groupes K_1 et K_2 sont isomorphes.

Écrivons les tables de Cayley des groupes K_1 et K_2 .

\times	I_2	$M_{1,-1}$	$M_{-1,1}$	$M_{-1,-1}$
I_2	I_2	$M_{1,-1}$	$M_{-1,1}$	$M_{-1,-1}$
$M_{1,-1}$	$M_{1,-1}$	I_2	$M_{-1,-1}$	$M_{-1,1}$
$M_{-1,1}$	$M_{-1,1}$	$M_{-1,-1}$	I_2	$M_{1,-1}$
$M_{-1,-1}$	$M_{-1,-1}$	$M_{-1,1}$	$M_{1,-1}$	I_2

\times	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Renommons les éléments de la table de Cayley du groupe K_1 à l'aide de la bijection $\varphi: K_1 \rightarrow K_2$ définie par

$$\varphi(I_2) = \bar{1}, \quad \varphi(M_{1,-1}) = \bar{3}, \quad \varphi(M_{-1,1}) = \bar{5} \quad \text{et} \quad \varphi(M_{-1,-1}) = \bar{7}.$$

En d'autres termes, remplaçons x par $\varphi(x)$ pour tout $x \in K_1$. Nous obtenons ainsi la même table de Cayley que celle de K_2 . Cela nous permet de conclure que les groupes K_1 et K_2 sont isomorphes.

Démontrons que K_1 et K_2 sont isomorphes au groupe de Klein.

Étant donné que K_1 et K_2 sont isomorphes, il suffit de démontrer que K_2 est isomorphe au groupe de Klein. Posons $H_1 = \{\bar{1}, \bar{3}\}$ et $H_2 = \{\bar{1}, \bar{5}\}$. Ce sont deux sous-groupes de K_2 tel que $H_1 \simeq \frac{\mathbf{Z}}{(2)}$ et $H_2 \simeq \frac{\mathbf{Z}}{(2)}$. Comme $\bar{3} \times \bar{5} = \bar{7}$, on a $K_2 = H_1 H_2$. De plus $H_1 \cap H_2 = \{\bar{1}\}$. La proposition 1.85 nous permet de conclure que

$$K_2 \simeq \frac{\mathbf{Z}}{(2)} \times \frac{\mathbf{Z}}{(2)}.$$

25. a) Nous avons montré que le groupe S_3 est isomorphe au sous-groupe Γ de $GL(2, \mathbf{R})$. Soit φ un isomorphisme entre S_3 et Γ . L'application $\rho: S_3 \rightarrow GL(2, \mathbf{R})$ définie par $\rho(x) = \varphi(x)$ pour tout $x \in S_3$ est une représentation matricielle fidèle de S_3 de degré 2 sur \mathbf{R} .

De même, les groupes Γ_2 , Γ_3 et K_2 admettent chacun une représentation matricielle fidèle de degré 2 sur \mathbf{R} .

- b) Puisque que pour tout $a + ib \in \mathbf{C}^*$, la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ a un déterminant $a^2 + b^2$ non nul, l'application $\rho: \mathbf{C}^* \rightarrow GL(2, \mathbf{R})$ telle que

$$\rho(a + ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

est donc bien définie. Cette application est un homomorphisme de groupe; en effet, pour tous nombres complexes non nuls $z = a + ib$ et $w = c + id$, nous avons

$$\rho(zw) = \rho(ac - db + i(ad + bc)) = \begin{pmatrix} ac - db & -ad - bc \\ ad + bc & ac - bd \end{pmatrix}$$

et

$$\rho(z)\rho(w) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -ad - bc \\ bc + ad & -db + ac \end{pmatrix}.$$

De plus, il est immédiat que $\text{Ker } \rho = \{0\}$.

Nous en déduisons que ρ est une représentation matricielle fidèle de degré 2 sur \mathbf{R} du groupe multiplicatif \mathbf{C}^* .

27. a) Soit f l'homographie de paramètre (a, b, c, d) . L'application de paramètre $(d, -b, -c, a)$ est une homographie telle que $f \circ g = g \circ f = \text{id}_{\mathbb{C}}$, donc $f \in S_{\mathbb{C}}$.

b) L'ensemble \mathcal{H} n'est pas vide et comme nous venons de le voir, il est stable par passage à l'inverse. De plus, si f est l'homographie de paramètre (a, b, c, d) et g l'homographie de paramètre $(\alpha, \beta, \gamma, \delta)$, alors

$$(f \circ g)(z) = \frac{(\alpha a + b\gamma)z + a\beta + b\delta}{(c\alpha + d\gamma)z + c\beta + d\delta}$$

où $(\alpha a + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) = (ad - bc)(\alpha\delta - \beta\gamma) \neq 0$, ainsi \mathcal{H} est stable pour la composition. Finalement, \mathcal{H} est un sous-groupe de $S_{\mathbb{C}}$.

c) Les homographies telles que $c = 0$ sont les applications de la forme $z \mapsto az + b$ avec $a \neq 0$. On reconnaît là l'expression complexe d'une similitude directe. Le groupe des similitudes directes du plan complexes, qui inclut les translations, est donc un sous-groupe de \mathcal{H} .

d) L'égalité

$$\frac{1}{z} = \overline{\left(\frac{1}{\bar{z}}\right)}$$

montre que l'homographie $z \mapsto 1/z$ est la composée de l'inversion $z \mapsto 1/\bar{z}$ de centre O et de puissance 1 avec la symétrie $z \mapsto \bar{z}$ par rapport à l'axe (Ox).

e) Soit l'homographie f de paramètre (a, b, c, d) . Si $c = 0$, alors f est une similitude directe, donc elle conserve les angles orientés. Supposons $c \neq 0$. De

$$az + b = \frac{a}{c}(cz + d) - \frac{ad - bc}{c}$$

on tire

$$f(z) = -\frac{ad-bc}{c^2} \frac{1}{z - \frac{d}{c}} + \frac{a}{c}.$$

Avec le résultat de la question c), nous en déduisons la décomposition $f = s \circ r \circ i \circ t$ où t est la translation $z \mapsto z - \frac{d}{c}$, i est l'inversion $z \mapsto \frac{1}{\bar{z}}$, r est la réflexion $z \mapsto \bar{z}$ et s est la similitude directe $z \mapsto -\frac{ad-bc}{c^2}z + \frac{a}{c}$. Les applications s , r , i et t conservent les angles, s et t préservant l'orientation, r et i changeant l'orientation; il s'ensuit que les homographies conservent les angles orientés.

- f) Posons $K = \{f_1, f_2, f_3, f_4\}$. L'homographie f_1 est l'identité, $f_i \circ f_i = f_1$ pour tout i , $f_2 \circ f_3 = f_3 \circ f_2 = f_4$, $f_2 \circ f_4 = f_4 \circ f_2 = f_3$ et $f_3 \circ f_4 = f_4 \circ f_3 = f_2$. L'ensemble K est stable pour l'inverse et le produit, c'est donc un sous-groupe de \mathcal{H} .

Considérons les sous-groupes $K_1 = \langle f_2 \rangle$ et $K_2 = \langle f_4 \rangle$. Alors $K_1 \simeq \frac{\mathbb{Z}}{(2)}$, $K_2 \simeq \frac{\mathbb{Z}}{(2)}$, $K_1 \cap K_2 = \{f_1\}$, $K_1 K_2 = K_2 K_1$ puisque K est abélien, et $K_1 K_2 = K$. La proposition 1.85 permet d'en déduire que le groupe K est isomorphe au groupe de Klein $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$.

- g) Posons $L = \{g_1, g_2, g_3, g_4, g_5, g_6\}$. Construisons la table de Cayley de l'ensemble (L, \circ) .

\circ	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_3	g_1	g_6	g_4	g_5
g_3	g_3	g_1	g_2	g_5	g_6	g_4
g_4	g_4	g_5	g_6	g_1	g_2	g_3
g_5	g_5	g_6	g_4	g_3	g_1	g_2
g_6	g_6	g_4	g_5	g_2	g_3	g_1

Elle montre que L est stable pour la composition et le passage à l'inverse, par conséquent L est un sous-groupe de \mathcal{H} .

En identifiant les éléments de S_3 (exemple 1.18) avec ceux de L via la bijection

$$e \mapsto g_1, \quad \tau_1 \mapsto g_4, \quad \tau_2 \mapsto g_5, \quad \tau_3 \mapsto g_6, \quad \sigma_1 \mapsto g_2, \quad \sigma_2 \mapsto g_3,$$

on constate que les tables de Cayley de S_3 (exemple 1.18) et de L sont identiques. Nous en déduisons que les groupes S_3 et L sont isomorphes.

- 28.** a) Raisonnons par récurrence sur l'entier n . La propriété est vraie pour $n = 2$ (proposition 1.47). Supposons la propriété vraie pour un entier $n \geq 2$. Soient $\{H_i\}_{1 \leq i \leq n+1}$ une famille de sous-groupes de G telle que $H_i H_j = H_j H_i$ pour tout (i, j) tel que $1 \leq i < j \leq n+1$. D'après l'hypothèse de récurrence, $H_1 H_2 \dots H_n$ est un sous-groupe de G . De plus, on a $(H_1 H_2 \dots H_n) H_{n+1} = H_{n+1} (H_1 H_2 \dots H_n)$ puisque $H_i H_{n+1} = H_{n+1} H_i$ pour tout $1 \leq i \leq n$. La proposition 1.47 nous permet alors de conclure que $H_1 H_2 \dots H_{n+1}$ est un sous-groupe de G .
- b) Supposons que $\sum_{i=1}^n H_i$ soit une somme directe. Soient $z \in \sum_{i=1}^n H_i$ et deux familles d'éléments de G presque tous nuls $\{x_i\}_{i \in I}$ et $\{y_i\}_{i \in I}$ telles que $(x_i, y_i) \in H_i^2$ pour tout $i \in I$ et

$$z = \sum_{i \in I} x_i = \sum_{i \in I} y_i.$$

Pour tout $j \in I$, on a

$$x_j - y_j = - \sum_{\substack{i \in I \\ i \neq j}} (x_i - y_i),$$

d'où

$$x_j - y_j = H_j \cap \sum_{\substack{i \in I \\ i \neq j}} H_i = \{0\},$$

donc $x_j = y_j$ et la décomposition de z est unique.

Réciproquement, supposons que tout $z \in \sum_{i \in I} H_i$ s'écrit de manière unique

$$z = \sum_{i \in I} x_i$$

où les $x_i \in H_i$ sont presque tous nuls. Soient $j \in J$ et $z \in H_j \cap \sum_{i \in I, i \neq j} H_i$. On peut écrire

$$z = \underbrace{z}_{z \in H_j} + \underbrace{0}_{0 \in \sum_{i \neq j} H_i} = \underbrace{0}_{0 \in H_j} + \underbrace{z}_{z \in \sum_{i \neq j} H_i}.$$

L'unicité de la décomposition implique que $z = 0$, d'où $H_j \cap \sum_{i \in I, i \neq j} H_i$.

29. Il est clair que la loi de composition ainsi définie est une loi interne. Montrons qu'elle est associative. Soit $f, g, h \in G^E$. Pour tout $x \in E$, on a :

$$\begin{aligned} (f(gh))(x) &= f(x)(gh)(x) \\ &= f(x)(g(x)h(x)) \\ &= (f(x)g(x))h(x) \\ &= (fg)(x)h(x) \\ &= ((fg)h)(x) \end{aligned}$$

d'où $f(gh) = (fg)h$.

Montrons l'existence d'un élément neutre. Soit $j \in G^E$ définie pour tout $x \in E$ par $j(x) = e$. Alors pour tout $x \in E$, on a $(fj)(x) = f(x)j(x) = f(x) = j(x)f(x) = (jf)(x)$ d'où $jf = f = fj$.

Reste à montrer que toute $f \in G^E$ est inversible. On définit $g \in G^E$ par $g(x) = f(x)^{-1}$ pour tout $x \in E$. On a $(fg)(x) = f(x)g(x) = f(x)f(x)^{-1} = e = j(x)$ i.e. $fg = j$. On montre de même que $gf = j$.

Finalement, G^E est un groupe.

On suppose que G est abélien. Soit $f, g \in G^E$. Pour tout $x \in E$, on a $f(x)g(x) = g(x)f(x)$ c'est-à-dire $fg = gf$; G^E est abélien. Réciproquement, supposons que G^E est abélien. Soit $a, b \in G$, et $f, g \in G^E$ deux applications constantes égales à a et b respectivement. Pour tout $x \in E$, nous avons $ab = f(x)g(x) = (fg)(x) = (gf)(x) = g(x)f(x) = ba$.

30. a) — L'ensemble $\mathcal{C}(J)$ n'est pas vide (il contient les fonctions constantes) et la différence de deux fonctions continues sur J est une fonction continue sur J , donc $\mathcal{C}(J)$ est un sous-groupe de $(\mathbf{R}^J, +)$.

— L'ensemble Γ est non vide, $\Gamma \subseteq \mathcal{C}(J)$ car les fonctions constantes de \mathbf{R}^J sont continues, et, pour tous réels a et b , on a $c_a - c_b = c_{a-b}$, donc Γ est bien un sous-groupe de $(\mathcal{C}(J), +)$.

b) F_1 est un morphisme de groupes. En effet, pour tout $(f, g) \in \mathcal{C}(J)$, on a $F_1(f + g) = (f + g)(1) = f(1) + g(1) = F_1(f) + F_1(g)$.

F_2 n'est pas un morphisme de groupes. En effet, $F_2(c_{-2} + c_1) = F_2(c_1) = |c_1(0)| = 1$ et $F_2(c_{-2}) + F_2(c_1) = |c_{-2}(0)| + |c_1(0)| = 2 + 1 = 3$.

F_3 est un morphisme de groupes. C'est une conséquence de la linéarité de l'intégrale.

F_4 est un morphisme de groupes. C'est une conséquence de la linéarité de l'intégrale.

F_5 n'est pas un morphisme de groupes. L'élément neutre du groupe $\mathcal{C}(J)$ est c_0 . Si F_5 était un morphisme de groupes, on aurait $F_5(c_0) = 0$ (proposition 1.55), or $F_5(c_0) = 1$.

Vérifier que $F_1(c_a) = a$, $F_3(c_a) = a$ et $F_4(c_a) = a$ pour tout $a \in \mathbf{R}$ est trivial.

Pour tout $i \in \{1, 3, 4\}$, on a $F_i(\text{id}_J - c_{m_i}) = F_i(\text{id}_J) - F_i(c_{m_i}) = F_i(\text{id}_J) - m_i$. Ainsi $m_i = F_i(\text{id}_J)$ est l'unique réel tel que $F_i(\text{id}_J - c_{m_i}) = 0$. On trouve $m_1 = 1$, $m_3 = 1/2$ et $m_4 = 1 + (6\sqrt{3} - 12)/\pi$. Comme m_1 , m_3 et m_4 sont deux à deux distincts, ce qui précède permet de conclure que $\text{Ker}F_1$, $\text{Ker}F_3$ et $\text{Ker}F_4$ sont deux à deux distincts.

c) Soit $F \in \text{Hom}(\mathcal{C}(J), \mathbf{R})$ tel que $F(c_a) = a$ pour tout $a \in \mathbf{R}$.

Tout $f \in \mathcal{C}(J)$ peut s'écrire $f = (f - c_{F(f)}) + c_{F(f)}$ où $c_{F(f)} \in \Gamma$ et $f - c_{F(f)} \in \text{Ker}F$ car $F(f - c_{F(f)}) = F(f) - F(c_{F(f)}) = F(f) - F(f) = 0$. Ainsi $\mathcal{C}(J) = (\text{Ker}F) + \Gamma$.

Soit $f \in \mathcal{C}(J) \cap \Gamma$. Il existe $a \in \mathbf{R}$ tel que $f = c_a$ et $F(c_a) = 0$. Or $F(c_a) = a$, donc $a = 0$. Il s'ensuit que $\text{Ker}F \cap \Gamma = \{c_0\}$, la fonction c_0 étant l'élément neutre du groupe $\mathcal{C}(J)$.

Nous avons démontré que $\mathcal{C}(J) = \text{Ker}F \oplus \Gamma$.

On a $\mathcal{C}(J) = H \oplus \Gamma$ pour tout sous-groupe $H \in \{\text{Ker}F_1, \text{Ker}F_3, \text{Ker}F_4\}$, mais trois choix pour H , cela n'est pas assez pour justifier l'usage de l'adjectif *nombreux*. Heureusement, nous allons en construire d'autres en nous inspirant de ceux déjà trouvés. Par exemple, nous pouvons considérer les morphismes $F_\alpha: f \mapsto f(\alpha)$ où $\alpha \in \mathbf{R}$ pour lesquels nous avons bien $F_\alpha(c_a) = a$ pour tout $a \in \mathbf{R}$ et $m_\alpha = F_\alpha(\text{id}_J) = \alpha$, donc $\mathcal{H} = \{\text{Ker}F_\alpha\}_{\alpha \in \mathbf{R}}$ est une famille infinie de sous-groupes deux à deux distincts telle que $\mathcal{C}(J) = H \oplus \Gamma$ pour tout $H \in \mathcal{H}$.

31. a) L'application $\varphi: G_1 \times G_2 \rightarrow G_2 \times G_1$ définie par $\varphi(g_1, g_2) = (g_2, g_1)$

est:

- *un homomorphisme*: en effet, pour tous éléments (g_1, g_2) et (h_1, h_2) de $G_1 \times G_2$, on a

$$\begin{aligned}\varphi((g_1, g_2)(h_1, h_2)) &= \varphi(g_1 h_1, g_2 h_2) \\ &= (g_2 h_2, g_1 h_1) \\ &= (g_2, g_1)(h_2, h_1) \\ &= \varphi(g_1, g_2)\varphi(h_1, h_2).\end{aligned}$$

- *une bijection*: pour tout élément (g_2, g_1) de $G_2 \times G_1$, on a $\varphi(g_1, g_2) = (g_2, g_1)$.

D'après la proposition 1.66, les groupes $G_1 \times G_2$ et $G_2 \times G_1$ sont isomorphes.

- b) Soient $\varphi_i : \Gamma_i \rightarrow G_i$ ($i = 1, 2$) des isomorphismes et

$$\varphi : \Gamma_1 \times \Gamma_2 \rightarrow G_1 \times G_2$$

l'application définie par $\varphi(g_1, g_2) = (\varphi_1(g_1), \varphi_2(g_2))$.

- *φ est un homomorphisme*: pour tous éléments (g_1, g_2) et (h_1, h_2) de $\Gamma_1 \times \Gamma_2$, on a

$$\begin{aligned}\varphi((g_1, g_2)(h_1, h_2)) &= \varphi(g_1 h_1, g_2 h_2) \\ &= (\varphi_1(g_1 h_1), \varphi_2(g_2 h_2)) \\ &= (\varphi_1(g_1)\varphi_1(h_1), \varphi_2(g_2)\varphi_2(h_2)) \\ &= (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(h_1), \varphi_2(h_2)) \\ &= \varphi(g_1, g_2)\varphi(h_1, h_2).\end{aligned}$$

- *φ est bijective*: c'est une conséquence de $\text{Im } \varphi = \text{Im } \varphi_1 \times \text{Im } \varphi_2$ et $\text{Ker } \varphi = \text{Ker } \varphi_1 \times \text{Ker } \varphi_2$.

Conclusion: les groupes $\Gamma_1 \times \Gamma_2$ et $G_1 \times G_2$ sont isomorphes.

- c) Contrairement à ce qu'affirme l'énoncé, tout sous-groupe d'un produit direct $G_1 \times G_2$ n'est pas de la forme $H_1 \times H_2$ où H_i ($i = 1, 2$)

est un sous-groupe de G_i . Par exemple, considérons le groupe de Klein $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$. Les seuls sous-groupes de $\frac{\mathbb{Z}}{(2)}$ sont $\{\bar{0}\}$ et $\frac{\mathbb{Z}}{(2)}$. On voit donc que le sous-groupe $\{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$ de $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$ n'est pas le produit direct de deux sous-groupes de $\frac{\mathbb{Z}}{(2)}$.

