Éléments de théorie des groupes
Solutions des exercices

Éric Guirbal

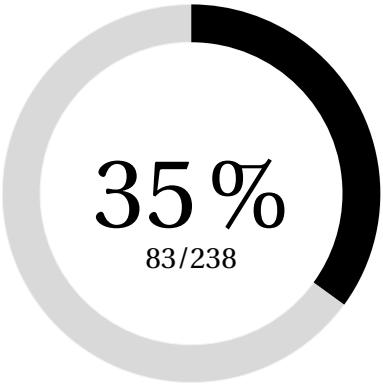
Éléments de théorie des groupes
Solutions des exercices

Éric GUIRBAL

Version : d2a863f
Compilé le 31 juillet 2019

Sommaire

État d'avancement du projet



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

— Soit $a, b \in \mathrm{A}$. 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 $\mathrm{A}\times\mathrm{A}$ définie bien une loi interne.

— On sait déjà que 0 est l'élément neutre de la loi $*$.

— Soit $a, b, c \in \mathrm{A}$, 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 $a \in \mathrm{A}$, 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 $x \in \mathrm{G}$, 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 $(\mathrm{G}, \cdot)$ 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 $(a, b) \in \mathrm{G}^2$, chacune des équations $ax = b$ et $xa = b$ d'inconnue x possède une unique solution.

Montrons l'existence d'un élément neutre. Soit $a \in \mathrm{G}$. Il existe $g \in \mathrm{G}$ tel que $ga = a$. Vérifions que g est un neutre à gauche. Soit $x \in \mathrm{G}$. 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 $f \circ f = \mathrm{id}_G$, 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 $\mathscr{R}$ ainsi :

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

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

puis $k = 2(n-l)$, c'est-à-dire que le nombre d'éléments $x \in \mathrm{G}$ tel que $x^2 = e$ est nécessairement pair. Comme e est l'un d'eux, il existe au moins un $x \in \mathrm{G}$ 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 $\varphi : \mathbf{U} \to \frac{\mathbf{Z}}{(2)}$ définie par $\varphi(1) = \overline{0}$ et $\varphi(-1) = \overline{1}$ est un homomorphisme de groupes ; en effet,

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

et

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

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

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

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 irrationel. [1] En particulier, la racine carrée d'un nombre premier est irrationel.

— $\mathrm{G}_1 = \left\{ a + b\sqrt{p}\,; (a,b) \in \mathbf{Z}\times\mathbf{Z} \right\}$ *est un sous-groupe de* $(\mathbf{R}, +)$.
On a $\mathrm{G}_1 \subset \mathbf{R}$. Soient $a + b\sqrt{p} \in \mathrm{G}_1$, $a' + b'\sqrt{p} \in \mathrm{G}_1$. On a

$$(a + b\sqrt{p}) - (a' + b'\sqrt{p}) = (a - a') + (b - b')\sqrt{p} \in \mathrm{G}_1$$

— $\mathrm{G}_2 = \left\{ a + b\sqrt{p}\,; (a,b) \in (\mathbf{Q}^2)^* \right\}$ *est un sous-groupe de* $(\mathbf{R}^*, \times)$.
Puisque $\sqrt{p}$ est irrationel, $\mathrm{G}_2 \subset \mathbf{R}^*$. Soient $a + b\sqrt{p} \in \mathrm{G}_2$ et $a' + b'\sqrt{p} \in \mathrm{G}_2$. En multipliant le dénominateur et le numérateur par le conjugué $a' - b'\sqrt{p}$ de $a' + b'\sqrt{p}$, nous obtenons

$$(a + b\sqrt{p}) \times (a' + b'\sqrt{p})^{-1} = \frac{aa' - pbb'}{a'^2 - pb'^2} + \frac{a'b - ab'}{a'^2 - pb'^2}\sqrt{p} \in \mathrm{G}_2.$$