32. Soit G_1 et G_2 deux groupes isomorphes et $f: G_1 \rightarrow G_2$ un isomorphisme.

a) On définit un morphisme de groupes $f_{\#}: \text{Aut}(G_1) \rightarrow \text{Aut}(G_2)$ en posant $f_{\#}(\psi) = f \circ \psi \circ f^{-1}$. En effet pour tout $\psi_1, \psi_2 \in \text{Aut}(G_1)$ on a :

$$\begin{aligned} f_{\#}(\psi_1 \circ \psi_2) &= f \circ (\psi_1 \circ \psi_2) \circ f^{-1} \\ &= (f \circ \psi_1 \circ f^{-1}) \circ (f \circ \psi_2 \circ f^{-1}) \\ &= f_{\#}(\psi_1) \circ f_{\#}(\psi_2) \end{aligned}$$

De plus si $\psi \in \text{Aut}(G_1)$,

$$\begin{aligned} f_{\#}(\psi) = \text{id}_{G_2} &\iff f \circ \psi \circ f^{-1} = \text{id}_{G_2} \\ &\iff \psi = f^{-1} \circ \text{id}_{G_2} \circ f \\ &\iff \psi = \text{id}_{G_1} \end{aligned}$$

et si $\psi \in \text{Aut}(G_2)$, on a $f^{-1} \circ \psi \circ f \in \text{Aut}(G_1)$ et

$$f_{\#}(f^{-1} \circ \psi \circ f) = f \circ (f^{-1} \circ \psi \circ f) \circ f^{-1} = \text{id}_{G_2} \circ \psi \circ \text{id}_{G_2} = \psi$$

Donc $f_{\#}$ est un isomorphisme de groupes et $\text{Aut}(G_1) \simeq \text{Aut}(G_2)$.

b) Si $\sigma_g \in \text{Int}(G_1)$, alors pour tout $x \in G_2$,

$$\begin{aligned} [f_{\#}(\sigma_g)](x) &= (f \circ \sigma_g \circ f^{-1})(x) \\ &= f(g f^{-1}(x) g^{-1}) \\ &= f(g) x f(g)^{-1} \\ &= \sigma_{f(g)}(x) \end{aligned}$$

c'est-à-dire $f_{\#}(\sigma_g) = \sigma_{f(g)} \in \text{Aut}(G_2)$ ou encore $f_{\#}(\text{Int}(G_1)) \subset \text{Int}(G_2)$. Ainsi on définit un homomorphisme de groupes $f_*: \text{Int}(G_1) \rightarrow$

$\text{Int}(G_2)$ en posant $f_* = f_{\#} \uparrow_{\text{Int}(G_1)}^{\text{Int}(G_2)}$. Il est injectif (comme $f_{\#}$) et est aussi surjectif, en effet si $\sigma_g \in \text{Int}(G_2)$, alors $f_*(\sigma_{f^{-1}(g)}) = \sigma_{f(f^{-1}(g))} = \sigma_g$. Donc f_* est un isomorphisme de groupes et $\text{Int}(G_1) \simeq \text{Int}(G_2)$.

33. La propriété universelle du produit direct (théorème 1.91) affirme que l'application

$$\begin{aligned} \varphi: \text{Hom}\left(G, \prod_{i \in I} G_i\right) &\rightarrow \prod_{i \in I} \text{Hom}(G, G_i) \\ h &\mapsto (p_i \circ h)_{i \in I}. \end{aligned}$$

est une bijection, donc les ensembles $\text{Hom}(G, \prod_{i \in I} G_i)$ et $\prod_{i \in I} \text{Hom}(G, G_i)$ sont équipotents.

Classes modulo un sous-groupe

1. Il est clair que $H \cap K \leq H$ et $H \cap K \leq K$ donc d'après le théorème de Lagrange on a $o(H \cap K) \mid o(H)$ et $o(H \cap K) \mid o(K)$. On en déduit que $o(H \cap K) \mid \text{pgcd}(o(H), o(K)) = \text{pgcd}(p, q) = 1$ puis que $o(H \cap K) = 1$ donc $H \cap K = (e)$.

2. a) — Supposons que $Kx_i = Kx_j$, où $(i, j) \in I^2$. Alors $x_i x_j^{-1} \in K$ et comme $(x_i, x_j) \in H^2$ on a aussi $x_i x_j^{-1} \in H$ d'où $x_i x_j^{-1} \in H \cap K$, c'est-à-dire $(H \cap K)x_i = (H \cap K)x_j$. Par définition de la famille $\{x_i\}_{i \in I}$, on a $i = j$. En conclusion : $Kx_i = Kx_j \iff i = j$. On en déduit que $\{x_i\}_{i \in I}$ est aussi une famille de représentants de classes à droite distinctes de G modulo K . D'où l'inégalité $[H : H \cap K] \leq [G : K]$ et $[H : H \cap K]$ est fini.

— Supposons que $G = HK$ et posons $n = [H : H \cap K]$. Nous savons déjà que $G \supseteq \bigcup_{i=1}^n Kx_i$. Soit $z = hk \in G$ où $(h, k) \in H \times K$. Il existe un $i \in \{1, \dots, n\}$ tel que $h \in (H \cap K)x_i \subseteq Kx_i$ d'où $z \in Kx_i$. Nous avons montré que $G = \bigcup_{i=1}^n Kx_i$ et d'après ce qui précède : $[H : H \cap K] = [G : K]$.

b) La formule des indices donne $[G : H \cap K] = [G : H][H : H \cap K]$ et d'après a), $[G : H \cap K] \leq [G : H][G : K]$. Si $G = HK$, alors toujours d'après a), $[G : H \cap K] = [G : H][G : K]$.

3. a) Soit $(i, j) \in \{1, \dots, n\}^2$ tel que $Hx_i \cap Hx_j \neq \emptyset$ et soit $z \in Hx_i \cap Hx_j$. Alors il existe $(h, h') \in H^2$ tel que $z = hx_i = h'x_j$ d'où $h'^{-1}h = x_j x_i^{-1} \in H \cap K$. Ainsi $(H \cap K)x_i = (H \cap K)x_j$, donc $i = j$.

On sait déjà que $HK \supseteq \bigcup_{i=1}^n Hx_i$. Soit $z = hk \in HK$ avec $(h, k) \in H \times K$. Il existe $i \in \{1, \dots, n\}$ tel que $k \in (H \cap K)x_i \subseteq Hx_i$ donc $z = hk \in Hx_i$ et $HK = \bigcup_{i=1}^n Hx_i$.

En conclusion, $\{Hx_i\}_{1 \leq i \leq n}$ est une partition de HK .

b) On a $HK = \bigcup_{i=1}^n Hx_i$ avec $Hx_i \cap Hx_j = \emptyset$ si $i \neq j$ et $|Hx_i| = |H|$. Donc

$$|HK| = n|H| = [K : H \cap K]|H| \text{ puis } |HK| = \frac{|K||H|}{|H \cap K|} = |KH|.$$

c) H, K sont des sous-groupes du groupe fini HK . Nous pouvons donc appliquer le résultat b) de l'exercice 2: $[HK : H \cap K] = [HK : H][HK : K]$

$$\text{c'est-à-dire } \frac{|HK|}{|H \cap K|} = \frac{|HK|}{|H|} \frac{|HK|}{|K|} \text{ et enfin } |KH| = |HK| = \frac{|H||K|}{|H \cap K|}.$$

4. Les sous-groupes H et K étant d'indices finis dans F , d'après le théorème de Poincaré (théorème 2.17) il en est de même du sous-groupe $H \cap K$. La formule des indices (théorème 2.18) nous donne alors

$$[F : H \cap K] = [F : H][H : H \cap K] \quad \text{et} \quad [F : H \cap K] = [F : K][K : H \cap K].$$

Nous avons donc l'égalité

$$[F : H][H : H \cap K] = [F : K][K : H \cap K].$$

Comme $[F : H]$ et $[F : K]$ sont premiers entre eux, le théorème de Gauss affirme que

$$[F : H] \mid [K : H \cap K] \quad \text{et} \quad [F : K] \mid [H : H \cap K],$$

d'où les inégalités

$$[F : H] \leq [K : H \cap K] \quad \text{et} \quad [F : K] \leq [H : H \cap K].$$

Dans l'exercice 2, nous avons montré que

$$[K : H \cap K] \leq [F : H] \quad \text{et} \quad [H : H \cap K] \leq [F : K].$$

Finalement, nous déduisons des inégalités précédentes que

$$[F : K] = [H : H \cap K] \quad \text{et} \quad [F : H] = [K : H \cap K].$$

5. a) — $\mathcal{R}_{H,K}$ est reflexive: Pour tout $x \in G$, on a $x = exe$, donc $x \mathcal{R}_{H,K} x$.

- $\mathcal{R}_{H,K}$ est symétrique : Soit $(x, y) \in G^2$ tel que $x \mathcal{R}_{H,K} y$. Il existe $(h, k) \in H \times K$ tel que $y = h x k$. On en déduit que $x = h^{-1} y k^{-1}$ où $(h^{-1}, k^{-1}) \in H \times K$, donc $y \mathcal{R}_{H,K} x$.
- $\mathcal{R}_{H,K}$ est transitive : Soit $(x, y, z) \in G^3$ tel que $x \mathcal{R}_{H,K} y$ et $y \mathcal{R}_{H,K} z$. Il existe $(h_1, k_1) \in H \times K$ et $(h_2, k_2) \in H \times K$ tels que $y = h_1 x k_1$ et $z = h_2 y k_2$. On en déduit que $z = h_2 h_1 x k_1 k_2$ où $(h_2 h_1, k_1 k_2) \in H \times K$, donc $x \mathcal{R}_{H,K} z$.

Nous avons montré que la relation binaire $\mathcal{R}_{H,K}$ est une relation d'équivalence sur G . La classe d'équivalence de tout $x \in G$ est

$$\bar{x} = \{h x k; (h, k) \in H \times K\} = H x K.$$

- b) — λ est injective; en effet, supposons $\lambda(h x k) = \lambda(h' x k')$, c'est-à-dire $x^{-1} h x k = x^{-1} h' x k'$. On a alors $h x k = h' x k'$.
- λ est surjective; il n'y a rien à faire.

En conclusion, λ est une bijection.

- c) α) À la question précédente, nous avons montré que les ensembles $H x_i K$ et $x_i^{-1} H x_i K$ sont équipotents, donc $|H x_i K| = |x_i^{-1} H x_i K|$.
- β) $x_i^{-1} H x_i$ est l'image du sous-groupe H de G par l'automorphisme intérieur $G \rightarrow G$, $g \mapsto x_i^{-1} g x_i$, il s'ensuit que $x_i^{-1} H x_i$ est un sous-groupe de G et que $o(x_i^{-1} H x_i) = o(H)$.
- γ) Pour tout i ($1 \leq i \leq r$), $x_i^{-1} H x_i$ et K sont deux sous-groupes finis. Appliquons leurs la formule de l'exercice 3. Il vient

$$|x_i^{-1} H x_i K| = \frac{o(x_i^{-1} H x_i) o(K)}{o(x_i^{-1} H x_i \cap K)},$$

puis, en utilisant les propriétés α) et β),

$$|H x_i K| = \frac{o(H) o(K)}{o(x_i^{-1} H x_i \cap K)}.$$

Les classes doubles de G modulo H et K constituent une partition du groupe G , donc

$$o(G) = \sum_{i=1}^r |H x_i K|.$$

D'après propriété γ), cette égalité devient

$$o(G) = o(H) o(K) \sum_{i=1}^r d_i^{-1} \quad \text{où} \quad d_i = o(x_i^{-1} H x_i \cap K).$$

- d) Soit $H = \langle \tau_1 \rangle = \{e, \tau_1\}$ et $K = \langle \tau_2 \rangle = \{e, \tau_2\}$. Déterminons les classes doubles de S_3 modulo H et K . Nous nous aiderons de la table de Cayley de S_3 (exemple 1.18). On trouve deux classes :

$$HeK = \{e, \tau_1, \tau_2, \sigma_1\} \quad \text{et} \quad H\tau_3K = \{\tau_3, \sigma_2\}.$$

Cet exemple montre que deux classes doubles distinctes ne sont pas, en général, équipotentes.

Déterminons, à présent, les classes doubles modulo K et H . On trouve encore deux classes :

$$KeH = \{e, \tau_1, \tau_2, \sigma_2\} \quad \text{et} \quad K\tau_3H = \{\tau_3, \sigma_1\}.$$

On remarque que $\{KeH, H\tau_3K\} \neq \{HeK, K\tau_3H\}$, ce qui montre, qu'en général, dans un groupe non abélien, $\mathcal{R}_{H,K} \neq \mathcal{R}_{K,H}$.

6. a) Soit $(a, b) \in \mathbf{R}^2$. Pour tout $x \in \mathbf{R}$, on a

$$\begin{aligned} \sigma_a^2(x) &= \sigma(a-x) = a - (a-x) = x, \\ (\sigma_b \circ \tau_a)(x) &= \sigma_b(x+a) = b - x - a = \tau_{-a}(\sigma_b(x)), \end{aligned}$$

donc $\sigma_a^2 = \text{id}_{\mathbf{R}}$ et $\sigma_b \circ \tau_a = \tau_{-a} \circ \sigma_b$.

- b) Soit $a \in \mathbf{R}$. Pour tout $x \in \mathbf{R}$, on a

$$\frac{x + \sigma_a(x)}{2} = \frac{a}{2},$$

donc σ_a est la symétrie par rapport au point $a/2$.

- c) *Isométries de \mathbf{R}* . Soit f une isométrie de \mathbf{R} . Pour tout réel x , on a $|f(x) - f(0)| = |x|$, d'où

$$f(x) = f(0) + x \quad \text{ou} \quad f(x) = f(0) - x.$$

Supposons qu'il existe $(x, y) \in \mathbf{R}^2$ tel que $x \neq y$,

$$f(x) = f(0) + x \quad \text{et} \quad f(y) = f(0) - y.$$

Par soustraction, nous obtenons

$$f(x) - f(y) = x + y.$$

Comme f est une isométrie, nous avons aussi $|f(x) - f(y)| = |x - y|$, d'où

$$x + y = x - y \quad \text{ou} \quad x + y = -x + y,$$

soit

$$y = 0 \quad \text{ou} \quad x = 0.$$

Nous avons montré que

$$\forall x \in \mathbf{R}, f(x) = f(0) + x$$

ou

$$\forall x \in \mathbf{R}, f(x) = f(0) - x.$$

En d'autres termes, $f = \tau_{f(0)}$ ou $f = \sigma_{f(0)}$, ou encore, une isométrie de \mathbf{R} est soit une translation, soit une symétrie par rapport à un point.

$\mathcal{I}(1)$ est un sous-groupe non abélien de $S_{\mathbf{R}}$. On vérifie sans peine que les symétries et les translations sont des bijections, donc $\mathcal{I}(1) \subseteq S_{\mathbf{R}}$. De plus, $\mathcal{I}(1)$ est non vide et pour tout $(f, g) \in \mathcal{I}(1)$, on a $f \circ g^{-1} \in \mathcal{I}(1)$. Par conséquent, $\mathcal{I}(1)$ est un sous-groupe de $S_{\mathbf{R}}$. Enfin, si $(a, b) \in \mathbf{R}^2$ alors $\sigma_b \circ \tau_a = \tau_{-a} \circ \sigma_b$. Or $\tau_{-a} \neq \tau_a$ si $a \neq 0$. Il s'ensuit que $\sigma_b \circ \tau_a \neq \tau_a \circ \sigma_b$ si $a \neq 0$, ce qui prouve que le sous-groupe $\mathcal{I}(1)$ est non abélien.

- d) Soient a et b deux réels. Les translations appartiennent à la même classe à droite modulo T ; en effet,

$$\tau_a \circ \tau_b^{-1} = \tau_a \circ \tau_{-b} = \tau_{a-b} \in T.$$

De même, les symétries appartiennent à la même classe à droite modulo T , car

$$\sigma_a \circ \sigma_b^{-1} = \sigma_a \circ \sigma_b = \tau_{a-b} \in T.$$

En revanche,

$$\tau_a \circ \sigma_b^{-1} = \tau_a \circ \sigma_b = \sigma_{a+b} \notin T$$

montre que les translations et les symétries appartiennent à des classes distinctes. Puisqu'une isométrie de \mathbf{R} est soit une translation, soit une symétrie, nous en déduisons qu'il y a exactement deux classes à droites modulo T dans $\mathcal{I}(1)$, d'où $[\mathcal{I}(1) : T] = 2$.

8. a) *L'application φ est un homomorphisme.* En effet, pour tous $(x, y) \in \mathbf{Z}^2$ et $(x', y') \in \mathbf{Z}^2$, on a

$$\begin{aligned} \varphi((x, y) + (x', y')) &= \varphi(x + x', y + y') \\ &= a(x + x') + b(y + y') \\ &= ax + by + ax' + by' \\ &= \varphi(x, y) + \varphi(x', y'). \end{aligned}$$

Noyau de φ . Le couple $(x, y) \in \mathbf{Z}^2$ appartient au noyau $\text{Ker } \varphi$ si et seulement si il est solution de l'équation diophantienne de degré 1,

$$ax + by = 0.$$

Étant donné que $d = \text{pgcd}(a, b)$, l'équation précédente est équivalente à l'équation diophantienne

$$\frac{a}{d}x + \frac{b}{d}y = 0,$$

dont les coefficients a/d et b/d sont premiers entre eux. Cette dernière équation implique que b/d divise $(a/d)x$; d'après le théorème de Gauss, il existe un entier relatif k tel que $x = (b/d)k$, d'où nous déduisons que $y = -(a/d)k$. Il s'ensuit que

$$\text{Ker } \varphi \subseteq \left\{ \left(\frac{b}{d}k, -\frac{a}{d}k \right); k \in \mathbf{Z} \right\}.$$

L'inclusion opposée est immédiate.

Image de φ . Soit $z \in \text{Im } \varphi$. Il existe donc $(x, y) \in \mathbf{Z}^2$ tel que $ax + by = z$. Puisque d divise a et b , il s'ensuit que d divise également z .

Réciproquement, supposons que z soit un multiple de d . Comme a/d et b/d sont premiers entre eux, le théorème de Bézout assure l'existence de $(x, y) \in \mathbf{Z}^2$ tel que

$$\frac{a}{d}x + \frac{b}{d}y = 1,$$

d'où

$$a \times \frac{xz}{d} + b \times \frac{yz}{d} = z.$$

Comme $(xz/d, yz/d) \in \mathbf{Z}^2$, nous en déduisons que $z \in \text{Im } \varphi$.

En conclusion, $\text{Im } \varphi = d\mathbf{Z}$.

b) Montrons que la correspondance

$$\begin{aligned} * : \frac{\mathbf{Z}}{(n)} \times \frac{\mathbf{Z}}{(n)} &\rightarrow \frac{\mathbf{Z}}{(n)} \\ (\bar{x}, \bar{y}) &\mapsto \overline{ax + by} \end{aligned}$$

est une application. Soient x, x', y, y' dans \mathbf{Z} tels que $\bar{x} = \overline{x'}$ et $\bar{y} = \overline{y'}$. On a $(ax + by) - (ax' + by') = a(x - x') + b(y - y')$ et n divise $x - x'$ et $y - y'$, par conséquent $\overline{ax + by} = \overline{ax' + by'}$, autrement dit $\overline{x * y} = \overline{x' * y'}$, donc $*$ induit sur $\mathbf{Z}/n\mathbf{Z}$ une loi de composition $\bar{*}$ définie par $\bar{x} * \bar{y} = \overline{x * y}$.

c) La loi $\bar{*}$ est associative si et seulement si pour tout $(x, y, z) \in \mathbf{Z}^3$, on a

$$\bar{x} * (\bar{y} * \bar{z}) = (\bar{x} * \bar{y}) * \bar{z},$$

c'est-à-dire

$$\overline{ax + b(ay + bz)} = \overline{a(ax + by) + bz},$$

ou encore

$$ax(a-1) + bz(b-1) \in n\mathbf{Z}.$$

Nous en déduisons que si n divise $a(a-1)$ et $b(b-1)$, alors la loi $\bar{*}$ est associative. Réciproquement, si la loi $\bar{*}$ est associative, alors en posant $x=0$ et $z=1$, puis $x=1$ et $z=0$ on démontre que n divise $a(a-1)$ et $b(b-1)$.

La loi $\bar{*}$ est commutative si et seulement si pour tout $(x, y) \in \mathbf{Z}^2$, on a $\bar{x} \bar{*} \bar{y} = \bar{y} \bar{*} \bar{x}$, c'est-à-dire si et seulement si $\overline{ax+by} = \overline{ay+bx}$, ou encore $(a-b)(x-y) \in n\mathbf{Z}$. Nous en déduisons que si n divise $a-b$, alors $\bar{*}$ est commutative. La réciproque se démontre en posant $x=1$ et $y=0$.

- d) Supposons que n divise $a-1$ et $b-1$. Alors n divise $a(a-1)$, $b(b-1)$ et $(a-1) - (b-1) = a-b$, donc d'après la question précédente, la loi $\bar{*}$ est associative et commutative.

La loi $*$ admet $\bar{0}$ pour élément neutre; en effet, pour tout $x \in \mathbf{Z}$, on a $ax - x = (a-1)x \in n\mathbf{Z}$, donc $\bar{x} \bar{*} \bar{0} = \bar{x}$. De plus la loi étant commutative, on a également $\bar{0} \bar{*} \bar{x} = \bar{x}$.

Tout élément \bar{x} a pour symétrique $\overline{-x}$; en effet,

$$\bar{x} \bar{*} \overline{-x} = \overline{(a-b)x} = \bar{0}$$

car n divise $a-b$.

Nous avons montré que $(\mathbf{Z}/n\mathbf{Z}, \bar{*})$ est un groupe abélien.

Réciproquement, supposons que $(\mathbf{Z}/n\mathbf{Z}, \bar{*})$ soit un groupe. Notons \bar{e} son élément neutre. On a $\bar{0} \bar{*} \bar{e} = \bar{0} = \bar{e} \bar{*} \bar{0}$, donc $ae \in n\mathbf{Z}$ et $be \in n\mathbf{Z}$. On a également $\bar{1} \bar{*} \bar{e} = \bar{1} = \bar{e} \bar{*} \bar{1}$, donc $a+be-1 \in n\mathbf{Z}$ et $ae+b-1 \in n\mathbf{Z}$, d'où nous déduisons que $a-1 \in n\mathbf{Z}$ et $b-1 \in n\mathbf{Z}$.

9. Suivons l'indication de l'énoncé et considérons la correspondance

$$\begin{aligned} \varphi: \left(\frac{G}{H} \right)_d &\longrightarrow \left(\frac{G}{H} \right)_d \\ Kx &\longmapsto K'gx. \end{aligned}$$

- Montrons que φ est une application. Supposons $Kx = Kx'$, c'est-à-dire $xx'^{-1} \in K$. Alors $gx(gx')^{-1} = gxx'^{-1}g^{-1} \in gKg^{-1} = K'$ donc $K'gx = K'gx'$, c'est-à-dire $\varphi(Kx) = \varphi(Kx')$.
- φ est injective. En effet,

$$\begin{aligned}
 \varphi(Kx) = \varphi(Kx') &\iff K'gx = K'gx' \\
 &\iff (gx)(gx')^{-1} \in K' \\
 &\iff gxx'^{-1}g^{-1} \in K' \\
 &\iff xx'^{-1} \in g^{-1}K'g = K \\
 &\iff Kx = Kx'
 \end{aligned}$$

- φ est surjective. En effet, quel que soit $K'x' \in \left(\frac{G}{K'}\right)_d$, on peut écrire $\varphi(Kg^{-1}x') = K'g(g^{-1}x') = K'x'$.

Nous avons démontré que $\left(\frac{G}{K}\right)_d$ et $\left(\frac{G}{K'}\right)_d$ sont équipotents, d'où l'égalité $[G : K] = [G : K']$.

CHAPITRE III

Groupes monogènes, symétriques et diédraux

1. 1) a) On a

$$\begin{aligned}\{k \in \mathbf{Z}; (a, b)^k = (e, e)\} &= \{k \in \mathbf{Z}; a^k = e\} \cap \{k \in \mathbf{Z}; b^k = e\} \\ &= r\mathbf{Z} \cap s\mathbf{Z} \\ &= l\mathbf{Z},\end{aligned}$$

où l est le plus petit commun multiple de r et s , donc l'ordre de (a, b) dans $C_m \times C_n$ est l .

b) Supposons que m et n soient premiers entre eux, $C_m = \langle a \rangle$ et $C_n = \langle b \rangle$. On a $|C_m \times C_n| = mn$ et, d'après le résultat obtenu à la question précédente, $o((a, b)) = mn$, donc le groupe $C_m \times C_n$ est cyclique.

Réciproquement, supposons que $C_m \times C_n$ soit cyclique. Soit (a, b) un générateur du groupe $C_m \times C_n$. Alors $o((a, b)) = mn$. D'après le résultat de la question précédente, $\text{ppcm}(o(a), o(b)) = mn$. De plus a et b sont respectivement des générateurs des groupes C_m et C_n , donc $\text{ppcm}(m, n) = mn$. Il s'ensuit que m et n sont premiers entre eux.

2. a) (\Rightarrow) : il existe $x \in \mathbf{Z}$ tel que $x \equiv 0 \pmod{m}$ et $x \equiv 1 \pmod{n}$. Nous en déduisons l'existence de deux entiers k et l tel que $x = km$ et $x - 1 = ln$. Ces deux entiers vérifient la relation $km - ln = 1$. D'après le théorème de Bézout, m et n sont premiers entre eux.

(\Leftarrow) : d'après le théorème de Bézout, il existe deux entiers k et l tel que $km + ln = 1$. Posons $x = bkm + aln$. De $bkm \equiv 0 \pmod{m}$ et

$ln \equiv 1 \pmod{m}$ nous déduisons

$$x \equiv a \pmod{m}.$$

De la même façon, $aln \equiv 0 \pmod{n}$ et $km \equiv 1 \pmod{n}$ impliquent que

$$x \equiv b \pmod{n}.$$

- b) L'application f est surjective si et seulement si, pour tout $(a, b) \in \mathbf{Z}^2$, il existe $x \in \mathbf{Z}$ tel que $\sigma(x) = \sigma(a)$ et $\pi(x) = \pi(b)$, c'est-à-dire si et seulement si pour tout $(a, b) \in \mathbf{Z}^2$, il existe $x \in \mathbf{Z}$ tel que $x \equiv a \pmod{m}$ et $x \equiv b \pmod{n}$. Le résultat de la question précédente permet de conclure que f est surjective si et seulement si m et n sont premiers entre eux.
3. a) Le groupe multiplicatif des éléments inversibles de $\frac{\mathbf{Z}}{15\mathbf{Z}}$ est (théorème 3.18 et proposition 3.24)

$$G_{15} = \{\bar{k}; 1 \leq k \leq 14, \text{pgcd}(k, 15) = 1\} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}.$$

- b) Soit les deux sous-groupes de G_{15} ,

$$\langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\} \quad \text{et} \quad \langle \bar{11} \rangle = \{\bar{1}, \bar{11}\}.$$

Nous avons :

- 1) $\langle \bar{2} \rangle \simeq C_4$ et $\langle \bar{11} \rangle \simeq C_2$.
- 2) Pour tout $h \in \langle \bar{2} \rangle$ et $k \in \langle \bar{11} \rangle$, on a $hk = kh$ (G_{15} est un groupe abélien).
- 3) $G_{15} = \langle \bar{2} \rangle \langle \bar{11} \rangle$ comme le montre la table de multiplication suivante

\times	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{8}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{14}$	$\bar{13}$

- 4) $\langle \bar{2} \rangle \cap \langle \bar{11} \rangle = (\bar{1})$.

Donc, d'après la proposition 1.85, nous avons l'isomorphisme

$$G_{15} \simeq C_2 \times C_4.$$

4. a) Soit $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}^*$ premier avec n . Nous savons que $|\mathbf{Z}_n^\times| = \varphi(n)$ (proposition (3.24)), donc d'après le corollaire (2.10) du théorème de Lagrange on a $\overline{a}^{\varphi(n)} = \overline{1}$ dans \mathbf{Z}_n^\times , c'est-à-dire $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- b) Soit p est un nombre premier et $a \in \mathbf{Z}$. Si p ne divise pas a alors d'après le théorème d'Euler $a^{\varphi(p)} \equiv 1 \pmod{p}$. Comme p est premier, $\varphi(p) = p - 1$ donc $a^{p-1} \equiv 1 \pmod{p}$ puis $a^p \equiv a \pmod{p}$. Si p divise a alors $a^p \equiv a \pmod{p}$ est évident. Le théorème de Fermat est démontré.
5. a) L'égalité

$$\langle S \rangle = \left\{ a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}; k_i \in \mathbf{Z} \text{ pour tout } i (1 \leq i \leq r) \right\}$$

est une conséquence immédiate de la commutativité de la multiplication. Si le groupe est additif, l'égalité précédente s'écrit

$$\langle S \rangle = \{ k_1 a_1 + k_2 a_2 + \dots + k_r a_r; k_i \in \mathbf{Z} \text{ pour tout } i (1 \leq i \leq r) \}.$$

- b) D'après la question précédente, l'application

$$\begin{aligned} \varphi: \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle &\rightarrow G \\ (x_1, x_2, \dots, x_r) &\mapsto x_1 x_2 \dots x_r \end{aligned}$$

est surjective. Puisque les éléments a_i sont d'ordre fini, nous avons

$$|G| \leq o(a_1) o(a_2) \dots o(a_r) < \infty.$$

6. a) *Existence*. Elle résulte immédiatement de l'exercice 5 et de l'égalité $x^n = x^k$ pour tout $n \in \mathbf{Z}$ où $k \in \{0, 1\}$ tel que $n \equiv k \pmod{2}$.
Unicité. Supposons qu'il n'y a pas unicité. Il existe donc deux r -uplets distincts $(k_1, k_2, \dots, k_r) \in \{0, 1\}^r$ et $(l_1, l_2, \dots, l_r) \in \{0, 1\}^r$ tels que

$$a_1^{k_1} a_2^{k_2} \dots a_r^{k_r} = a_1^{l_1} a_2^{l_2} \dots a_r^{l_r}.$$

Soit $j \in \{1, 2, \dots, r\}$ tel que $k_j \neq l_j$. On a donc

$$a_j = \begin{cases} \prod_{i=1, i \neq j}^r a_i^{l_i - k_i} & \text{si } k_j - l_j = 1 \\ \prod_{i=1, i \neq j}^r a_i^{k_i - l_i} & \text{si } k_j - l_j = -1. \end{cases}$$

Nous en déduisons que $\{a_1, a_2, \dots, a_r\} \setminus \{a_j\}$ est une famille génératrice de G ce qui contredit la minimalité de $\{a_1, a_2, \dots, a_r\}$.

b) L'application $\varphi: \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle \rightarrow G$ définie par

$$\varphi(x_1, x_2, \dots, x_r) = x_1 x_2 \dots x_r$$

est un homomorphisme de groupes; en effet, pour tout $(x_1, x_2, \dots, x_r) \in \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle$ et $(y_1, y_2, \dots, y_r) \in \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle$, on a

$$\begin{aligned} \varphi((x_1, x_2, \dots, x_r)(y_1, y_2, \dots, y_r)) &= \varphi(x_1 y_1, x_2 y_2, \dots, x_r y_r) \\ &= x_1 y_1 x_2 y_2 \dots x_r y_r \\ &= (x_1 x_2 \dots x_r)(y_1 y_2 \dots y_r) \\ &= \varphi(x_1, x_2, \dots, x_r) \varphi(y_1, y_2, \dots, y_r). \end{aligned}$$

Cette homomorphisme est bijective d'après la question précédente. De plus, la minimalité de $\{a_1, a_2, \dots, a_r\}$ implique que $a_i \neq e$ pour tout i , donc chaque élément a_i est d'ordre 2, c'est-à-dire $\langle a_i \rangle \simeq C_2$. Nous en déduisons que G est isomorphe à C_2^r et concluons que le groupe G est d'ordre 2^r .

7. Supposons que le groupe $\mathbf{Z} \times \mathbf{Z}$ soit monogène. Soit $x = (x_1, x_2)$ un générateur, alors $\mathbf{Z} \times \mathbf{Z} = \{(kx_1, kx_2); k \in \mathbf{Z}\}$. Si $x_1 \neq 0$ et $x_2 \neq 0$, alors il n'existe pas de $k \in \mathbf{Z}$ tel que $(kx_1, kx_2) = (0, 1)$, donc l'un des x_i ($i = 1, 2$) est nul. Supposons que $x_1 = 0$, alors il n'existe pas de $k \in \mathbf{Z}$ tel que $(kx_1, kx_2) = (1, 0)$. Bien entendu, $x_2 = 0$ ne convient pas non plus. Nous en déduisons que le groupe $\mathbf{Z} \times \mathbf{Z}$ n'est pas monogène.

8. a) Supposons que le groupe $(\mathbf{Q}, +)$ soit monogène. Alors il existe $(m, n) \in \mathbf{Z}^* \times \mathbf{N}^*$ tel que $\mathbf{Q} = \langle \frac{m}{n} \rangle$. Comme $\frac{1}{2n} \in \mathbf{Q}$, il existe un entier

k tel que $\frac{1}{2n} = k\frac{m}{n}$. Il s'ensuit que $k = \frac{1}{2m} \notin \mathbf{Z}$: contradiction. Nous en déduisons que le groupe $(\mathbf{Q}, +)$ n'est pas monogène.

Si le groupe $(\mathbf{R}, +)$ était monogène, alors le sous-groupe $(\mathbf{Q}, +)$ de $(\mathbf{R}, +)$ serait également monogène (théorème 3.10). Il s'ensuit que le groupe $(\mathbf{R}, +)$ n'est pas monogène.

b) Pour tout $(m, n) \in \mathbf{Z} \times \mathbf{N}^*$, on a

$$\frac{m}{n} = m(n-1)! \times \frac{1}{n!}$$

avec $m(n-1)! \in \mathbf{Z}$, ce qui prouve que l'ensemble $\{\frac{1}{n!}; n \in \mathbf{N}\}$ engendre le groupe $(\mathbf{Q}, +)$.

c) Soit H un sous-groupe monogène non nul de $(\mathbf{Q}, +)$. Il existe donc $x \in \mathbf{Q}^*$ tel que $H = \langle x \rangle$. Si k est un entier tel que $kx = 0$, alors $k = 0$. Par conséquent, x est d'ordre infini, donc H est un sous-groupe monogène infini.

d) Soit H un sous-groupe non nul de $(\mathbf{Q}, +)$ engendré par la famille fini de nombres rationnels $\{p_i/q_i\}_{1 \leq i \leq r}$ avec $r \in \mathbf{N}^*$. Posons $q = q_1 q_2 \dots q_r$. Alors qH est un sous-groupe non nul de \mathbf{Z} . Il existe donc un entier $a > 0$ tel que $qH = a\mathbf{Z}$, d'où $H = (a/q)\mathbf{Z}$. Nous en déduisons que le sous-groupe H est isomorphe au groupe \mathbf{Z} .

9. a) Soit un entier $n > 0$. Notons g^n la composée $g \circ g \circ \dots \circ g$ de n fonctions g . Pour tout $z \in \tilde{\mathbf{C}}$, on a $g^n(z) = z + n$, donc $g^n \neq \text{id}_{\tilde{\mathbf{C}}}$. Il s'ensuit que g est d'ordre infini; le sous-groupe G est monogène infini, donc isomorphe à \mathbf{Z} .

b) On montre facilement par récurrence que pour tout entier $n > 0$, on a $h^n(z) = \alpha^n z + \beta(1 - \alpha^n)/(1 - \alpha)$ quel que soit $z \in \tilde{\mathbf{C}}$. Par suite, $h^n = \text{id}_{\tilde{\mathbf{C}}}$ si et seulement si $\alpha^n = 1$. Nous en déduisons que h est d'ordre fini dans \mathcal{H} si et seulement si α est une racine de l'unité dans \mathbf{C} .

10. a) Les groupes cycliques étant abéliens, on a $(ab)^r = a^r b^r$ pour tout $(a, b) \in \mathbf{C}_n^2$, donc $f \in \text{End}(\mathbf{C}_n)$. D'après le corollaire 3.7, on a $\text{Ker } f = \{a \in \mathbf{C}_n; \text{o}(a) \text{ divise } r\}$. Des équivalences

$$x^l \in \text{Ker } f \iff rl \in n\mathbf{Z} \iff l \in s\mathbf{Z},$$

nous déduisons que $a \in \text{Ker } f$ si et seulement s'il existe un entier k tel que $a = x^{ks}$; autrement dit, $\text{Ker } f = \{x^{ks}; k \in \mathbf{Z}\}$. Or, quel que soit $(k, k') \in \mathbf{Z}^2$,

$$x^{ks} = x^{k's} \iff ks \equiv k's \pmod{n} \iff k \equiv k' \pmod{r},$$

si bien que $\text{Ker } f = \{x^{ks}; k \in \mathbf{N}_r\}$; il s'ensuit que $o(\text{Ker } f) = r$. À l'aide du 1^{er} théorème d'isomorphisme et de la proposition 2.15, on conclut que $o(\text{Im } f) = o(C_n) / o(\text{Ker } f) = s$.

- b) Pour tout $a \in C_n$, on a $(h \circ f)(a) = (a^r)^s = a^n = e$, donc $\text{Im } f \subseteq \text{Ker } h$. De la question précédente, nous déduisons que $o(\text{Ker } h) = s$ et $o(\text{Im } f) = s$; il s'ensuit que $\text{Im } f = \text{Ker } h$. Par symétrie, nous avons également $\text{Im } h = \text{Ker } f$.

11. Déterminons l'ordre des matrices suivantes :

$$\begin{aligned} A &= \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, & B &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & C &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \\ D &= \begin{pmatrix} 2 & -3i \\ 1 & i \end{pmatrix}, & E &= \begin{pmatrix} 2 & -2i \\ -3 & 2i \end{pmatrix}, & F &= \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

On note I la matrice identité.

Pour toute matrice $M \in \text{GL}(2, \mathbf{C})$ et tout entier n , on a $\det(M^n) = (\det(M))^n$, d'où nous déduisons que si M est une matrice d'ordre fini, alors son déterminant est une racine de l'unité.

Ordre de A. Son déterminant est -1 , donc l'ordre de A , s'il est fini, est nécessairement pair. On calcule successivement $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $A^4 = I$. La matrice A est d'ordre 4.

Ordre de B. En écrivons $B = I + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et calculons B^n à l'aide de la formule de Newton :

$$B^n = \sum_{k=0}^n \binom{n}{k} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^k.$$

Or $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, donc pour tout entier $k > 1$, on a $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^k = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Il s'ensuit que

$$B^n = I + n \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

ce qui montre que B est une matrice d'ordre infini.

Ordre de C. De $C^2 = -I$, nous déduisons que C est d'ordre 4.

Ordre de D. Son déterminant $5i$ n'est pas une racine de l'unité, donc D est d'ordre infini.

Ordre de E. Son déterminant $-2i$ n'est pas une racine de l'unité, donc E est d'ordre infini.