— $\mathrm{G}_3 = \left\{ a + \mathrm{i}b\sqrt{p}\,; \mathbf{Z}\times\mathbf{Z} \right\}$ *est un sous-groupe de* $(\mathbf{C}, +)$.
Clairement $\mathrm{G}_3 \subset \mathbf{C}$. Soient $a + \mathrm{i}b\sqrt{p} \in \mathrm{G}_3$ et $a' + \mathrm{i}b'\sqrt{p} \in \mathrm{G}_3$. On a

$$(a + \mathrm{i}b\sqrt{p}) - (a' + \mathrm{i}b\sqrt{p}) = (a - a') + \mathrm{i}(b - b')\sqrt{p} \in \mathrm{G}_3.$$

— $\mathrm{G}_4 = \left\{ a + \mathrm{i}b\sqrt{p}\,; (a,b) \in (\mathbf{Q}^2)^* \right\}$ *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 $\mathrm{S} = \{ k \in \mathbf{N}^* \,; k\sqrt{d} \in \mathbf{N} \}$ est une partie non vide de $\mathbf{N}^*$. Notons m sont 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 $l \in \mathrm{S}$. Or $l < m$, ce qui contredit la définition de m, donc $\sqrt{d}$ est irrationel.

Puisque $\sqrt{p}$ est irrationel, $G_4 \subset \mathbf{C}^*$. 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. 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 $w \neq 0$ et $(zw^{-1})^{nm} = (z^n)^m (w^m)^{-n} = 1$ donc $zw^{-1} \in \Gamma_\infty$: Γ_∞ est un sous-groupe de $(\mathbf{C}^*, \times)$.

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 homorphisme de groupes. De plus

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

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

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

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

donc g est homorphisme de groupes. De plus

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

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

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 sujective, 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 $Z(G) \cap H \leqslant Z(H)$.

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 $f(Z(G)) \leqslant Z(G')$.

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

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

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

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

Montrons que $\mathscr{H}_{A \cup B \cup C} = \mathscr{H}_{H \cup C}$. Soit $L \in \mathscr{H}_{A \cup B \cup C}$. Comme $A \cup B \subseteq L$, nécessairement $H \subseteq L$ donc $L \in \mathscr{H}_{H \cup C}$. Réciproquement, soit $L \in \mathscr{H}_{H \cup C}$. On a $A \cup B \subseteq H \subseteq L$, donc $L \in \mathscr{H}_{A \cup B \cup C}$. Nous avons montré que $\mathscr{H}_{A \cup B \cup C} = \mathscr{H}_{H \cup C}$, 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

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

muni de la multiplication des matrices.

Montrons que $\mathrm{Q}_8 = \langle \mathrm{A}, \mathrm{B} \rangle$. Comme $\mathrm{A} \in \mathrm{Q}_8$ et $\mathrm{B} \in \mathrm{Q}_8$, on a $\langle \mathrm{A}, \mathrm{B} \rangle \subseteq \mathrm{Q}_8$. De plus, on vérifie que $q_1 = \mathrm{A}^4$, $q_2 = \mathrm{A}^2$, $q_3 = \mathrm{A}$, $q_4 = \mathrm{A}^3$, $q_5 = \mathrm{B}$, $q_6 = \mathrm{B}^3$, $q_7 = \mathrm{BA}$ et $q_8 = \mathrm{AB}$, donc $\mathrm{Q}_8 \subseteq \langle \mathrm{A}, \mathrm{B} \rangle$.

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

$$\mathrm{M}_x \mathrm{M}_y = \mathrm{M}_{xy} = \mathrm{M}_{yx} = \mathrm{M}_y \mathrm{M}_x$$

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 $\mathrm{M}_{x^{-1}}$, en effet $\mathrm{M}_x \mathrm{M}_{x^{-1}} = \mathrm{M}_{xx^{-1}} = \mathrm{M}_1$. 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 $\mathrm{GL}(2, \mathbf{R})$; en effet, les matrices M_x ont un déterminant nul et donc ne sont pas inversibles dans $\mathrm{GL}(2, \mathbf{R})$.