Ordre de F. Comme $\det(F) = -1$, l'ordre de la matrice F, s'il est fini, est nécessairement pair. Écrivons $F = I + G$ où $G = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Soit $n \geq 1$ un entier. La formule du binôme de Newton donne

$$F^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} G^k = \sum_{k=0}^n \binom{2n}{2k} G^{2k} + \sum_{k=0}^{n-1} \binom{2n}{2k+1} G^{2k+1}.$$

On démontre facilement par récurrence que pour tout entier naturel p , on a

$$G^{2p} = \begin{pmatrix} 2^p & 0 \\ 0 & 2^p \end{pmatrix} \quad \text{et} \quad G^{2p+1} = \begin{pmatrix} 0 & 2^{p+1} \\ 2^p & 0 \end{pmatrix},$$

donc le coefficient d'indice (1, 1) de F^{2n} est $\sum_{k=0}^n \binom{2n}{2k} 2^k \neq 1$, par conséquent $F^{2n} \neq I$. Nous en déduisons que la matrice F est d'ordre infini.

12. a) Soit

$$M = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{et} \quad N = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

deux matrices de G. On trouve

$$MN^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} ac' & -ab' + ba' \\ 0 & a'c \end{pmatrix}$$

avec $(ac')(a'c) = (ac)(a'c') \neq 0$, donc $MN^{-1} \in G$ et G est un sous-groupe de $GL(2, \mathbf{R})$.

L'application

$$\mathbf{R} \rightarrow G, \quad a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

est injective, donc le groupe G est infini.

Les matrices

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

sont des éléments de G tels que

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \quad \text{et} \quad BA = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix},$$

donc le groupe G n'est pas abélien.

b) L'application $\varphi: \mathbf{R} \rightarrow G$ définie par

$$\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

est un homomorphisme de groupes; en effet, pour tout $(x, x') \in \mathbf{R}^2$,

$$\varphi(x+x') = \begin{pmatrix} 1 & x+x' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' \\ 0 & 1 \end{pmatrix} = \varphi(x)\varphi(x').$$

Son image est H , donc H est un sous-groupe de G . De plus, l'homomorphisme φ est injectif, donc d'après le 1^{er} théorème d'isomorphisme, nous en déduisons que le groupe $(\mathbf{R}, +)$ est isomorphe au groupe H .

c) Les éléments d'ordre 2 du groupe G sont les matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ telles que

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^2 = \begin{pmatrix} a^2 & ab+bc \\ 0 & c^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

donc les coefficients a , b et c sont les solutions du système

$$\begin{cases} a \in \{\pm 1\} \\ c \in \{\pm 1\} \\ b(a+c) = 0 \\ (a, b, c) \neq (1, 0, 1) \end{cases}$$

soit

$$\begin{cases} a = 1 \\ b = -1 \\ b \in \mathbf{R} \end{cases} \quad \text{ou} \quad \begin{cases} a = -1 \\ c = 1 \\ b \in \mathbf{R} \end{cases} \quad \text{ou} \quad \begin{cases} a = -1 \\ c = -1 \\ b = 0 \end{cases}$$

Les éléments d'ordre 2 de G sont les matrices

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{et} \quad \left\{ \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}; b \in \mathbf{R} \right\}.$$

Les matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$$

sont des éléments d'ordre 2, mais leur produit

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

est un élément d'ordre infini; en effet, on démontre par récurrence que pour tout entier $n > 0$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

13. Soit $C_n = \langle x \rangle$ un groupe cyclique d'ordre $n > 1$, et k un entier tel que $1 \leq k \leq n - 1$. Soit $d = \text{pgcd}(k, n)$. Nous avons les équivalences

$$\begin{aligned} (x^k)^l = e &\iff x^{kl} = e \\ &\iff n \mid kl && \text{(corollaire 3.7)} \\ &\iff \frac{n}{d} \mid \frac{k}{d} l && \text{où } \text{pgcd}\left(\frac{n}{d}, \frac{k}{d}\right) = 1 \\ &\iff \frac{n}{d} \mid l && \text{(lemme de Gauss).} \end{aligned}$$

Ainsi l'ordre de x^k est égal à $\frac{n}{d}$.

Remarque. Une conséquence immédiate est que x^k ($0 \leq k < n$) est un générateur du groupe C_n si et seulement si k et n sont premiers entre eux.

14. a) Comme x et y permutent, on a $(xy)^{mn} = (x^m)^n (y^n)^m = e$, donc l'ordre de xy est fini.
- b) Notons ω l'ordre de xy . De a) , on déduit que ω divise mn . De plus $e = (xy)^{\omega m} = (x^m)^\omega y^{m\omega} = e y^{m\omega} = y^{m\omega}$ implique que n divise $m\omega$. Comme m et n sont premiers entre eux, d'après le théorème de Gauss n divise ω . De même, on montre que m divise ω . Comme m et n sont premiers entre eux, mn divise ω , ce qui achève la démonstration de $\omega = mn$.
- c) Comme l est un multiple de m et n , il vient $(xy)^l = x^l y^l = e$, donc ω divise l . De plus $x^\omega y^\omega = (xy)^\omega = e$ donc $x^\omega = y^{-\omega} \in \langle x \rangle \cap \langle y \rangle = \{e\}$ c'est-à-dire $x^\omega = y^\omega = e$. Il s'ensuit que ω est un multiple de m et n , donc ω est un multiple de l . En fin de compte $l = \omega$.
- Si $\langle x \rangle \cap \langle y \rangle \neq \{e\}$, on ne peut faire mieux que $o(xy) \mid l$ comme le prouve l'exemple suivant. Soit $G = \langle x \rangle$ le groupe cyclique d'ordre 9. On a $\langle x^3 \rangle \cap \langle x^6 \rangle = \langle x^3 \rangle \neq \{e\}$, $o(x^3) = 9/(3,9) = 3$ et $o(x^6) = 9/(6,9) = 3$ mais $o(x^3 x^6) = o(e) = 1 < 3 = \text{ppcm}(3,6)$.
- d) Les cycles $(\gamma_i)_{1 \leq i \leq 9}$ sont à supports disjoints donc ils commutent deux à deux. De plus si γ est l'un de ces cycles, pour tout $n \in \mathbf{Z}^*$, $\text{supp}(\gamma^n) \subseteq \text{supp}(\gamma)$, donc pour tout $i \neq j$, $\langle \gamma_i \rangle \cap \langle \gamma_j \rangle = \{e\}$. Donc d'après b) et c), nous trouvons que l'ordre de σ est le PPCM des longueurs (des ordres) des cycles $(\gamma_i)_{1 \leq i \leq 9}$.

15. Soient g un élément de G d'ordre s et x un élément quelconque dont l'ordre est noté t . Désignons par \mathcal{P} l'ensemble des nombres premiers. On définit deux entiers s' et t' par

$$s' = \prod_{\substack{p \in \mathcal{P} \\ v_p(s) \geq v_p(t)}} p^{v_p(s)} \quad \text{et} \quad t' = \prod_{\substack{p \in \mathcal{P} \\ v_p(t) > v_p(s)}} p^{v_p(t)}$$

où $v_p(n)$ désigne l'exposant du nombre premier p dans la factorisation en produit de nombres premiers de l'entier n . Il est clair que s' divise

s et t' divise t . Si p est un nombre premier, on ne peut avoir simultanément $v_p(s) \geq v_p(t)$ et $v_p(t) > v_p(s)$, donc s' et t' sont premiers entre eux. De plus,

$$s't' = \prod_{p \in \mathcal{P}} p^{\max(v_p(s), v_p(t))} = \text{ppcm}(s, t).$$

L'élément $g' = g^{s's'}$ est d'ordre s' (exercice 3.13). De même, $x' = x^{t't'}$ est d'ordre t' . Considérons $y = x'g'$. D'après le résultat de la question b) de l'exercice 3.14, l'ordre de y est égal $s't' = \text{ppcm}(s, t)$. Par définition du plus petit commun multiple, on a $\text{ppcm}(s, t) \geq s$ et, s étant l'ordre maximal d'un élément de G , on a également $\text{ppcm}(s, t) \leq s$. Il s'ensuit que $\text{ppcm}(s, t) = s$, si bien que t divise s , donc $x^s = e$.

17. a) Soit $\alpha \in \text{Aut}(G)$. On a

$$\langle \alpha(x) \rangle = \{ \alpha(x)^n ; n \in \mathbf{Z} \} = \{ \alpha(x^n) ; n \in \mathbf{Z} \} = \alpha(G) = G,$$

ce qui prouve que $\alpha(x)$ est un générateur de G .

b) L'application λ_k est un automorphisme de G . Pour tout entier k premier avec n , notons λ_k l'application notée λ dans l'énoncé. Dans le groupe abélien G , on a $(ab)^k = a^k b^k$ pour tout $(a, b) \in G^2$; par conséquent, l'application λ_k est un homomorphisme de groupes.

Soit $a \in \text{Ker}(\lambda_k)$. Il existe $l \in \mathbf{Z}$ tel que $a = x^l$. Alors $a^k = e$ implique $x^{kl} = e$, d'où $kl \in n\mathbf{Z}$ (proposition 3.6). Comme k et n sont premiers entre eux, on a $l \in n\mathbf{Z}$ (lemme de Gauss), donc $a = e$ (proposition 3.6), prouvant ainsi que l'homomorphisme λ_k est injectif. Puisque G est fini, l'homomorphisme λ_k est aussi surjectif. Finalement λ_k est un automorphisme de G .

Les groupes $\text{Aut}(G)$ et G_n sont isomorphes. Montrons que $\lambda_k = \lambda_l$ si et seulement si $\bar{k} = \bar{l}$. Supposons que $\lambda_k = \lambda_l$. Alors $x^k = x^l$, puis $x^{k-l} = e$, donc $k-l \in n\mathbf{Z}$, soit $\bar{k} = \bar{l}$. Réciproquement, si $\bar{k} = \bar{l}$, alors $k-l \in n\mathbf{Z}$, puis $a^{k-l} = e$ (corollaire 2.10), si bien que $a^k = a^l$, c'est-à-dire $\lambda_k = \lambda_l$.

Ce résultat montre que la correspondance

$$\begin{aligned}\psi: G_n &\rightarrow \text{Aut}(G) \\ \bar{k} &\mapsto \lambda_k.\end{aligned}$$

définit une application injective. Elle est également surjective ; en effet, si $\lambda \in \text{Aut}(G)$, alors il existe un entier k premier avec n tel que $\lambda(x) = x^k$ (question précédente et théorème 3.18 2°) et pour tout $i \in \mathbf{Z}$, on a

$$\lambda(x^i) = \lambda(x)^i = x^{ki} = (x^i)^k = \lambda_k(x^i),$$

donc $\lambda = \psi(\bar{k})$.

L'application ψ est un homomorphisme de groupes ; en effet, pour tout $(\bar{k}, \bar{l}) \in G_n^2$ et tout $a \in G$, on a

$$(\lambda_k \circ \lambda_l)(a) = \lambda_k(\lambda_l(a)) = \lambda_k(a^l) = a^{kl} = \lambda_{kl}(a),$$

c'est-à-dire

$$\psi(\bar{k}\bar{l}) = \psi(\bar{k}) \circ \psi(\bar{l}).$$

On conclut que les groupes G_n et $\text{Aut}(G)$ sont isomorphes. Par conséquent, le groupe $\text{Aut}(G)$ est abélien comme G_n et $|\text{Aut}(G)| = \varphi(n)$ (proposition 3.24).

- c) Soit $\lambda \in \text{Aut}(G)$. On sait que $\lambda(x)$ est un générateur de G , or les seuls générateurs du groupe monogène G sont x et x^{-1} (théorème 3.18), donc $\text{Aut}(G)$ est un groupe d'ordre 2, dont les éléments sont l'identité id_G et l'application inverse $G \rightarrow G, a \mapsto a^{-1}$. La proposition 3.9 nous permet de conclure que $\text{Aut}(G)$ est un groupe cyclique.
- d) Les groupes \mathbf{Z} et $\frac{\mathbf{Z}}{(6)}$ ne sont pas isomorphes. Cependant, d'après ce qui précède, on a $|\text{Aut}(\mathbf{Z})| = 2$ et $|\text{Aut}(\frac{\mathbf{Z}}{(p)})| = \varphi(6) = 2$, donc $\text{Aut}(\mathbf{Z}) \simeq \text{Aut}(\frac{\mathbf{Z}}{(3)})$.

Les groupes $\frac{\mathbf{Z}}{(5)}$ et $\frac{\mathbf{Z}}{(10)}$ ne sont pas isomorphes. On sait que $\text{Aut}(\frac{\mathbf{Z}}{(5)}) \simeq G_5$ et $\text{Aut}(\frac{\mathbf{Z}}{(10)}) \simeq G_{10}$, or G_5 et G_{10} sont des groupes cycliques d'ordre 4, donc $\text{Aut}(\frac{\mathbf{Z}}{(5)}) \simeq \text{Aut}(\frac{\mathbf{Z}}{(10)})$.

18.

21. *Permutation* σ_1 . Les σ_1 -orbites non ponctuelles sont $\Omega_{\sigma_1}(1) = (1, 3, 4, 6)$ et $\Omega_{\sigma_1}(2) = (2, 5)$. Nous en déduisons la décomposition canonique de σ_1 en produit de cycles disjoints :

$$\sigma_1 = (1, 3, 4, 6)(2, 5).$$

Les cycles de la décomposition ont pour longueurs 2 et 4, donc (théorème 3.59) l'ordre de σ_1 est $\text{ppcm}(2, 4) = 4$. D'après le théorème 3.70 et la remarque 3.66, on a $\varepsilon(\sigma_1) = (-1)^3 \times (-1) = 1$. Une décomposition en produit de transpositions nous est fourni dans la démonstration du théorème 3.60 :

$$\sigma_1 = (1, 3)(3, 4)(4, 6)(2, 5).$$

Étant donné que σ_1 est d'ordre 4 et que $50 \equiv 2 \pmod{4}$, on a $\sigma_1^{50} = \sigma_1^2$, donc

$$\sigma_1^{50} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 1 & 5 & 3 \end{pmatrix}.$$

Permutation σ_2 . La permutation σ_2 possède 3 orbites non ponctuelles : $\Omega_{\sigma_2}(1) = (1, 4, 7, 8)$, $\Omega_{\sigma_2}(2) = (2, 6, 5)$ et $\Omega_{\sigma_2}(3) = (3, 9)$. Nous en déduisons sa décomposition canonique en produit de cycles disjoints

$$\sigma_2 = (1, 4, 7, 9)(2, 6, 5)(3, 9),$$

son ordre $\text{ppcm}(4, 3, 2) = 12$, sa signature $\varepsilon(\sigma_2) = (-1)^3 \times (-1)^2 \times (-1) = 1$ et une décomposition en produit de transpositions

$$\sigma_2 = (1, 4)(4, 7)(7, 9)(2, 6)(6, 5)(3, 9).$$

Les cycles de la décomposition canonique commutent, donc

$$\sigma_2^{100} = (1, 4, 7, 9)^{100}(2, 6, 5)^{100}(3, 9)^{100}.$$

Le cycle $(1, 4, 7, 9)$ est d'ordre 4 et $100 \equiv 0 \pmod{4}$, le cycle $(2, 6, 5)$ est d'ordre 3 et $100 \equiv 1 \pmod{3}$, le cycle $(3, 9)$ est d'ordre 2 et $100 \equiv 0 \pmod{2}$, donc

$$\sigma_2^{100} = (1, 4, 7, 9)^0(2, 6, 5)^1(3, 9)^0 = (2, 6, 5)$$

ou encore

$$\sigma_2^{100} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 6 & 3 & 4 & 2 & 5 & 7 & 8 & 9 \end{pmatrix}.$$

Permutation σ_3 . Sa décomposition en produit de cycle disjoints est

$$\sigma_3 = (1, 3, 2, 4)(5, 8, 11)(6, 7, 9, 12).$$

Son ordre est $\text{ppcm}(4, 3, 4) = 12$, sa signature est $\varepsilon(\sigma_3) = (-1)^3 \times (-1)^2 \times (-1)^3 = 1$, une décomposition en produit de transpositions est

$$\sigma_3 = (1, 3)(3, 2)(2, 4)(5, 8)(8, 11)(6, 7)(7, 9)(9, 12),$$

et

$$\sigma_3^{10} = (1, 3, 2, 4)^2(5, 8, 11)(6, 7, 9, 12)^2,$$

soit

$$\sigma_3^{10} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 1 & 4 & 3 & 8 & 9 & 12 & 11 & 6 & 10 & 5 & 7 \end{pmatrix}.$$

22. Posons $\gamma' = (j_1, j_r)(j_1, j_{r-1}) \dots (j_1, j_2)$. Si $j \in \mathbf{N}_n \setminus \{j_1, j_2, \dots, j_r\}$, alors $\gamma'(k) = k = \gamma(k)$. Si $k \in \mathbf{N}_{r-1}$, alors

$$\begin{aligned} \gamma'(j_k) &= (j_1, j_r) \dots (j_1, j_2)(j_k) \\ &= (j_1, j_r) \dots (j_1, j_k)(j_k) \\ &= \dots (j_1, j_{k+1})(j_1) \\ &= j_{k+1} \\ &= \gamma(j_k). \end{aligned}$$

Et enfin $\gamma'(j_r) = (j_1, j_r)(j_r) = j_1 = \gamma(j_r)$. Par conséquent $\gamma' = \gamma$, c'est-à-dire

$$(j_1, j_2, \dots, j_r) = (j_1, j_r)(j_1, j_{r-1}) \dots (j_1, j_2).$$

23. Soit $p \in \{1, 2, \dots, r-1\}$. Sans perte de généralité, posons $\gamma = (1, 2, \dots, r)$. Montrons que $\text{supp}(\gamma^p) = \mathbf{N}_r$. On sait déjà que $\text{supp}(\gamma^p) \subset \mathbf{N}_r$ (remarque 3.38 3°). Montrons l'inclusion opposée. Soit $i \in \mathbf{N}_r$. Comme

$\gamma^p(i)$ est le reste de la division euclidienne par r de $i + p$, si $\gamma^p(i) = i$ alors p est un multiple de r , ce qui contredit la définition de p , donc $i \in \text{supp}(\gamma^p)$.

Étant donné que γ^p a pour support \mathbf{N}_r et qu'une permutation est un cycle si et seulement si elle a une seule orbite non ponctuelle (proposition 3.53), la permutation γ^p est un cycle si et seulement si $o(\gamma^p) = r$ (proposition 3.50). Or (exercice 3.13),

$$o(\gamma^p) = \frac{o(\gamma)}{\text{pgcd}(o(\gamma), p)} = \frac{r}{\text{pgcd}(r, p)}.$$

Il s'ensuit que γ^p est un cycle si et seulement si r et p sont premiers entre eux.

Remarque. Un corollaire est que si r est un nombre premier, alors toute puissance d'un r -cycle est soit un r -cycle, soit l'identité.

24. a) Nous avons r entiers distincts $\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r)$ tels que

$$\sigma \circ \gamma \circ \sigma^{-1}(\sigma(j_k)) = \sigma \circ \gamma(j_k) = \begin{cases} \sigma(j_{k+1}) & \text{si } 1 \leq k \leq r-1 \\ \sigma(j_1) & \text{si } k = r, \end{cases}.$$

De plus, pour tout entier $k \in \mathbf{N}_n \setminus \{\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r)\}$, il existe un unique entier $j \in \mathbf{N}_n \setminus \{j_1, j_2, \dots, j_r\}$ tel que $k = \sigma(j)$, et on a

$$\sigma \circ \gamma \circ \sigma^{-1}(k) = \sigma \circ \gamma(j) = \sigma(j) = k.$$

Nous avons prouvé que $\sigma \circ \gamma \circ \sigma^{-1}$ est le r -cycle $(\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r))$.

b) Pour tout entier p tel que $1 \leq p \leq n$, on a

$$\gamma_1^p = \begin{pmatrix} 1 & 2 & \dots & n-p & n-p+1 & \dots & n \\ p+1 & p+2 & \dots & n & 1 & \dots & p \end{pmatrix}.$$

De la question précédente, nous déduisons que $\gamma_1^p \circ \tau_1 \circ \gamma_1^{-p}$ est la transposition

$$(\gamma_1^p(1), \gamma_1^p(2)) = \begin{cases} (p+1, p+2) & \text{si } 1 \leq p \leq n-2 \\ (1, n) & \text{si } p = n-1 \\ (1, 2) & \text{si } p = n. \end{cases}$$

Remarquons que

$$\{(i, i+1); 1 \leq i \leq n-1\} \subseteq \{\gamma_1^p \circ \tau_1 \circ \gamma_1^{-p}; 1 \leq p \leq n\} \subseteq \langle \tau_1, \gamma_1 \rangle \subseteq S_n.$$

Or l'ensemble des transpositions $(i, i+1)$ telles que $1 \leq i \leq n-1$ engendrent le groupe S_n (proposition 3.64), d'où la conclusion :

$$S_n = \langle \tau_1, \gamma_1 \rangle.$$

25. À toute permutation $\sigma \in S_n$ associons l'automorphisme intérieur f_σ définie par sur S_n par $f_\sigma(\gamma) = \sigma \circ \gamma \circ \sigma^{-1}$. L'application

$$f: S_n \rightarrow \text{Int}(S_n), \quad \sigma \mapsto f_\sigma$$

est un homomorphisme de groupes; en effet, pour tout $(\sigma_1, \sigma_2) \in S_n^2$, on a

$$\begin{aligned} f_{\sigma_1 \circ \sigma_2}(\gamma) &= (\sigma_1 \circ \sigma_2) \circ \gamma \circ (\sigma_1 \circ \sigma_2)^{-1} \\ &= \sigma_1 \circ (\sigma_2 \circ \gamma \circ \sigma_2^{-1}) \circ \sigma_1^{-1} \\ &= (f_{\sigma_1} \circ f_{\sigma_2})(\gamma). \end{aligned}$$

Par définition, l'homomorphisme f est surjectif. Intéressons-nous à son noyau :

$$\begin{aligned} \text{Ker}(f) &= \{\sigma \in S_n; f_\sigma = \text{id}_{S_n}\} \\ &= \{\sigma \in S_n; \sigma \circ \gamma \circ \sigma^{-1} = \gamma\} \\ &= \{\sigma \in S_n; \sigma \circ \gamma = \gamma \circ \sigma\} \\ &= Z(S_n). \end{aligned}$$

Démontrons par l'absurde que le centre de S_n pour $n \geq 3$ est trivial. Soient $\sigma \in Z(S_n) \setminus \{e\}$ et $j \in \text{supp}(\sigma)$. Comme $n \geq 3$, il existe $k \in \mathbb{N}_n \setminus \{j, \sigma(j)\}$. Notons τ la transposition (j, k) . En utilisant le résultat de la question a) de l'exercice précédent, on a

$$(j, k) = \sigma \circ \tau \circ \sigma^{-1} = (\sigma(j), \sigma(k)).$$

Cela implique que $j = \sigma(j)$ ou $k = \sigma(j)$ ce qui est impossible.

Nous avons montré que f est un isomorphisme de groupes.

26. Soient $n \geq 4$ dans \mathbf{N} et i, j, k, l trois entiers distincts dans \mathbf{N}_n . La décomposition

$$(i, j, k) = (i, j)(j, k)$$

est triviale. Nous en déduisons que

$$(i, j, k)(j, k, l) = (i, j)(j, k)(j, k)(k, l).$$

Une transposition étant d'ordre 2, nous obtenons

$$(i, j, k)(j, k, l) = (i, j)(k, l).$$

a) Soit $n \geq 3$ un entier. Les 3-cycles de S_n appartiennent à A_n ; il suffit donc de montrer que toute permutation paire $\sigma \neq e$ de S_n peut s'écrire comme un produit de 3-cycles. Nous savons déjà que σ se décompose en un produit d'un nombre pair de transpositions distinctes (théorèmes 3.60 et 3.65) :

$$\gamma = \tau_1 \tau_2 \dots \tau_{2s} \quad (s \in \mathbf{N}^*).$$

Regroupons les deux par deux :

$$\gamma = (\tau_1 \tau_2) \dots (\tau_{2s-1} \tau_{2s}).$$

Pour tout $k \in \mathbf{N}_s$, si $\text{supp}(\tau_{2k-1}) \cap \text{supp}(\tau_{2k}) = \emptyset$, alors $\tau_{2k-1} \tau_{2k}$ est un produit de deux 3-cycles, sinon $\tau_{2k-1} \tau_{2k}$ est un 3-cycle.

On conclut que, pour tout entier $n \geq 3$, l'ensemble des 3-cycles engendrent le groupe alterné A_n .

b) Soient i, j, k trois entiers distincts dans $\mathbf{N}_n \setminus \{1\}$ où $n \geq 3$. On vérifie aisément que

$$(1, i, j) = (1, i)(i, j) = (1, i)(1, i)(1, j)(1, i) = (1, j)(1, i).$$

Nous en déduisons la décomposition

$$\begin{aligned} (i, j, k) &= (i, j)(j, k) \\ &= (1, i)(1, j)(1, i)(1, j)(1, k)(1, j) \\ &= (1, j, i)(1, j, i)(1, j, k) \end{aligned}$$

qui permet de conclure que l'ensemble des 3-cycles de la forme $(1, i, j)$ engendrent le groupe alterné A_n .

- c) Compte tenu de ce qui précède, il suffit d'écrire un 3-cycle comme un produit de 3-cycles de la forme $(1, i, j)$. Or

$$(1, i, j) = (1, 2, j)(1, 2, i)^2$$

$$(2, i, j) = (1, 2, j)^2(1, 2, i)$$

et pour tout $k \in \mathbf{N}_n \setminus \{1, 2\}$,

$$(k, i, j) = (1, 2, k)(1, 2, j)^2(1, 2, i)(1, 2, k)^2,$$

donc l'ensemble des 3-cycles de la forme $(1, 2, i)$ engendrent le groupe alterné A_n .

27. Posons $\sigma_1 = (1, 2)(3, 4)$, $\sigma_2 = (1, 3)(2, 4)$ et $\sigma_3 = (1, 4)(2, 3)$. Chacune de ses permutations, ainsi que e , ont une signature égale à 1, donc $K \subseteq A_4$. La table de multiplication ci-dessous est un carré latin, ce qui prouve que K est un sous-groupe de A_4 .

\times	e	σ_1	σ_2	σ_3
e	e	σ_1	σ_2	σ_3
σ_1	σ_1	e	σ_3	σ_2
σ_2	σ_2	σ_3	e	σ_1
σ_3	σ_3	σ_2	σ_1	e

Nous reconnaissons la table de multiplication du groupe de Klein, donc le groupe K est isomorphe au groupe de Klein.

28. a) H est un sous-groupe de S_5 . L'ensemble H est non vide, puisque $e \in H$. Soient σ et τ deux permutations de H . Alors $\sigma \circ \tau^{-1}$ est une permutation de S_5 telle que $\sigma \circ \tau^{-1}(1) = \sigma(1) = 1$, donc $\sigma \circ \tau^{-1} \in H$. Par conséquent, H est un sous-groupe de S_5 .

Ordre de H . L'application $H \rightarrow S_{\mathbf{N}_5 \setminus \{1\}}$, $\sigma \mapsto \sigma|_{\mathbf{N}_5 \setminus \{1\}}$ est une bijection. De plus, les ensembles $\mathbf{N}_5 \setminus \{1\}$ et \mathbf{N}_4 sont équipotents, donc H est un sous-groupe d'ordre $4! = 24$.

- b) Les transpositions $\sigma = (2, 3)$ et $\tau = (1, 2)$ sont deux éléments de K telles que $(\sigma \circ \tau^{-1})(1) = \sigma(2) = 3$, donc K n'est pas un sous-groupe de S_5 .

- c) F est un sous-groupe de S_n . L'ensemble F est non vide car $e \in F$. De plus, toute application injective d'un ensemble fini dans lui-même étant bijective, on a $F = \{\sigma \in S_n ; \sigma|_{N_r} \in S_{N_r}\}$. Ainsi, si σ et τ sont deux permutations de F alors $(\sigma \circ \tau^{-1})(N_r) = N_r$. Par conséquent, F est un sous-groupe de S_n .

Ordre de F . Soit $\varphi: N_n \setminus N_r \rightarrow N_{n-r}$ une bijection. Elle induit une bijection $S_{N_n \setminus N_r} \rightarrow S_{N_{n-r}}$, $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$. Alors l'application

$$\begin{aligned} \psi: F &\rightarrow S_{N_r} \times S_{N_{n-r}} \\ \sigma &\mapsto (\sigma|_{N_r}, \varphi \circ \sigma \circ \varphi^{-1}). \end{aligned}$$

est bijective, d'où nous déduisons que l'ordre du sous-groupe F est égal à

$$|S_{N_r}| \times |S_{N_{n-r}}| = r!(n-r)!$$

- 29.** a) La commutativité de π avec σ résulte de la commutativité de deux cycles disjoints. On montre que

$$\pi \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 4 & 8 & 9 & 7 & 2 & 3 & 1 \end{pmatrix} = \tau \circ \pi.$$

- b) Les permutations π , σ et τ sont d'ordre 3. Décomposons $\sigma \circ \tau$ en produit de cycles disjoints :

$$\begin{aligned} \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 4 & 8 & 9 & 7 & 1 & 2 & 3 \end{pmatrix} \\ &= (1, 5, 9, 3, 4, 8, 2, 6, 7). \end{aligned}$$

Nous en déduisons que la permutation $\sigma \circ \tau$ est d'ordre 9.

- c) On a

$$\begin{aligned} \tau \circ \sigma \circ \tau^{-1} &= (1, 4, 7)(2, 5, 8)(3, 6, 9)(4, 5, 6)(7, 8, 9)(1, 7, 4)(2, 8, 5)(3, 9, 6) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 5 & 6 & 8 & 9 & 7 \end{pmatrix} \\ &= (1, 2, 3)(7, 8, 9), \end{aligned}$$

et

$$\begin{aligned}\tau^{-1} \circ \sigma \circ \tau &= (1, 7, 4)(2, 8, 5)(3, 9, 6)(4, 5, 6)(7, 8, 9)(1, 4, 7)(2, 5, 8)(3, 6, 9) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 5 & 6 & 4 & 7 & 8 & 9 \end{pmatrix} \\ &= (1, 2, 3)(4, 5, 6).\end{aligned}$$

Enfin, s'il existe un entier k tel que $\pi = (\sigma \circ \tau)^k$, on peut prendre $k \in \{1, \dots, 8\}$ et d'après l'exercice III.13, $9/(9, k) = 3$, d'où $k = 3$ ou $k = 6$. On vérifie immédiatement que $k = 6$ convient.

32. a) La matrice X est diagonale, donc pour tout entier $k \geq 0$, on a

$$X^k = \begin{pmatrix} \alpha^k & 0 \\ 0 & \alpha^{-k} \end{pmatrix}.$$

De plus, $\alpha^k = 1$ si et seulement si k est un multiple de n . Nous en déduisons que X est une matrice d'ordre n . Les matrices Y et $XY = \begin{pmatrix} 0 & \alpha \\ \alpha^{-1} & 0 \end{pmatrix}$ sont d'ordre 2. Le théorème 3.74 nous permet alors de conclure que le groupe multiplicatif engendré par les matrices X et Y est isomorphe au groupe diédral D_n .

b) Les matrices U , V et UV sont respectivement d'ordre 4, 2 et 2, donc d'après le théorème 3.74, le groupe multiplicatif engendré par les matrices U et V est isomorphe au groupe diédral D_4 .

33. Les seuls éléments de S_2 sont l'identité et la transposition $(1, 2)$; la propriété à démontrer est donc trivialement vraie pour $n = 2$.

Supposons à présent la propriété vraie pour un entier $n \geq 2$ fixé et considérons une permutation $\sigma \in S_{n+1}$. Distinguons deux cas :

Cas $\sigma(n) = n$. On a alors $\sigma|_{\mathbb{N}_n} \in S_n$. Par hypothèse de récurrence, $\sigma|_{\mathbb{N}_n}$ est un produit de transpositions; il en est de même de σ .

Cas $\sigma(n) \neq n$. Posons $k = \sigma(n)$ et $\tau = (k, n)$. On vérifie que $\tau \circ \sigma(n) = n$, ce qui nous ramène au cas précédent; ainsi $\tau \circ \sigma$ est un produit de transpositions. Nous en déduisons que $\sigma = \tau \circ (\tau \circ \sigma)$ est aussi un produit de transpositions.

Sous-groupes normaux

1. Soit $H = \{e, h\}$ avec $h \neq e$. On sait déjà que $e \in \mathcal{Z}(G)$. Reste à montrer que $h \in \mathcal{Z}(G)$. Comme $H \triangleleft G$, pour tout $g \in G$, on a $ghg^{-1} \in H$. De plus $h \neq e$ implique que $ghg^{-1} = h$, c'est-à-dire que $gh = hg$ donc $h \in \mathcal{Z}(G)$.

2. D'après le lemme 4.32, il existe un unique homomorphisme $\bar{\alpha} \in \text{Hom}(\frac{G}{H}, \frac{G}{H'})$ tel que $\pi' \circ \alpha = \bar{\alpha} \circ \pi$ où $\pi: G \rightarrow \frac{G}{H}$ et $\pi': G \rightarrow \frac{G}{H'}$ sont les épimorphismes canoniques. La remarque 4.33 permet de conclure immédiatement que $\bar{\alpha}$ est un isomorphisme.

3. Soit $h = (h_1, h_2) \in H_1 \times H_2$. Pour tout $g = (g_1, g_2) \in G_1 \times G_2$, on a

$$\begin{aligned} ghg^{-1} &= (g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} \\ &= (g_1, g_2)(h_1, h_2)(g_1^{-1}, g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \in H_1 \times H_2 \quad (\text{car } H_1 \triangleleft G_1 \text{ et } H_2 \triangleleft G_2), \end{aligned}$$

donc

$$H_1 \times H_2 \triangleleft G_1 \times G_2.$$

Soit $\pi_i: G_i \rightarrow G_i/H_i$ ($i = 1, 2$) les épimorphismes canoniques. On construit l'homomorphisme

$$\begin{aligned} \pi = \pi_1 \times \pi_2: G_1 \times G_2 &\rightarrow (G_1/H_1) \times (G_2/H_2) \\ (g_1, g_2) &\mapsto (\pi_1(g_1), \pi_2(g_2)) \end{aligned}$$

La surjectivité de π résulte immédiatement de sa définition. Soit $(g_1, g_2) \in G_1 \times G_2$. On a

$$(g_1, g_2) \in \text{Ker } \pi \iff (g_1, g_2) \in \text{Ker } \pi_1 \times \text{Ker } \pi_2 = H_1 \times H_2.$$

Le 1^{er} théorème d'isomorphisme permet de conclure :

$$\frac{G_1 \times G_2}{H_1 \times H_2} \simeq \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$

4. Notons a un générateur du groupe cyclique C_4 . Les sous-groupes $H_1 = C_2 \times (e)$ et $H_2 = (e) \times \langle a^2 \rangle$ sont cycliques d'ordre 2, donc $H_1 \simeq H_2$. En utilisant le résultat de l'exercice 4.4, nous établissons que

$$\frac{G}{H_1} \simeq \frac{C_2}{C_2} \times \frac{C_4}{(e)} = (e) \times C_4 \simeq C_4 \quad \text{et} \quad \frac{G}{H_2} \simeq \frac{C_2}{(e)} \times \frac{C_4}{\langle a^2 \rangle} \simeq C_2 \times C_2.$$

Comme le groupe de Klein $C_2 \times C_2$ n'est pas cyclique (exemple 1.86), les groupes C_4 et $C_2 \times C_2$ ne sont pas isomorphes, donc $G/H_1 \not\simeq G/H_2$.

Les sous-groupes $K_1 = (e) \times C_4$ et $K_2 = C_2 \times \langle a^2 \rangle \simeq C_2 \times C_2$ ne sont pas isomorphes. En revanche, les groupes quotients

$$\frac{G}{K_1} = \frac{C_2}{(e)} \times \frac{C_4}{C_4} \simeq C_2 \times (e) \quad \text{et} \quad \frac{G}{K_2} = \frac{C_2}{C_2} \times \frac{C_4}{\langle a^2 \rangle} \simeq (e) \times C_2$$

sont isomorphes.

5. Posons $G_1 = \frac{Z}{(4)}$, $H_1 = \langle \bar{2} \rangle$, $G_2 = D_2$ et $H_2 = \langle a \rangle$ où $a \in G_2 \setminus \{e\}$. Les groupes G_1 et G_2 sont des groupes d'ordre 4. Le groupe G_1 est cyclique, le groupe G_2 n'est pas cyclique, donc ils ne sont pas isomorphes. Ils sont abéliens, donc $H_1 \triangleleft G_1$ et $H_2 \triangleleft G_2$. De plus,

$$o\left(\frac{G_i}{H_i}\right) = \frac{o(G_i)}{o(H_i)} = \frac{4}{2} = 2 \quad (i = 1, 2),$$

donc les groupes quotients sont cycliques. On en déduit que

$$\frac{G_1}{H_1} \simeq \frac{G_2}{H_2}.$$

6. Pour tout $(a, b, c) \in \mathbf{K}^3$, on note $M_{a,b,c}$ la matrice

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

En développant le déterminant par rapport à la première colonne, on trouve immédiatement $\det(M_{a,b,c}) = 1$, donc $\Gamma \subset \text{GL}_3(\mathbf{K})$.

Soit $M_{a,b,c} \in \Gamma$ et $M_{a',b',c'} \in \Gamma$. On a

$$M_{a,b,c}M_{a',b',c'} = M_{a+a',b+ac'+b',c+c'}$$

et

$$M_{a,b,c}^{-1} = M_{-a,ac-b,-c},$$

donc Γ est un sous-groupe de $\text{GL}_3(\mathbf{K})$.

D'après l'une des formules ci-dessus,

$$M_{a,b,c} \in Z(\Gamma) \iff \forall (a',b',c') \in \mathbf{K}^2, \quad ac' = a'c.$$

On trouve $a = 0$ et $c = 0$. Ainsi

$$Z(\Gamma) = \{M_{0,b,0}; b \in \mathbf{K}\}.$$

L'application $\varphi: \mathbf{K} \rightarrow Z(\Gamma)$ définie par

$$\varphi(x) = M_{0,x,0}$$

est un homomorphisme. Il est clairement bijectif, donc $Z(\Gamma) \simeq \mathbf{K}$.

Soit l'application $\psi: \Gamma \rightarrow \mathbf{K} \times \mathbf{K}$ définie par

$$\psi(M_{a,b,c}) = (a, c).$$

ψ est un homomorphisme de groupes. En effet, pour tout $(M_{a,b,c}, M_{a',b',c'}) \in \Gamma^2$,

$$\begin{aligned} \psi(M_{a,b,c}M_{a',b',c'}) &= \psi(M_{a+a',b+ac'+b',c+c'}) \\ &= (a+a', c+c') \\ &= (a, c) + (a', c') \\ &= \psi(M_{a,b,c}) + \psi(M_{a',b',c'}). \end{aligned}$$

Il est surjectif et $\text{Ker } \psi = Z(\Gamma)$. Le 1^{er} théorème d'isomorphisme permet de conclure :

$$\frac{\Gamma}{Z(\Gamma)} \simeq \mathbf{K} \times \mathbf{K}.$$

8. Nous savons déjà que $A_3 \triangleleft S_3$ (théorème 4.7). Soit $H \neq (e)$ un sous-groupe propre normal de S_3 . Alors, d'après le théorème de Lagrange, $o(H) \in \{2, 3\}$. Supposons que $o(H) = 2$, alors $H = \langle \tau \rangle$ où τ est une transposition. Notons $\tau = (i, j)$, et soit la transposition $\gamma = (i, k)$ où $k \in \mathbb{N}_3 \setminus \{i, j\}$. Alors $\gamma \circ \tau \circ \gamma^{-1} = (j, k) \notin H$, donc $H \not\triangleleft S_3$. On en déduit que $o(H) = 3$. Le sous-groupe H est cyclique (car d'ordre premier) et est donc engendré par l'un des cycles $\sigma_1 = (1, 2, 3)$ ou $\sigma_2 = (1, 3, 2)$. On remarque que $\sigma_2 = \sigma_1^2$ et que $\sigma_1 \in A_3$ donc $H = \langle \sigma_1 \rangle \subseteq A_3$. Comme $|A_3| = 3!/2 = 3$, il vient $H = A_3$. En résumé, A_3 est l'unique sous-groupe propre normal de S_3 différent de (e) .