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

$$\varphi(\mathrm{M}_x \mathrm{M}_y) = \varphi(\mathrm{M}_{xy}) = xy = \varphi(\mathrm{M}_x)\varphi(\mathrm{M}_y).$$

Le morphisme φ est injectif, car $\varphi(\mathrm{M}_x) = 1$ implique $x = 1$ c'est-à-dire $\mathrm{M}_x = \mathrm{M}_1$. Enfin, le morphisme φ est surjectif, car pour tout $x \in \mathbf{R}^*$, on a $\varphi(\mathrm{M}_x) = x$. 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 $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $\overline{xy} = \overline{x'y'}$.
$\frac{\mathbf{Z}}{(n)}$ *est un anneau unitaire commutatif.*
La multiplication dans $\frac{\mathbf{Z}}{(n)}$ est associative : quels que soient $\overline{x}$, $\overline{y}$, $\overline{z}$ dans $\frac{\mathbf{Z}}{(n)}$, on a

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

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

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

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

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

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

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

b) L'ensemble G_p est fini et nous avons déjà démontré que la multiplication est associative. Soient $\overline{a}$, $\overline{x}$ et $\overline{y}$ trois éléments de G_p tels que $\overline{a}\,\overline{x} = \overline{a}\,\overline{y}$. Alors $\overline{ax} = \overline{ay}$, donc p divise $a(x-y)$. Or p ne divise pas a puisque $\overline{a} \neq \overline{0}$, donc p divise $x - y$ ce qui signifie que $\overline{x} = \overline{y}$. 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 $\overline{k}\,\overline{l}=\overline{n}=\overline{0}$ avec $\overline{k}\neq\overline{0}$ et $\overline{l}\neq\overline{0}$, donc $\overline{k}$ n'est pas inversible : $\frac{\mathbf{Z}}{(n)}$ n'est pas un corps.

22. *L'ensemble* Γ *est un sous-groupe de* $\mathrm{GL}(2,\mathbf{R})$. 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

$$\Gamma=\{\mathrm{I},\mathrm{A},\mathrm{I}_x,\mathrm{A}_x,\mathrm{A}_y,\mathrm{A}_{xy}\}.$$

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

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

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

nous pouvons donc définir l'application

$$\begin{aligned}\varphi\colon\Gamma&\to\mathrm{GL}\left(2,\frac{\mathbf{Z}}{(2)}\right)\\ \mathrm{M}&\mapsto\overline{\mathrm{M}}.\end{aligned}$$

L'application φ est un homomorphisme de groupes : soient

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

alors

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

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

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

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

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

×	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 $g\colon \Gamma \to S_3$ la bijection définie par

$$g(\mathrm{I}) = e, \qquad g(\mathrm{A}) = \sigma_1, \qquad g(\mathrm{A}_{xy}) = \sigma_2,$$
$$g(\mathrm{A}_x) = \tau_1, \qquad g(\mathrm{I}_x) = \tau_2, \qquad g(\mathrm{A}_y) = \tau_3.$$

Si nous identifions chaque élement 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 $\Gamma_1 \subseteq \mathrm{GL}(2,\mathbf{R})$, $\Gamma_2 \subset \mathbf{C}^*$ 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 $\mathrm{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathrm{A} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\mathrm{B} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $\mathrm{C} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ de sorte que $\Gamma_1 = \{\mathrm{I}, \mathrm{A}, \mathrm{B}, \mathrm{C}\}$. Sa table de Cayley est :

×	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 :

×	1	i	−1	−i
1	1	i	−1	−i
i	i	−1	−i	1
−1	−1	−i	1	i
−i	−i	1	i	−1

×	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Nous en déduisons que Γ_1 est un sous-groupe de $\mathrm{GL}(2,\mathbf{R})$, 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 $f\colon \Gamma_1 \to \Gamma_2$ définie par $f(\mathrm{I}) = 1$, $f(\mathrm{A}) = \mathrm{i}$, $f(\mathrm{B}) = -1$ et $f(\mathrm{C}) = -\mathrm{i}$, 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 $g\colon \Gamma_1 \to \Gamma_3$ définie par $g(\mathrm{I}) = \overline{1}$, $g(\mathrm{A}) = \overline{(2)}$, $g(\mathrm{B}) = \overline{4}$ et $g(\mathrm{C}) = \overline{3}$.

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

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

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

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

$$\mathrm{M}_{a,b} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

et notons I_2 la matrice unité $\mathrm{M}_{1,1}$. Ainsi

$$\mathrm{K}_1 = \{\mathrm{I}_2, \mathrm{M}_{1,-1}, \mathrm{M}_{-1,1}, \mathrm{M}_{-1,-1}\}.$$

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

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

donc

$$\mathrm{M}_{a,b}\mathrm{M}_{a',b'} \in \mathrm{K}_1.$$

On vérifie que $\mathrm{M}_{a,b}^2 = \mathrm{I}_2$, donc

$$\mathrm{M}_{a,b}^{-1} = \mathrm{M}_{a,b} \in \mathrm{K}_1.$$

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

Démontrons que K_2 est un groupe.

Soit $\overline{x}$ et $\overline{y}$ 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 déduitt que $\overline{x} \cdot \overline{y} = \overline{xy} \in K_2$, 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 $\overline{1}$. De plus, pour tout $\overline{x} \in K_2$, on a $\overline{x}^2 = \overline{1}$, donc $\overline{x}^{-1} = \overline{x} \in K_2$. 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

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

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

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

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 $H_1 = \{\overline{1}, \overline{3}\}$ et

$H_2 = \{\overline{1}, \overline{5}\}$. 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 $\overline{3} \times \overline{5} = \overline{7}$, on a $K_2 = H_1 H_2$. De plus $H_1 \cap H_2 = (\overline{1})$. 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 $\rho\colon S_3 \to GL(2,\mathbf{R})$ 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 $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ a un déterminant $a^2 + b^2$ non nul, l'application $\rho\colon \mathbf{C}^* \to GL(2,\mathbf{R})$ 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 $\operatorname{Ker}\rho = \{0\}$.

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

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 $j \in \mathrm{G}^{\mathrm{E}}$ définie pour tout $x \in \mathrm{E}$ par $j(x) = e$. Alors pour tout $x \in \mathrm{E}$, 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 $f \in \mathrm{G}^{\mathrm{E}}$ est inversible. On définit $g \in \mathrm{G}^{\mathrm{E}}$ par $g(x) = f(x)^{-1}$ pour tout $x \in \mathrm{E}$. 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 $f, g \in \mathrm{G}^{\mathrm{E}}$. Pour tout $x \in \mathrm{E}$, 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 $a, b \in \mathrm{G}$, et $f, g \in \mathrm{G}^{\mathrm{E}}$ deux applications constantes égales à a et b respectivement. Pour tout $x \in \mathrm{E}$, nous avons $ab = f(x)g(x) = (fg)(x) = (gf)(x) = g(x)f(x) = ba$.

30. a) — La différence de deux fonctions continues sur J est une fonction continue sur J, donc $\mathscr{C}(\mathrm{J})$ est un sous-groupe de $(\mathbf{R}^{\mathrm{J}}, +)$.

— Les fonctions constantes de $\mathbf{R}^{\mathrm{J}}$ sont continues, donc $\Gamma \subseteq \mathscr{C}(\mathrm{J})$. De plus, pour tous réels a et b, on a $c_a - c_b = c_{a-b}$, donc Γ est bien un sous-groupe de $(\mathscr{C}(\mathrm{J}), +)$.

b) F_1 *est un morphisme de groupes.* En effet, pour tout $(f, g) \in \mathscr{C}(\mathrm{J})$, on a $\mathrm{F}_1(f+g) = (f+g)(1) = f(1) + g(1) = \mathrm{F}_1(f) + \mathrm{F}_2(g)$.