9. H est un sous-groupe de S_4 : Son unique élément $\neq e$ est un produit de deux transpositions à supports disjoints donc est d'ordre 2. Il s'ensuit que H est stable pour l'inverse et le produit, donc $H < S_4$.

K est un sous-groupe de S_4 : Les éléments $\neq e$ de K sont des transpositions à supports disjoints, donc ils sont d'ordre 2 Il s'ensuit que K est stable pour l'inverse. Reste à vérifier la stabilité du produit. Sachant que dans un groupe, si deux éléments ainsi que leur produit sont d'ordre 2 alors ils commutent (exercice 5, chapitre I), il suffit d'effectuer les produits suivants :

$$(1, 2)(3, 4)(1, 3)(2, 4) = (1, 4)(2, 3)$$

$$(1, 2)(3, 4)(1, 4)(2, 3) = (1, 3)(2, 4)$$

$$(1, 3)(2, 4)(1, 4)(2, 3) = (1, 2)(3, 4).$$

On a bien $K < S_4$.

K est un sous-groupe normal de S_4 : Soit $\sigma \in S_4$ et $(i, j)(k, l)$ un produit de transpositions à supports disjoints. On a

$$\begin{aligned} \sigma \circ (i, j) \circ (k, l) \circ \sigma^{-1} &= \sigma \circ (i, j) \sigma^{-1} \sigma \circ (k, l) \circ \sigma^{-1} \\ &= (\sigma(i), \sigma(j)) \circ (\sigma(k), \sigma(l)). \end{aligned}$$

Les deux transpositions $(\sigma(i), \sigma(j))$ et $(\sigma(k), \sigma(l))$ sont disjointes, et K contient toutes les permutations qui sont le produit de deux transpositions à supports disjoints, donc

$$\sigma \circ (i, j) \circ (k, l) \circ \sigma^{-1} \in K.$$

H est normal dans K : Le sous-groupe H est inclus dans le sous-groupe abélien K donc $H \triangleleft K$.

H n'est pas normal dans S_4 : Soit $\sigma = (2, 3)$. Alors

$$\begin{aligned}\sigma(12)(34)\sigma^{-1} &= \sigma(12)\sigma^{-1}\sigma(34)\sigma^{-1} \\ &= (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) \\ &= (13)(24) \notin H,\end{aligned}$$

Donc $H \not\triangleleft S_4$.

13. a) Le groupe $\frac{G}{H}$ est d'ordre n , donc pour tout $x \in G$, on a $\overline{x^n} = \overline{\bar{x}^n} = \bar{e}$, c'est-à-dire $x^n \in H$.
- b) Soit $x \in G$ et $d = o(\bar{x})$. D'après le théorème de Lagrange $d \mid n$. L'inclusion $x^k \in H$ implique $\overline{x^k} = \bar{e}$ donc $d \mid k$. Comme $(k, n) = 1$, on en déduit que $d = 1$, c'est-à-dire $\bar{x} = \bar{e}$ puis $x \in H$.

15. a) Notons k l'ordre de \bar{x} .

Montrons que k divise n . Cela résulte de $\overline{x^n} = \overline{\bar{x}^n} = \bar{e}$ et du corollaire 3.7.

Montrons à présent que n divise k . On a $x^k \in H$ puisque $\overline{x^k} = \overline{\bar{x}^k} = \bar{e}$. Il s'ensuit que $o(x^k)$ divise m (corollaire 2.10). Or, nous avons montré à l'exercice 3.13 que $o(x^k) = n / \text{pgcd}(n, k)$. Par conséquent, $o(x^k)$ divise également n . Or n et m sont premiers entre, donc $o(x^k) = 1$, si bien que n divise k . Finalement, $n = k$; autrement dit, on a bien $o(\bar{x}) = n$.

- b) Les entiers m et n étant premiers entre eux, il existe deux entiers u et v tels que $mu + nv = 1$. Nous en déduisons que $x = yh$ où $y = x^{mu}$ et $h = x^{nv}$. Étant donné que $o(\bar{x}) = n$, on a $x^n \in H$, donc $h \in H$, puis $y \in \bar{x}$. Il nous reste à montrer que $o(y) = n$.

Notons p l'ordre de x et k l'entier tel que $p = kn$ ($o(\bar{x})$ divise $o(x)$). On a $m = o(H)$, or $o(x^n) = p / \text{pgcd}(p, n) = kn / \text{pgcd}(kn, n) = nk / n = k$. Or $x^n \in H$ implique que $o(x^n)$ divise $m = o(H)$, par conséquent k divise m . Soit l l'entier tel que $m = kl$. De $1 = mu + nv = k(lu) + nv$, on déduit que les entiers lu et n sont premiers entre eux, ce qui

nous permet de conclure que

$$o(y) = \frac{p}{\text{pgcd}(p, mu)} = \frac{kn}{\text{pgcd}(kn, klu)} = \frac{n}{\text{pgcd}(n, lu)} = n.$$

16. Démontrons par récurrence forte sur l'entier n que l'assertion suivante est vraie pour tout $n \geq 2$:

Soit G un groupe abélien d'ordre n . Si p est un diviseur premier de n , alors G contient un élément d'ordre p .

Soit G est un groupe d'ordre 2. L'unique diviseur premier de 2 est 2, or l'unique élément x distinct de l'élément neutre est d'ordre 2, donc l'assertion est vraie pour $n = 2$.

Soit un entier $k > 1$. Supposons que l'assertion est vraie pour tout entier n tel que $2 \leq n \leq k$. Soient G un groupe d'ordre $k + 1$ et p un diviseur premier de $k + 1$. Distinguons deux cas.

Cas 1: le groupe G n'a pas d'autres sous-groupes que G et $\{e\}$. Dans ce cas, G est cyclique d'ordre premier (proposition 3.16), donc tout élément de G distinct de e est d'ordre p (proposition 3.18).

Cas 2: le groupe G admet un sous-groupe propre $H \neq \{e\}$. Comme G est abélien, le sous-groupe H est normal dans G et $\frac{G}{H}$ est un groupe abélien (proposition 2.24). De $o(G) = o\left(\frac{G}{H}\right) o(H)$ (proposition 2.15), on déduit que p divise $o\left(\frac{G}{H}\right)$ ou $o(H)$. Supposons que p divise $o(H)$. Étant donné que $2 \leq o(H) \leq n$, d'après l'hypothèse de récurrence, il existe dans H un élément d'ordre p . Supposons que p divise $o\left(\frac{G}{H}\right)$. Comme $2 \leq o\left(\frac{G}{H}\right) \leq n$, d'après l'hypothèse de récurrence, le groupe $\frac{G}{H}$ contient un élément d'ordre p et celui-ci possède un représentant d'ordre p dans G (exercice 4.15).

Dans les deux cas, nous avons montré que l'assertion est vraie pour $n = k + 1$. Le principe de la récurrence forte nous permet alors de conclure que l'assertion est vraie pour tout entier $n \geq 2$.

17. a) Soient σ et τ deux permutations de l'ensemble E .

- 1) Pour tout $x \in E$, on a $\sigma(x) \neq x$ si et seulement si $x \neq \sigma^{-1}(x)$, d'où $s(\sigma) = s(\sigma^{-1})$.

- 2) Soit $x \in s(\sigma \circ \tau)$. Si $x \notin s(\tau)$, alors $(\sigma \circ \tau)(x) \neq x$ devient $\sigma(x) \neq x$, donc $x \in s(\sigma)$. Par conséquent, $s(\sigma \circ \tau) \subseteq s(\sigma) \cup s(\tau)$.
- 3) Soit $x \in E$. On a $(\sigma \circ \tau \circ \sigma^{-1})(x) \neq x$ si et seulement si $\tau(\sigma^{-1}(x)) \neq \sigma^{-1}(x)$, d'où $s(\sigma \circ \tau \circ \sigma^{-1}) = s(\tau)$.
- 4) Soit $x \in E$. Si $x \notin s(\sigma) \cup s(\tau)$, alors $(\sigma \circ \tau)(x) = \sigma(x) = x$ et $(\tau \circ \sigma)(x) = \tau(x) = x$. Si $x \in s(\sigma)$ alors $x \notin s(\tau)$ d'où $(\sigma \circ \tau)(x) = \sigma(x)$. Remarquons que $\sigma(x) \in s(\sigma)$ car $\sigma(\sigma(x)) \neq \sigma(x)$, donc $(\tau \circ \sigma)(x) = \sigma(x)$. De même, si $x \in s(\tau)$ on a $(\tau \circ \sigma)(x) = (\sigma \circ \tau)(x)$. Nous concluons que $\sigma \circ \tau = \tau \circ \sigma$.
- b) $S_{(E)}$ est un sous-groupe normal de S_E . L'ensemble $S_{(E)}$ est non vide; en effet, $\text{id}_E \in S_{(E)}$. Soient σ et τ deux permutations de E à support fini. D'après les propriétés 1 et 2, on a $s(\sigma \circ \tau^{-1}) \subseteq s(\sigma) \cup s(\tau^{-1}) = s(\sigma) \cup s(\tau)$. Nous en déduisons que $|s(\sigma \circ \tau^{-1})| \leq |s(\sigma)| + |s(\tau)| < \infty$, donc $S_{(E)}$ est un sous-groupe de S_E .

De plus, d'après la propriété 3, pour tout $\sigma \in S_{(E)}$ et $\tau \in S_E$, on a $|s(\tau \circ \sigma \circ \tau^{-1})| = |\tau(s(\sigma))| = |s(\sigma)| < \infty$, donc $S_{(E)} \triangleleft S_E$.

Les groupes S_E et $S_{(E)}$ sont égaux si et seulement si E est fini. Quel que soit l'ensemble E , on a toujours $S_{(E)} \subseteq S_E$. Si E est fini, il est clair que $S_E \subseteq S_{(E)}$, donc $S_E = S_{(E)}$. Si E est infini, considérons une suite injective $(x_n)_{n \geq 0}$ d'éléments de E . Alors la permutation σ définie par

$$\begin{cases} \sigma(x_{2i}) = x_{2i+1} \\ \sigma(x_{2i+1}) = x_{2i} \end{cases}$$

est à support infini, ce qui montre que $S_{(E)}$ est un sous-groupe propre de S_E . Par conséquent, si $S_{(E)} = S_E$, alors E est fini.

Si E est un ensemble infini, alors $S_{(E)}$ est un groupe infini dont tout élément est d'ordre fini et $S_E/S_{(E)}$ est un groupe infini. Soit $(x_n)_{n \geq 0}$ une suite d'éléments de E . Alors $\{(x_0, x_k); k \in \mathbf{N}^*\}$ est une famille infinie de transpositions de $S_{(E)}$, donc $S_{(E)}$ est un groupe infini.

Soit $\sigma \in S_{(E)}$. Alors $\sigma \parallel_{s(\sigma)} \in S_{s(\sigma)}$. Notons n l'ordre de $\sigma \parallel_{s(\sigma)}$. Il est clair que $\sigma^n = e$, donc σ est d'ordre fini. Ainsi, tout élément de $S_{(E)}$ est d'ordre fini.

Puisque $S_{(E)}$ est un sous-groupe normal de S_E , l'ensemble $S_E/S_{(E)}$ est un groupe. Si ce groupe est fini, alors pour toute permutation $\sigma \in S_E$, il existe un entier $n > 0$ tel que $\sigma^n \in S_{(E)}$. Comme $S_{(E)}$ est fini, cela implique que σ est d'ordre fini. Soit $(x_n)_{n \in \mathbf{Z}}$ une suite injective d'éléments de E . Alors le cycle $\gamma = (\dots, x_2, x_{-1}, x_0, x_1, x_2, \dots)$ défini par $\gamma(x_i) = x_{i+1}$ pour tout $i \in \mathbf{Z}$, est d'ordre infini. Il s'ensuit que le groupe $S_E/S_{(E)}$ est d'ordre infini.

19. Nous avons $H \triangleleft G$ et $Z(H) \sqsubset H$ (proposition 4.43), donc $Z(H) \triangleleft G$ (proposition 4.44).

Dans le groupe Q_8 (exercice 4.18), considérons le sous-groupe normal $H = \langle a \rangle$. Étant donné que $Z(H) = H$ et que H est d'ordre 4 alors que $Z(Q_8)$ est d'ordre 2, l'inclusion $Z(H) \subseteq Z(Q_8)$ est exclue.

21. Soient g et g' deux éléments conjugués d'un groupe fini G . Il existe $x \in G$ tel que $g' = xgx^{-1}$, d'où $g'^n = xg^n x^{-1}$ pour tout $n \in \mathbf{N}$. Il s'ensuit que $g'^n = e$ si et seulement si $g^n = e$. Par conséquent, les éléments g et g' ont le même ordre.

22. Soient les décompositions canoniques des permutations u et v en produit de cycles disjoints, $u = (1, 2, 5)(4, 6)$ et $v = (1, 5)(2, 3, 4)$, et soit $\sigma \in S_6$ telle que $(\sigma(1), \sigma(2), \sigma(5)) = (2, 3, 4)$ et $(\sigma(4), \sigma(6)) = (1, 5)$, par exemple

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 1 & 4 & 5 \end{pmatrix}.$$

Alors en utilisant le résultat de la question a) de l'exercice III.24, on trouve

$$\begin{aligned} \sigma \circ u \circ \sigma^{-1} &= \sigma \circ (1, 2, 5) \circ \sigma^{-1} \circ \sigma \circ (4, 6) \circ \sigma^{-1} \\ &= (\sigma(1), \sigma(2), \sigma(5))(\sigma(4), \sigma(6)) \\ &= (2, 3, 4)(1, 5) \\ &= v, \end{aligned}$$

ainsi les permutations u et v sont conjuguées dans S_6 .

Groupe opérant sur un ensemble

1. Pour tous nombres réels a, b et c , notons $M(a, b, c)$ la matrice

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

de sorte que

$$G = \{M(a, b, c); ac \neq 0\}.$$

On a $\det(M(a, b, c)) = ac$, donc $G \subseteq GL(2, \mathbf{R})$. L'ensemble G est non vide, car il contient la matrice identité $I = M(1, 0, 1)$. Soient $M(a, b, c)$ et $M(a', b', c')$ deux matrices de G . Alors

$$M(a, b, c)^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = M\left(\frac{1}{a}, -\frac{b}{ac}, \frac{1}{c}\right) \in G$$

et

$$M(a, b, c)M(a', b', c') = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} = M(aa', ab' + bc', cc') \in G$$

donc G est un sous-groupe de $GL(2, \mathbf{R})$.

L'application

$$G \times \mathbf{R} \rightarrow \mathbf{R}, \quad (M(a, b, c), x) \mapsto M(a, b, c) \cdot x = \frac{ax + b}{c}$$

définit une action de G sur \mathbf{R} car elle vérifie les deux conditions suivantes :

— pour tout $x \in \mathbf{R}$, on a $I \cdot x = x$;

— pour toutes matrices $M(a, b, c)$ et $M(a', b', c')$ de G , on a

$$\begin{aligned} M(a, b, c) \cdot (M(a', b', c') \cdot x) &= M(a, b, c) \cdot \frac{a'x + b'}{c'} \\ &= \frac{a \frac{a'x + b'}{c'} + b}{c} \\ &= \frac{aa'x + ab' + bc'}{cc'} \\ &= M(aa', ab' + bc', cc') \cdot x \\ &= (M(a, b, c)M(a', b', c')) \cdot x. \end{aligned}$$

Le noyau de cette action est le sous-groupe

$$\begin{aligned} &\{M(a, b, c) \in G; M(a, b, c) \cdot x = x \text{ pour tout } x \in \mathbf{R}\} \\ &= \{M(a, b, c) \in G; (ax + b)/c = x \text{ pour tout } x \in \mathbf{R}\} \\ &= \{M(a, b, c) \in G; (a - c)x = -b \text{ pour tout } x \in \mathbf{R}\} \\ &= \{M(a, b, c) \in G; a = c \text{ et } b = 0\} \\ &= \{aI; a \in \mathbf{R}^*\}. \end{aligned}$$

Le stabilisateur de 0 est le sous-groupe

$$\begin{aligned} G_0 &= \{M(a, b, c) \in G; M(a, b, c) \cdot 0 = 0\} \\ &= \{M(a, b, c) \in G; b/c = 0\} \\ &= \{M(a, 0, c) \in G\}, \end{aligned}$$

c'est-à-dire le sous-groupe de G des matrices diagonales.

L'orbite de 0 est l'ensemble

$$\begin{aligned} \Omega_0 &= \{M(a, b, c) \cdot 0; M(a, b, c) \in G\} \\ &= \{b/c; (b, c) \in \mathbf{R} \times \mathbf{R}^*\} \\ &= \mathbf{R}. \end{aligned}$$

2. a) Soit $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des G -orbites non ponctuelles. Puisque $E_G = \emptyset$, on a l'égalité

$$17 = \sum_{i=1}^r |\Omega_{x_i}|.$$

Pour chaque $i \in \{1, \dots, r\}$, $|\Omega_{x_i}|$ divise $|G| = 15$, donc $|\Omega_{x_i}| \in \{3, 5, 15\}$. Notons α (resp. β , γ) le nombre de G -orbites de longueur 3 (resp. 5, 15). Le triplet (α, β, γ) vérifie l'équation

$$17 = 3x + 5y + 15z$$

dont l'unique solution dans \mathbf{N}^3 est $(4, 1, 0)$. Nous concluons qu'il y a 5 G -orbites : 4 G -orbites de longueur 3 et une G -orbite de longueur 5.

- b) Soit $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des G -orbites non ponctuelles. Supposons que E_G soit vide. On a alors

$$19 = \sum_{i=1}^r |\Omega_{x_i}|.$$

Pour chaque $i \in \{1, \dots, r\}$, $|\Omega_{x_i}|$ divise $|G| = 33$, donc $|\Omega_{x_i}| \in \{3, 11, 33\}$. Soit α (resp. β , γ) le nombre de G -orbites de longueur 3 (resp. 11, 33). Le triplet (α, β, γ) est solution de l'équation

$$19 = 3x + 11y + 33z.$$

Or, nous pouvons facilement vérifier que cette équation n'a pas de solution dans \mathbf{N}^3 . Contradiction. Nous en déduisons que l'ensemble E_G des points fixes n'est pas vide.

3. a) Soit $G = \langle (1, 2, 3) \rangle = \{e, (1, 2, 3), (1, 3, 2)\}$. Nous avons une partition de \mathbf{N}_4 en exactement deux G -orbites : $\Omega_1 = \{1, 2, 3\}$ et $\Omega_4 = \{4\}$. Les stabilisateurs de l'élément $i \in \mathbf{N}_4$ sont les permutations $\sigma \in G$ telles que $i \notin \text{supp}(\sigma)$, d'où $G_1 = G_2 = G_3 = \{e\}$ et $G_4 = G$.
- b) Soit $G = \langle (1, 2), (3, 4) \rangle = \{e, (1, 2), (3, 4), (1, 2)(3, 4)\}$. Le G -ensemble \mathbf{N}_4 a deux orbites, $\Omega_1 = \{1, 2\}$ et $\Omega_3 = \{3, 4\}$, et les stabilisateurs sont $G_1 = G_2 = \{e, (3, 4)\}$ et $G_3 = G_4 = \{e, (1, 2)\}$.
- c) Soit $G = A_4$. C'est un groupe d'ordre 12 dont les éléments sont e , les produits de deux transpositions à supports disjoints et les 3-cycles. Déterminons l'orbite de 1. Comme G contient les permutations $(1, 2)(3, 4)$, $(1, 3)(2, 4)$ et $(1, 4)(2, 3)$, nous en déduisons

que $\Omega_1 = \mathbf{N}_4$, et donc qu'il n'y a qu'une seule G -orbite. Les stabilisateurs sont $G_1 = \{e, (2, 3, 4), (2, 4, 3)\}$, $G_2 = \{e, (1, 3, 4), (1, 4, 3)\}$, $G_3 = \{e, (1, 2, 4), (1, 4, 2)\}$ et $G_4 = \{e, (1, 2, 3), (1, 3, 2)\}$.