F_2 *n'est pas un morphisme de groupes.* En effet, $\mathrm{F}_2(c_{-2}+c_1) = \mathrm{F}_2(c_1) = |c_1(0)| = 2$ et $\mathrm{F}_2(c_{-2}) + \mathrm{F}_2(c_1) = |c_{-2}(0)| + |c_1(0)| = 2 + 1 = 3$.

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 $\mathscr{C}(J)$ est c_0. Si F_5 était un morphisme de groupes, on aurait $F_5(c_0) = 0$ (proposition 1.55), or $F_5(c_0) = 1$.

Soit $a \in \mathbf{R}$. On a $F_1(c_a) = a$, $F_3(c_a) = a$ et $F_4(c_a) = a$.

Pour tout $i \in \{1,3,4\}$, on a $F_i(\mathrm{id}_J - c_{m_i}) = F_i(\mathrm{id}_J) - F_i(c_{m_i}) = F_i(\mathrm{id}_J) - m_i$. Ainsi il existe un unique m_i tel que $F_i(\mathrm{id}_J - c_{m_i}) = 0$; il s'agit de $m_i = F_i(\mathrm{id}_J)$.

On trouve $m_1 = 1$, $m_3 = 1/2$ et $m_4 = 1 - 6 \times (2 - \sqrt{3})/\pi$. Comme m_1, m_3 et m_4 sont deux à deux distincts, ce qui précède permet de conclure que $\operatorname{Ker} F_1$, $\operatorname{Ker} F_3$ et $\operatorname{Ker} F_4$ sont deux à deux distincts.

c) Soit $F \in \operatorname{Hom}(\mathscr{C}(J), \mathbf{R})$. Alors $g = f - c_{F(f)}$ et $h = c_{F(f)}$ sont deux fonctions continues sur J telles que $h \in \Gamma$ et $g \in \operatorname{Ker} F$ car $F(f - c_{F(f)}) = F(f) - F(c_{F(f)}) = F(f) - F(f) = 0$.

Soit $F \in \mathscr{C}(J) \cap \Gamma$. Il existe $a \in \mathbf{R}$ tel que $F = c_a$. Or $F(c_a) = a$, il s'ensuit que $\operatorname{Ker} F \cap \Gamma = \{c_0\}$, la fonction c_0 étant l'élément nul de $\mathscr{C}(J)$.

31. a) L'application $\varphi : G_1 \times G_2 \to G_2 \times G_1$ 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 $\varphi_i : \Gamma_i \to G_i$ $(i = 1,2)$ des isomorphismes et

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

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

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

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

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 $\frac{\mathbf{Z}}{(2)} \times \frac{\mathbf{Z}}{(2)}$. Les seuls sous-groupes de $\frac{\mathbf{Z}}{(2)}$ sont $\{\overline{0}\}$ et $\frac{\mathbf{Z}}{(2)}$. On voit donc que le sous-groupe $\{(\overline{0},\overline{0}), (\overline{1},\overline{1})\}$ de $\frac{\mathbf{Z}}{(2)} \times \frac{\mathbf{Z}}{(2)}$ n'est pas le produit direct de deux sous-groupes de $\frac{\mathbf{Z}}{(2)}$.

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

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

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

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

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

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

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

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

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

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

c'est-à-dire $f_\sharp(\sigma_g) = \sigma_{f(g)} \in \mathrm{Aut}(G_2)$ ou encore $f_\sharp(\mathrm{Int}(G_1)) \subset \mathrm{Int}(G_2)$. Ainsi on définit un homomorphisme de groupes $f_* \colon \mathrm{Int}(G_1) \to \mathrm{Int}(G_2)$ en posant $f_* = f_\sharp|^{\mathrm{Int}(G_2)}_{\mathrm{Int}(G_1)}$. Il est injectif (comme $f_\sharp$) et est aussi surjectif, en effet si $\sigma_g \in \mathrm{Int}(G_2)$, alors $f_*(\sigma_{f^{-1}(g)}) = \sigma_{f(f^{-1}(g))} = \sigma_g$. Donc f_* est un isomorphisme de groupes et $\mathrm{Int}(G_1) \simeq \mathrm{Int}(G_2)$.

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

$$\begin{aligned} \varphi \colon \mathrm{Hom}\Big(G, \prod_{i\in I} G_i\Big) &\to \prod_{i\in I} \mathrm{Hom}(G, G_i) \\ h &\mapsto (p_i \circ h)_{i\in I}. \end{aligned}$$

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

CHAPITRE II

Classes modulo un sous-groupe

1. Il est clair que $H \cap K \leqslant H$ et $H \cap K \leqslant K$ 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 $[H : H \cap K] \leqslant [G : K]$ 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 $i \in \{1, \ldots, n\}$ 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), $[G : H \cap K] \leqslant [G : H][G : K]$. Si $G = HK$, alors toujours d'après a), $[G : H \cap K] = [G : H][G : K]$.

3. a) Soit $(i, j) \in \{1, \ldots, n\}^2$ 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 $i \in \{1, \ldots, n\}$ 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, $\{Hx_i\}_{1\leqslant i\leqslant n}$ 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 $|HK| = n|H| = [K\colon H\cap K]|H|$ puis $|HK| = \dfrac{|K||H|}{|H\cap K|} = |KH|$.

c) H, K sont des sous-groupes du groupe fini HK. Nous pouvons donc appliquer le résultat b) de l'exercice 2 : $[HK\colon H\cap K] = [HK\colon H][HK\colon K]$ c'est-à-dire $\dfrac{|HK|}{|H\cap K|} = \dfrac{|HK|}{|H|}\dfrac{|HK|}{|K|}$ et enfin $|KH| = |HK| = \dfrac{|H||K|}{|H\cap K|}$.

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

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

Dans l'exercice 2, nous avons montré que

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

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

— $\mathscr{R}_{H,K}$ est symétrique : Soit $(x,y) \in G^2$ tel que $x \mathscr{R}_{H,K} y$. Il existe $(h,k) \in H \times K$ tel que $y = hxk$. On en déduit que $x = h^{-1} y k^{-1}$ où $(h^{-1}, k^{-1}) \in H \times K$, donc $y \mathscr{R}_{H,K} x$.

— $\mathscr{R}_{H,K}$ est transitive : Soit $(x,y,z) \in G^3$ tel que $x \mathscr{R}_{H,K} y$ et $y \mathscr{R}_{H,K} z$. 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 $x \mathscr{R}_{H,K} z$.

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

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

b) — λ est injective ; en effet, supposons $\lambda(hxk) = \lambda(h'xk')$, c'est-à-dire $x^{-1}hxk = x^{-1}h'xk'$. On a alors $hxk = h'xk'$.

— 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 Hx_iK et $x_i^{-1}Hx_iK$ sont équipotents, donc $|Hx_iK| = \left|x_i^{-1}Hx_iK\right|$.

β) $x_i^{-1}Hx_i$ est l'image du sous-groupe H de G par l'automorphisme intérieur $G \to G$, $g \mapsto x_i^{-1} g x_i$, il s'ensuit que $x_i^{-1}Hx_i$ est un sous-groupe de G et que $o(x_i^{-1}Hx_i) = o(H)$.

γ) Pour tout i $(1 \leqslant i \leqslant r)$, $x_i^{-1}Hx_i$ et K sont deux sous-groupes finis. Appliquons leurs la formule de l'exercice 3. Il vient

$$\left|x_i^{-1}Hx_iK\right| = \frac{o(x_i^{-1}Hx_i)\, o(K)}{o(x_i^{-1}Hx_i \cap K)},$$

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

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

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

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

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 :

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

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 :

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

On remarque que $\{KeH, H\tau_3 K\} \neq \{HeK, K\tau_3 H\}$, ce qui montre, qu'en général, dans un groupe non abélien, $\mathscr{R}_{H,K} \neq \mathscr{R}_{K,H}$.