4. a) On note I la matrice identité du groupe G . Pour tout $(x, y) \in \mathbf{R}^2$, on a

$$(x, y) \cdot I = (x, y).$$

L'égalité

$$(x, y) \cdot AB = ((x, y) \cdot A) \cdot B$$

pour tous $(x, y) \in \mathbf{R}^2$ et $(A, B) \in G^2$ est une conséquence de la distributivité de la multiplication matricielle. Ainsi G opère bien à droite sur \mathbf{R}^2 .

- b) La correspondance

$$\begin{aligned} \mathcal{D} \times G &\rightarrow \mathcal{D} \\ (\text{Vect}\{u\}, A) &\mapsto \text{Vect}\{u \cdot A\}. \end{aligned}$$

est une application; en effet, si u et v sont deux vecteurs non nuls tels que $\text{Vect}\{u\} = \text{Vect}\{v\}$, alors il existe $\lambda \in \mathbf{R}^*$ tel que $v = \lambda u$, donc $v \cdot A = \lambda(u \cdot A)$, si bien que $\text{Vect}\{v \cdot A\} = \text{Vect}\{u \cdot A\}$.

Cette application définit une action à droite de G sur \mathcal{D} . Soient A et B deux matrices de G et u un vecteur non nul de \mathbf{R}^2 . On a

$$\text{Vect}\{u\} \cdot I = \text{Vect}\{u \cdot I\} = \text{Vect}\{u\}$$

et

$$\begin{aligned} \text{Vect}\{u\} \cdot (AB) &= \text{Vect}\{u \cdot (AB)\} \\ &= \text{Vect}\{(u \cdot A) \cdot B\} \\ &= \text{Vect}\{u \cdot A\} \cdot B \\ &= (\text{Vect}\{u\} \cdot A) \cdot B \end{aligned}$$

Déterminons le sous-groupe d'isotropie G_D de la droite $D = \text{Vect}\{(2, 1)\}$.

Méthode 1. On a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_D$ si et seulement si $D \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = D$, c'est-à-dire si et seulement si les vecteurs $(2a + c, 2b + d)$ et $(2, 1)$ sont colinéaires, donc

$$G_D = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G; 2a - 4b + c - 2d = 0 \right\}.$$

Méthode 2. Soit $A \in G$. Alors $A \in G_D$ si et seulement si il existe $\lambda \in \mathbf{R}$ tel que

$$(2, 1) \cdot A = \lambda(2, 1).$$

c'est-à-dire, si et seulement si

$${}^t A \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

où $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ est la matrice du vecteur $(2, 1)$ dans la base canonique $\mathcal{B} = (e_1, e_2)$. Notons u l'isomorphisme linéaire de \mathbf{R}^2 tel que

$${}^t A = \text{Mat}_{\mathcal{B}}(u).$$

Considérons la base $\mathcal{C} = (f_1, f_2)$ où $f_1 = (2, 1)$ et $f_2 = (-1, 2)$. On a

$$\text{Mat}_{\mathcal{C}}(u) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

avec $(a, b, c) \in \mathbf{R}^3$ et $ac \neq 0$. La matrice de passage de la base \mathcal{B} à la base \mathcal{C} est

$$P_{\mathcal{B}, \mathcal{C}} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}.$$

Son inverse est

$$P_{\mathcal{B}, \mathcal{C}}^{-1} = \frac{1}{5} \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}.$$

Du coup,

$$\begin{aligned} \text{Mat}_{\mathcal{B}}(u) &= P_{\mathcal{B}, \mathcal{C}} \text{Mat}_{\mathcal{C}}(u) P_{\mathcal{B}, \mathcal{C}}^{-1} \\ &= \frac{1}{5} \begin{pmatrix} 4a - 2b + c & 2a + 4b - 2c \\ 2a - b - 2c & a + 2b + 4c \end{pmatrix}. \end{aligned}$$

Étant donné que $\lambda M \in G_D$ pour tout $(\lambda, M) \in \mathbf{R} \times G_D$, on conclut que

$$G_D = \left\{ \begin{pmatrix} 4a - 2b + c & 2a - b - 2c \\ 2a + 4b - 2c & a + 2b + 4c \end{pmatrix}; (a, b, c) \in \mathbf{R}^3, ac \neq 0 \right\}.$$

Méthode 3. Soit $E_1 = \text{Vect}\{e_1\}$ la droite engendrée par le premier vecteur de la base canonique de \mathbf{R}^2 . Son stabilisateur G_{E_1} est l'ensemble des matrices de $GL(2, \mathbf{R})$ telles que

$$E_1 \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = E_1$$

soit

$$\text{Vect}\{(a, b)\} = E_1,$$

donc

$$G_{E_1} = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}; ad \neq 0 \right\}.$$

La matrice $A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ appartient à $GL(2, \mathbf{R})$ et

$$D = E_1 \cdot A,$$

donc, d'après le théorème 5.18 adaptée aux actions à droite, on a

$$\begin{aligned} G_D &= A^{-1} G_{E_1} A \\ &= \left\{ \begin{pmatrix} 4a - 2c & 2a - c - 2d \\ 4c & 2c + 4d \end{pmatrix}; (a, c, d) \in \mathbf{R}^3, ad \neq 0 \right\}. \end{aligned}$$

Déterminons l'orbite de la droite D . Soient $D_1 = \text{Vect}\{(x_1, y_1)\}$ et $D_2 = \text{Vect}\{(x_2, y_2)\}$ deux droites du plan. Du cours d'algèbre linéaire, nous savons qu'il existe une matrice $A \in G$ telle que

$$A \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Il s'ensuit que

$$(x_1, y_1) \cdot {}^t A = (x_2, y_2),$$

donc

$$D_1 \cdot A = D_2,$$

ce qui prouve que $\Omega_D = \mathcal{D}$. D'après le théorème 5.19, la H-orbite de D contient $|\mathcal{H}|/|H_D| = 4$ droites :

$$\begin{aligned} D &= \text{Vect}\{(2, 1)\}, & D \cdot A &= \text{Vect}\{(-2, 1)\}, \\ D \cdot B &= \text{Vect}\{(1, -2)\}, & D \cdot AB &= \text{Vect}\{(1, 2)\}. \end{aligned}$$

c) Soient

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie facilement que $o(A) = 2$, $o(B) = 4$ et $o(AB) = 2$, donc le sous-groupe H est isomorphe au groupe diédral D_4 (proposition 3.74) d'ordre 8 (proposition 3.71) et on a

$$H = \{I, A, B, B^2, B^3, AB, AB^2, AB^3\}$$

où

$$\begin{aligned} B^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, & B^3 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & AB &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ AB^2 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & AB^3 &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \end{aligned}$$

Le stabilisateur de la droite D pour l'action de H sur \mathcal{D} est $H_D = G_D \cap H$ (remarque 5.39), donc $H_D = \{I, B^2\}$.

5. Pour toute matrice $M = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \Gamma$, on a

$$(0, 0)M = (0, 0), \quad (1, 1)M = (a, b), \quad \text{et} \quad (0, 1)M = (0, b),$$

d'où nous déduisons immédiatement que

$$\Gamma_{(0,0)} = \Gamma, \quad \Gamma_{(1,1)} = I \quad \text{et} \quad \Gamma_{(0,1)} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}; a > 0 \right\}.$$

Les 9 Γ -orbites sont :

— les quatre quadrants

$$\Gamma_{(1,1)} = \{(x, y) \in \mathbf{R}^2; x > 0, y > 0\},$$

$$\Gamma_{(-1,1)} = \{(x, y) \in \mathbf{R}^2; x < 0, y > 0\},$$

$$\Gamma_{(-1,-1)} = \{(x, y) \in \mathbf{R}^2; x < 0, y < 0\},$$

$$\Gamma_{(1,-1)} = \{(x, y) \in \mathbf{R}^2; x > 0, y < 0\};$$

— les quatre demi-droites

$$\Gamma_{(1,0)} = \{(x, y) \in \mathbf{R}^2; x > 0, y = 0\},$$

$$\Gamma_{(0,1)} = \{(x, y) \in \mathbf{R}^2; x = 0, y > 0\},$$

$$\Gamma_{(-1,0)} = \{(x, y) \in \mathbf{R}^2; x < 0, y = 0\},$$

$$\Gamma_{(0,-1)} = \{(x, y) \in \mathbf{R}^2; x = 0, y < 0\};$$

— le point $\Gamma_{(0,0)} = (0, 0)$.

7. a) Soient $(x, y) \in \mathbf{N}_n^2$. Étant donné que G opère transitivement sur \mathbf{N}_n , il existe une permutation $\pi \in G$ telle que $\pi(x) = y$. Soit $\sigma \in H_x$. Comme $H \triangleleft G$, on a $\pi \circ \sigma \circ \pi^{-1} \in H$. De plus, $(\pi \circ \sigma \circ \pi^{-1})(y) = (\pi \circ \sigma)(x) = \pi(x) = y$, donc $\pi \circ \sigma \circ \pi^{-1} \in H_y$. Il s'ensuit que $\pi H_x \pi^{-1} \subseteq H_y$, d'où $o(H_x) \leq o(H_y)$. Par symétrie, l'inégalité opposée est également vraie, donc $o(H_y) = o(H_x)$. La conclusion vient du théorème 5.19 et de la proposition 2.15 :

$$|\Omega_x| = o(H) / o(H_x) = o(H) / o(H_y) = |\Omega_y|.$$

- b) L'énoncé de la question n'est pas correct. En effet, si $H = (e)$, alors les H -orbites de \mathbf{N}_n sont ponctuelles. Puisque $n \geq 2$, nous en déduisons que H est intransitif sur \mathbf{N}_n . Dans la suite, nous démontrerons le résultat suivant :

Si H est non trivial et que n est un nombre premier, alors H opère transitivement sur \mathbf{N}_n .

Puisque les H-orbites forment une partition de N_n , le nombre d'orbits r , leur cardinal m ainsi que n sont liés par la relation $rm = n$. La primalité de n implique que $r = 1$ ou $r = n$. Le cas $r = n$ est exclu, car toutes les orbites seraient alors ponctuelles, ce qui entraînerait $H = (e)$. Nous en déduisons que $r = 1$; autrement dit, le groupe H opère transitivement sur N_n .

10. a) — Remarquons que $G_X = \bigcap_{x \in X} G_x$ et que pour tout $x \in X$, on a $G_{gx} = gG_xg^{-1}$ (théorème 5.18). Il s'ensuit que

$$G_{gX} = \bigcap_{x \in X} G_{gx} = \bigcap_{x \in X} gG_xg^{-1} = g \left(\bigcap_{x \in X} G_x \right) g^{-1} = gG_Xg^{-1}.$$

— L'action de G sur E induit une action de G sur $\mathcal{P}(E)$ par l'application $G \times \mathcal{P}(E) \rightarrow \mathcal{P}(E)$, $(g, X) \mapsto gX$. Les ensembles G_X^* et G_{gX}^* sont alors les stabilisateurs de X et gX pour cette action. L'égalité $G_{gX}^* = gG_X^*g^{-1}$ résulte alors du théorème 5.18.

- b) Bien entendu, G_X , égal à l'intersection des sous-groupes $\{G_x; x \in X\}$, est un sous-groupe de G. De même, G_X^* est un sous-groupe puisque c'est le stabilisateur pour l'action de G sur $\mathcal{P}(E)$ décrite à la question précédente.

Enfin, pour tout $g \in G_X^*$, on a $gG_Xg^{-1} = G_{gX} = G_X$, donc $G_X \triangleleft G_X^*$.

- c) Pour tout $g \in G$, on a $gX = X$, d'où $G_X^* = G$. D'après la question précédente, on a $G_X \triangleleft G$. Soit l'homomorphisme $G \rightarrow S_X$ associée à l'action de G sur X. Son noyau est $\{x \in X; gx = x \text{ pour tout } g \in G\} = G_X$. Nous en déduisons, d'après le 1^{er} théorème d'isomorphisme, que $\frac{G}{G_X}$ est isomorphe à un sous-groupe de S_X .

11. On a

$$\text{Ker } \varphi = \bigcap_{i=1}^k \text{Ker } \pi_i = \bigcap_{i=1}^k G_i = \left\{ g \in G; gx = x \text{ pour tout } x \in \bigcup_{i=1}^k X_i = E \right\}.$$

Comme G opère fidèlement sur E, nous en déduisons que l'homomorphisme φ est injectif. Le 1^{er} théorème d'isomorphisme permet alors de conclure que G est isomorphe à un sous-groupe de $S_{n_1} \times S_{n_2} \times \dots \times S_{n_k}$.

12. Le groupe G opère par translation à gauche sur l'ensemble quotient $Q_H = \left(\frac{G}{H}\right)_g$. Considérons le morphisme de groupes $\gamma: G \rightarrow S_{Q_H}$ associé à cette action et notons K son noyau. Il est normal dans G et est inclus dans H (proposition 5.15). Le groupe $\frac{G}{K}$ est isomorphe à un sous-groupe de S_{Q_H} (1^{er} théorème d'isomorphisme), donc $[G:K]$ divise $|S_{Q_H}| = [G:H]! = n!$.

13. Faisons une démonstration par l'absurde. Supposons que $Z(G) = (e)$. Soient $\{x_1, \dots, x_{k-1}\}$ une famille de représentants des classes de conjugaison distinctes et non ponctuelles de G . D'après l'équation aux classes, nous avons

$$o(G) = 1 + \sum_{i=1}^{k-1} |\Omega_{x_i}|.$$

Comme $|\Omega_{x_i}|$ divise $o(G)$ pour tout $i \in \{1, \dots, k-1\}$, on a $|\Omega_{x_i}| \geq p$. Par conséquent, $o(G) \geq 1 + (k-1)p$, puis

$$\frac{o(G)}{p} \geq \frac{1}{p} + k - 1 > k - 1,$$

d'où la contradiction

$$\frac{o(G)}{p} \geq k.$$

Nous avons donc bien $Z(G) \neq (e)$.

14. a) Les cycles $\gamma_1, \gamma_2, \dots, \gamma_t$ étant disjoints, ils commutent deux à deux (proposition 3.39); on peut donc supposer que $1 \leq n_1 \leq n_2 \leq \dots \leq n_t$. L'unicité de la décomposition à l'ordre des facteurs près permet de conclure que toute permutation de S_n détermine une partition de l'entier n .

b) *Deux cycles sont conjugués dans S_n si et seulement si ils ont même longueur.* Soient $\gamma = (j_1, j_2, \dots, j_t)$ et $\gamma' = (j'_1, j'_2, \dots, j'_t)$ deux cycles dans S_n .

Supposons que γ et γ' sont conjugués. Alors il existe $\sigma \in S_n$ telle que

$$\gamma' = \sigma \circ \gamma \circ \sigma^{-1}.$$

On a montré à l'exercice 3.24 que γ' est le t -cycle

$$(\sigma(j_1), \sigma(j_2), \dots, \sigma(j_t)),$$

donc $\text{long } \gamma = \text{long } \gamma'$.

Réciproquement, supposons que $\text{long } \gamma = \text{long } \gamma'$. Il existe une permutation $\sigma \in S_n$ telle que $\sigma(j_k) = j'_k$ pour tout $k \in \{1, 2, \dots, t\}$. Elle vérifie

$$\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(j_1), \sigma(j_2), \dots, \sigma(j_t)) = (j'_1, j'_2, \dots, j'_t) = \gamma',$$

donc les cycles γ et γ' sont conjugués.

Deux permutations sont conjuguées dans S_n si et seulement si elles déterminent la même partition de n . Soient σ et σ' deux permutations dans S_n . D'après la première question, il existe deux familles de cycles disjoints $(\gamma_i)_{1 \leq i \leq t}$ et $(\gamma'_i)_{1 \leq i \leq t'}$ telles que

$$\begin{aligned} \sigma &= \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_t, & 1 \leq n_1 \leq n_2 \leq \dots \leq n_t & \quad \text{et} \quad \sum_{i=1}^t n_i = n \\ \sigma' &= \gamma'_1 \circ \gamma'_2 \circ \dots \circ \gamma'_{t'}, & 1 \leq n'_1 \leq n'_2 \leq \dots \leq n'_{t'} & \quad \text{et} \quad \sum_{i=1}^{t'} n'_i = n. \end{aligned}$$

Supposons que σ et σ' déterminent la même partition de n . D'après la première partie de la question, il existe une famille de permutations $(\pi_i)_{1 \leq i \leq t}$ dans S_n telle que

$$\gamma'_i = \pi_i \circ \gamma_i \circ \pi_i^{-1}.$$

Les cycles $\gamma_1, \gamma_2, \dots, \gamma_t$ étant disjoints, nous pouvons définir une permutation π dans S_n en posant

$$\pi|_{\text{supp}(\gamma_i)} = \pi_i.$$

On a alors

$$\gamma'_i = \pi \circ \gamma_i \circ \pi^{-1}$$

pout tout $i \in \mathbf{N}_t$. Il s'ensuit que

$$\begin{aligned}\pi \circ \sigma \circ \pi^{-1} &= \pi \circ (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_t) \circ \pi^{-1} \\ &= (\pi \circ \gamma_1 \circ \pi^{-1}) \circ (\pi \circ \gamma_2 \circ \pi^{-1}) \circ \cdots \circ (\pi \circ \gamma_t \circ \pi^{-1}) \\ &= \gamma'_1 \circ \gamma'_2 \circ \cdots \circ \gamma'_t \\ &= \sigma',\end{aligned}$$

donc les permutations σ et σ' sont bien conjuguées dans S_n .

Réciproquement, supposons que σ et σ' sont conjuguées dans S_n . Alors il existe $\pi \in S_n$ telle que

$$\sigma' = \pi \circ \sigma \circ \pi^{-1}.$$

On a alors

$$\gamma'_1 \circ \gamma'_2 \circ \cdots \circ \gamma'_t = (\pi \circ \gamma_1 \circ \pi^{-1}) \circ (\pi \circ \gamma_2 \circ \pi^{-1}) \circ \cdots \circ (\pi \circ \gamma_t \circ \pi^{-1})$$

avec, pour tout $i \in \mathbf{N}_t$,

$$\text{long}(\pi \circ \gamma_i \circ \pi^{-1}) = \text{long} \gamma_i.$$

L'unicité de la décomposition en cycles disjoints (théorème 3.55) entraîne $t = t'$ et

$$(n_1, n_2, \dots, n_t) = (n'_1, n'_2, \dots, n'_t).$$

Des permutations conjuguées déterminent donc bien la même partition de n .

Le nombre de classes de conjugaison de S_n est égal à $p(n)$.

La question a) définit une application de S_n vers l'ensemble des partitions de n . Comme deux permutations conjuguées déterminent la même partition, elle induit une application φ de l'ensemble des classes de conjugaison de S_n vers les partitions de n . Puisque deux permutations qui déterminent la même partition sont conjuguées, l'application φ est injective. Reste à démontrer la surjectivité de φ . Pour cela considérons une partition (n_1, n_2, \dots, n_t) de n . Pour tout

$i \in \mathbf{N}_t$, notons γ_i le n_i -cycles $(s_{i-1}, s_{i-1} + 1, \dots, s_i - 1)$ où $s_0 = 1$ et $s_i = \sum_{j=1}^i n_j$ pour tout \mathbf{N}_t . La classe conjugaison de $\gamma_1 \gamma_2 \dots \gamma_t$ a alors pour image (n_1, n_2, \dots, n_t) .

17. a) Il est clair que pour tout $(a, a') \in X^2$ tel que $a \neq a'$, on a $S(a, \cdot) \cap S(a', \cdot) = \emptyset$. Par construction, $S(a, \cdot) \subseteq S$ pour tout $a \in X$, d'où l'inclusion $\cup_{a \in X} S(a, \cdot) \subseteq S$. Comme $(a, b) \in S(a, \cdot)$ pour tout $(a, b) \in S$, nous avons l'inclusion réciproque, d'où l'égalité $S = \cup_{a \in X} S(a, \cdot)$. Il s'ensuit que la famille $\{S(a, \cdot); a \in X\}$ est une partition de S . Il en est de même de la famille $\{S(\cdot, b); b \in Y\}$. Nous en déduisons que

$$|S| = \sum_{a \in X} |S(a, \cdot)| = \sum_{b \in Y} |S(\cdot, b)|.$$

b) — Soit $(g, x) \in G \times E$. On a

$$\begin{aligned} S(g, \cdot) &= \{(g, x) \in S\} \\ &= \{(g, x) \in G \times E; gx = x\} \\ &= \{(g, x) \in G \times E; x \in F(g)\} \\ &= \{g\} \times F(g) \end{aligned}$$

et

$$\begin{aligned} S(\cdot, x) &= \{(g, x) \in S\} \\ &= \{(g, x) \in G \times E; gx = x\} \\ &= \{(g, x) \in G \times E; g \in G_x\} \\ &= G_x \times \{x\}. \end{aligned}$$

Par conséquent,

$$\sum_{g \in G} |S(g, \cdot)| = \sum_{g \in G} |\{g\} \times F(g)| = \sum_{g \in G} |F(g)|$$

et

$$\sum_{x \in E} |S(\cdot, x)| = \sum_{x \in E} |G_x \times \{x\}| = \sum_{x \in E} |G_x|.$$

D'après l'égalité établie à la question précédente, nous avons donc

$$\sum_{g \in G} |\mathbb{F}(g)| = \sum_{x \in E} |G_x|.$$

Comme les G -orbites de E forment une partition de E , on a

$$\sum_{x \in E} |G_x| = \sum_{i=1}^t \sum_{x \in \Omega_{x_i}} |G_x|,$$

si bien que

$$\sum_{g \in G} |\mathbb{F}(g)| = \sum_{i=1}^t \sum_{x \in \Omega_{x_i}} |G_x|.$$

- Pour tout $x \in \Omega_{x_i}$, les sous-groupes G_x et G_{x_i} sont conjugués (théorème 5.18), d'où $|G_x| = |G_{x_i}|$. La formule précédente peut donc s'écrire

$$\sum_{g \in G} |\mathbb{F}(g)| = \sum_{i=1}^t |\Omega_{x_i}| |G_{x_i}|.$$

Or $|\Omega_{x_i}| = [G : G_{x_i}]$ (théorème 5.19) et $|G| = |G_{x_i}| [G : G_{x_i}]$ (proposition 2.15), d'où la formule de Burnside :

$$\sum_{g \in G} |\mathbb{F}(g)| = t|G|.$$

- c) Si G opère transitivement sur E , alors il n'y a qu'une seule G -orbite ($t = 1$). La formule de Burnside devient alors

$$\sum_{g \in G} |\mathbb{F}(g)| = |G|.$$

19. a) Évident.

- b) Supposons que G est k -transitif sur E . Soient $x \in E$ et deux $(k-1)$ -uplets $(x_1, x_2, \dots, x_{k-1})$, $(y_1, y_2, \dots, y_{k-1})$ d'éléments distincts de $E \setminus \{x\}$. Alors (x, x_1, \dots, x_{k-1}) et (x, y_1, \dots, y_{k-1}) sont deux k -uplets d'éléments distincts de E , donc il existe $g \in G$ tel $g \cdot x = x$ et $g \cdot x_i = y_i$

pour tout $i \in \mathbf{N}_{k-1}$, ce qui nous permet de conclure que G_x est $(k-1)$ -transitif sur $E \setminus \{x\}$.

Réciproquement, supposons que pour tout $x \in E$, le groupe G_x est $(k-1)$ -transitif sur $E \setminus \{x\}$. Soient (x_1, x_2, \dots, x_k) et (y_1, y_2, \dots, y_k) deux k -uplets d'éléments distincts de E . Il existe $(g, h) \in G_{x_k} \times G_{y_{k-1}}$ tel que $g \cdot x_i = y_i$ pour tout $i \in \mathbf{N}_{k-1}$, $h \cdot y_i = y_i$ pour tout $i \in \mathbf{N}_{k-2}$ et $h \cdot x_k = y_k$. On vérifie que

$$hg \cdot x_i = h \cdot g \cdot x_i = \begin{cases} h \cdot y_i = y_i & \text{si } i \in \mathbf{N}_{k-1} \\ h \cdot x_k = y_k & \text{si } i = k. \end{cases}$$

Le groupe G est bien k -transitif sur E .

- c) — D'après la question a), G est transitif sur E , donc la formule de Burnside (exercice 5.17) s'écrit

$$|G| = \sum_{g \in G} |F(g)|.$$

Soit $x \in E$. Le groupe G_x opère transitivement sur $E \setminus \{x\}$; les G_x -orbites de E sont donc $E \setminus \{x\}$ et $\{x\}$. La formule établie à l'exercice 18 donne

$$2|G| = \sum_{g \in G} |F(g)|^2.$$

- Notons $E^{(k)}$ l'ensemble de k -uplets d'éléments deux à deux distincts de E . L'action de G sur E induit une action de G sur $E^{(k)}$ définie par

$$g \cdot (x_1, x_2, \dots, x_k) = (g \cdot x_1, g \cdot x_2, \dots, g \cdot x_k)$$

pour tout $g \in G$ et $(x_1, x_2, \dots, x_k) \in E^{(k)}$. L'action de G sur E étant k -transitive, celle de G sur $E^{(k)}$ est transitive. Par conséquent, nous déduisons du théorème 5.19 que

$$|G| = |G_x| |E^{(k)}|$$

où $x \in E^{(k)}$. Or $|E^{(k)}| = n(n-1) \dots (n-k+1)$, ce qui prouve que $|G|$ est divisible par $n(n-1) \dots (n-k+1)$.

22. Soit f un isomorphisme de N_1 sur N_2 . Nous savons que

$$\begin{aligned} f_{\#} : \text{Aut}(N_1) &\rightarrow \text{Aut}(N_2) \\ g &\mapsto f \circ g \circ f^{-1} \end{aligned}$$

est un isomorphisme de groupes (exercice 32, chapitre I). Considérons l'application

$$\begin{aligned} \varphi : \text{Hol}(N_1) &\rightarrow \text{Hol}(N_2) \\ (x, \alpha) &\rightarrow (f(x), f_{\#}(\alpha)). \end{aligned}$$

L'application φ est un morphisme de groupes ; en effet, quels que soient (x, α) et (y, β) dans $\text{Hol}(N_1)$, on a

$$\begin{aligned} \varphi(x, \alpha)\varphi(y, \beta) &= (f(x), f_{\#}(\alpha))(f(y), f_{\#}(\beta)) \\ &= (f(x)f_{\#}(\alpha)(f(y)), f_{\#}(\alpha) \circ f_{\#}(\beta)) \\ &= (f(x)f(\alpha(y)), f_{\#}(\alpha \circ \beta)) \\ &= (f(x\alpha(y)), f_{\#}(\alpha \circ \beta)) \\ &= \varphi(x\alpha(y), \alpha \circ \beta) \\ &= \varphi((x, \alpha)(y, \beta)). \end{aligned}$$

L'application φ est bijective, car, $\text{Ker } \varphi = \text{Ker } f \times \text{Ker } f_{\#} = (e, \text{id}_{N_1})$ et $\text{Im } \varphi = \text{Im } f \times \text{Im } f_{\#} = N_2 \times \text{Aut}(N_2)$.

En conclusion, les groupes $\text{Hol}(N_1)$ et $\text{Hol}(N_2)$ sont isomorphes.

27. 1° a) Soit $x \in E$. Étant donné que θ est un isomorphisme, il nous suffit de démontrer que $\theta(G_x) = G'_{\lambda(x)}$. Quel que soit $g \in G_x$, on a $\theta(g) \cdot \lambda(x) = \lambda(g \cdot x) = \lambda(x)$, donc $\theta(G_x) \subseteq G'_{\lambda(x)}$. Réciproquement, si $g' \in G'_{\lambda(x)}$, il existe $g \in G$ tel que $\theta(g) = g'$. On a alors $\lambda(g \cdot x) = \theta(g) \cdot \lambda(x) = g' \cdot \lambda(x) = \lambda(x)$, si bien que $g \cdot x = x$, donc $G'_{\lambda(x)} \subseteq \theta(G_x)$.

b) G transitif sur $E \iff G'$ transitif sur E' . Soit $x \in E$. L'orbite de x

étant notée Ω_x et celle de $\lambda(x)$ étant notée $\Omega'_{\lambda(x)}$, on a

$$\begin{aligned}\Omega'_{\lambda(x)} &= \{g' \cdot \lambda(x); g' \in G'\} \\ &= \{\theta(g) \cdot \lambda(x); g \in G\} \\ &= \{\lambda(g \cdot x); g \in G\} \\ &= \lambda(\Omega_x).\end{aligned}$$

Nous en déduisons immédiatement que G est transitif sur E si et seulement si G' est transitif sur E' .

G transitif sur $E \implies \forall (x, y) \in E \times E', G_x \simeq G'_y$. Soit $(x, y) \in E \times E'$. D'après la question précédente, les sous-groupes G_x et $G'_{\lambda(x)}$ sont isomorphes. Nous venons de démontrer que G' est transitif sur E' , donc il existe $g' \in G'$ tel que $y = g' \cdot \lambda(x)$. Il s'ensuit que G'_y et $G'_{\lambda(x)}$ sont isomorphes (théorème 5.18). Finalement, les sous-groupes G'_y et G_x sont isomorphes.

- c) Soient les sous-groupes $H = \bigcap_{x \in E} G_x$ et $H' = \bigcap_{x \in E'} G_{x'}$. Remarquons que le groupe G opère fidèlement sur E si et seulement si $H = (e)$. Comme θ est injective, on a

$$\theta(H) = \bigcap_{x \in E} \theta(G_x),$$

puis d'après la question 1° a),

$$\theta(H) = \bigcap_{x \in E} G'_{\lambda(x)},$$

et enfin, λ étant surjective,

$$\theta(H) = \bigcap_{x' \in E'} G_{x'};$$

autrement dit,

$$\theta(H) = H'.$$

Étant donné que θ est un monomorphisme, nous en déduisons immédiatement que G opère fidèlement sur E si et seulement si G' opère fidèlement sur E' .

2° Pour tout $(g, h) \in G^2$, on a

$$\begin{aligned}\varphi(gh) &= \lambda \circ \gamma_{gh} \circ \lambda^{-1} \\ &= \lambda \circ \gamma_g \circ \gamma_h \circ \lambda^{-1} \\ &= \lambda \circ \gamma_g \circ \lambda^{-1} \circ \lambda \circ \gamma_h \circ \lambda^{-1} \\ &= \varphi(g) \circ \varphi(h).\end{aligned}$$

De plus,

$$\begin{aligned}\text{Ker } \varphi &= \{g \in G; \lambda \circ \gamma_g \circ \lambda^{-1} = \text{id}_{E'}\} \\ &= \{g \in G; \lambda_g = \lambda^{-1} \circ \text{id}_{E'} \circ \lambda\} \\ &= \{g \in G; \lambda_g = \text{id}_E\}\end{aligned}$$

et puisque G agit fidèlement sur E ,

$$\text{Ker } \varphi = \{e\}.$$

Nous avons prouvé que φ est un monomorphisme de groupes.

Il s'ensuit que la corestriction de φ à G' , que nous noterons $\hat{\varphi}$, est un isomorphisme de groupes. Soit γ' le morphisme de groupes de G' dans $S_{E'}$ associé à l'action naturelle de G' sur E' . Il est définie par $\gamma'_g(x) = g(x)$ pour tout $(g, x) \in G' \times E'$. Pour tout $(g, x) \in G \times E$, on a

$$\begin{aligned}\hat{\varphi}(g) \cdot \lambda(x) &= \hat{\varphi}(g)(\lambda(x)) \\ &= (\lambda \circ \gamma_g \circ \lambda^{-1})(\lambda(x)) \\ &= \lambda(\gamma_g(x)) \\ &= \lambda(g \cdot x),\end{aligned}$$

ce qui nous permet de conclure que l'action de G sur E est équivalente à l'action naturelle de G' sur E' .

Groupes finis. Théorèmes de Sylow

1. Soit H un sous-groupe de Sylow de D_n .

Si H est d'ordre impair, alors $H \subseteq \langle \rho \rangle$ où ρ est la rotation d'angle $2\pi/n$, car tous les éléments de $D_n \setminus \langle \rho \rangle$ sont d'ordre 2 (proposition 3.72). Par conséquent, H est un sous-groupe de $\langle \rho \rangle$, donc il est cyclique (théorème 3.10).

Si H est d'ordre pair, alors H est un 2-sous-groupe de Sylow. Comme $o(D_n) = 2n$ avec n non divisible par 2, le sous-groupe H est d'ordre 2, donc il est cyclique.

3. $35 = 5 \times 7$ avec 5 et 7 premiers, $7 \not\equiv 1 \pmod{5}$ et $5 \not\equiv 1 \pmod{7}$, donc selon la proposition 6.16, tout groupe d'ordre 35 est cyclique.

4. Soit G un groupe d'ordre $42 = 6 \times 7$. Notons n_7 le nombre de 7-sous-groupe de Sylow. D'après le second théorème de Sylow, $n_7 \mid 6$ et $n_7 \equiv 1 \pmod{7}$ d'où $n_7 = 1$. Le groupe G possède un unique 7-sous-groupe de Sylow. D'après le corollaire 6.9, il est normal dans G , il s'ensuit que le groupe G n'est pas simple.

5. a) D'après le second théorème de Sylow, le nombre de 7-sous-groupes de Sylow est un diviseur de 56 congru à 1 modulo 7, donc n_7 est égal à 1 ou 8.

b) Supposons que $n_7 = 8$. Tout élément d'ordre 7 engendre un 7-sous-groupe, donc appartient à un 7-sous-groupe de Sylow d'après le second théorème de Sylow. Comme $o(G) = 2^3 \times 7$, les 7-sous-groupes de Sylow sont d'ordre 7. Étant donné que 7 est un nombre premier, l'intersection de deux de ces sous-groupes distincts est trivial (théorème de Lagrange) et chacun de ces sous-groupe de Sylow a

exactement 6 éléments d'ordre 7 (corollaire 2.10 du théorème de Lagrange). Il s'ensuit que le groupe G comporte $6 \times 8 = 48$ éléments d'ordre 7.

Toujours d'après le second théorème de Sylow, n_2 est un diviseur impair de 56, donc n_2 est égal à 1 ou 7. Chacun des 2-sous-groupes de Sylow est d'ordre 8. Or, nous avons déjà 48 éléments d'ordre 7, si bien qu'il ne reste que 8 éléments pour former ces 2-sous-groupes de Sylow, donc $n_2 = 1$.

c) D'après les questions précédentes, nous avons $n_7 = 1$ ou $n_2 = 1$. Le corollaire 6.9 permet de conclure que dans les deux cas le groupe n'est pas simple.

6. Soit G un groupe d'ordre 300. Puisque $300 = 2^2 \times 3 \times 5^2$, il admet au moins un 5-sous-groupe de Sylow S . Notons n_5 le nombre de 5-sous-groupe de Sylow. D'après le second théorème de Sylow, n_5 est congru à 1 modulo 5 et n_5 divise 6, donc $n_5 \in \{1, 6\}$. Si $n_5 = 1$, alors $S \triangleleft G$, donc G n'est pas simple. Si $n_5 = 6$, alors $[G : N_G(S)] = 6$ (corollaire 5.20). Or 300 ne divise pas $6!$, donc G n'est pas simple (proposition 5.17). Nous avons démontré qu'il n'existe pas de groupe simple d'ordre 300.

12. Pour tout $g \in G$, on a $gHg^{-1} \subseteq gKg^{-1} = K$ et $|gHg^{-1}| = |H|$, donc gHg^{-1} est un p -sous-groupe de Sylow de K . D'après le second théorème de Sylow, les p -sous-groupes de Sylow gHg^{-1} et H sont conjugués dans K , c'est-à-dire qu'il existe $x \in K$ tel que $gHg^{-1} = xHx^{-1}$. Comme $H \triangleleft K$, il vient $gHg^{-1} = H$. Ainsi nous avons prouvé que $H \triangleleft G$.

13. S' est un p -sous-groupe de G . D'après le second théorème de Sylow, il existe un p -sous-groupe de Sylow S de G tel que $S' \subset S$ d'où $S' = S' \cap H \subset S \cap H$. De $|S \cap H| \mid |S|$, on déduit que $S \cap H$ est un p -sous-groupe de H . Comme S' est un p -sous-groupe de Sylow de H , nécessairement $S' = S \cap H$, ce que l'on voulait démontrer.

Suites de composition

1. a) Soit K un sous-groupe normal minimal de G . On sait que $Z(K) \sqsubset K$ (proposition 4.43) donc $Z(K) \triangleleft G$ (proposition 4.44). La minimalité de K implique $Z(K) = (e)$ ou $Z(K) = K$.
- b) Commençons par montrer que KL est un sous-groupe de G . De $K \triangleleft G$, on déduit $LKL^{-1} \subseteq K$, puis $LK \subseteq KL$. De même, $L \triangleleft G$ implique $KL \subseteq LK$, si bien que $LK = KL$. La proposition 1.47 permet de conclure.

Montrons que l'application

$$\varphi: K \times L \rightarrow KL, (k, l) \mapsto kl$$

est un isomorphisme de groupes.

Vérifions que $kl = lk$ pour tout $(k, l) \in K \times L$. Nous savons que

$$K \triangleleft G \text{ et } L \triangleleft G \implies K \cap L \triangleleft G \text{ et } K \cap L \leq K.$$

La minimalité de K implique que $K \cap L = (e)$ ou $K \cap L = K$. Supposons que $K \cap L = K$. On a alors $K \subseteq L$. La minimalité de L et $K \neq L$ impliquent que $K = (e)$, puis $K \cap L = (e)$. On en déduit que si $k \in K$ et $l \in L$ alors

$$klk^{-1}l^{-1} = k(lk^{-1}l^{-1}) \in K \quad \text{et} \quad klk^{-1}l^{-1} = (klk^{-1})l^{-1} \in L,$$

c'est-à-dire $klk^{-1}l^{-1} \in L \cap K = (e)$, donc $kl = lk$.

L'application φ est un homomorphisme de groupes. En effet, pour tout $(k, l) \in K \times L$ et $(k', l') \in K \times L$, on a

$$\varphi(k, l)\varphi(k', l') = klk'l' = kk'l'l' = \varphi(kk', l'l') = \varphi((k, l)(k', l')).$$

Par construction, φ est clairement surjectif. Enfin, soit $(k, l) \in K \times L$ tel que $\varphi(k, l) = e$, c'est-à-dire $kl = e$. Alors $k = l^{-1} \in K \cap L$ et $l = k^{-1} \in K \cap L$, si bien que $(k, l) = (e, e)$; l'homomorphisme φ est injectif.

En résumé, le sous-groupe KL est isomorphe au groupe $K \times L$.

- c) Soit H un sous-groupe normal de \mathbf{Z} différent de (0) . Il existe $n \in \mathbf{N}^*$ tel que $H = n\mathbf{Z}$. Soit $H' = 2n\mathbf{Z}$. Alors $H' \triangleleft \mathbf{Z}$ et $H' < H$ avec $H' \neq (0)$. Donc H n'est pas minimal. On conclut que $(\mathbf{Z}, +)$ n'a pas de sous-groupe normal minimal.

CHAPITRE VIII

Groupes abéliens

CHAPITRE IX

*Groupes libres. Générateurs et relations.
Produit libre de groupes*

Bibliographie

[Cal14] Josette Calais. *Éléments de théorie des groupes*. PUF, 2014.