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

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

donc $\sigma_a^2 = \mathrm{id}_{\mathbf{R}}$ 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 $\big|f(x) - f(y)\big| = \big|x - y\big|$, 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.

$\mathscr{I}(1)$ *est un sous-groupe non abélien de* $\mathrm{S}_{\mathbf{R}}$. On vérifie sans peine que les symétries et les translations sont des bijections, donc $\mathscr{I}(1) \subseteq \mathrm{S}_{\mathbf{R}}$. De plus, $\mathscr{I}(1)$ est non vide et pour tout $(f, g) \in \mathscr{I}(1)$, on a $f \circ g^{-1} \in \mathscr{I}(1)$. Par conséquent, $\mathscr{I}(1)$ est un sous-groupe de $\mathrm{S}_{\mathbf{R}}$. 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 $\mathscr{I}(1)$ est non abélien.

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

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

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

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

En revanche,

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

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 $\mathscr{I}(1)$, d'où $[\mathscr{I}(1) : \mathrm{T}] = 2$.

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

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

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

$$ax + by = 0.$$

Étant donné que $d = \mathrm{pgcd}(a, b)$, 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

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

L'inclusion opposée est immédiate.

Image de φ. Soit $z \in \operatorname{Im}\varphi$. 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 $z \in \operatorname{Im}\varphi$.

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

b) Montrons que la correspondance

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

est une application. Soient x, x', y, y' dans $\mathbf{Z}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. 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 $\overline{*}$ définie par $\overline{x} \,\overline{*}\, \overline{y} = \overline{x * y}$.

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

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

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 $\overline{*}$ est associative. Réciproquement, si la loi $\overline{*}$ 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 $\overline{*}$ est commutative si et seulement si pour tout $(x,y)\in\mathbf{Z}^2$, on a $\overline{x}\,\overline{*}\,\overline{y}=\overline{y}\,\overline{*}\,\overline{x}$, 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 $\overline{*}$ 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 $\overline{*}$ est associative et commutative.

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

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

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

car n divise $a-b$.

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

Réciproquement, supposons que $(\mathbf{Z}/n\mathbf{Z},\overline{*})$ soit un groupe. Notons $\overline{e}$ son élément neutre. On a $\overline{0}*\overline{e}=\overline{0}=\overline{e}*\overline{0}$, donc $ae\in n\mathbf{Z}$ et $be\in n\mathbf{Z}$. On a également $\overline{1}*\overline{e}=\overline{1}=\overline{e}*\overline{1}$, 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

$$\begin{aligned}\varphi\colon \left(\frac{\mathrm{G}}{\mathrm{H}}\right)_{\mathrm{d}} &\longrightarrow \left(\frac{\mathrm{G}}{\mathrm{H}}\right)_{\mathrm{d}}\\ \mathrm{K}x &\longmapsto \mathrm{K}'gx.\end{aligned}$$

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

— φ est injective. En effet,

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

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

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

CHAPITRE III

Groupes monogènes, symétriques et diédraux

1. 1) a) On a

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

où l est le plus petit commun multiple de r et s, donc l'ordre de (a,b) dans $\mathrm{C}_m \times \mathrm{C}_n$ est l.

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

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

$$G_{15} = \{\overline{k}; 1 \leqslant k \leqslant 14, \operatorname{pgcd}(k,15) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}.$$

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

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

Nous avons :

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\varphi\colon \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_r\rangle \to \mathrm{G}$ 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 $(x_1, x_2, \dots, x_r) \in \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_r\rangle$ et $(y_1, y_2, \dots, y_r) \in \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_r\rangle$, 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 $\langle a_i\rangle \simeq \mathrm{C}_2$. 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 $\mathbf{Q} = \left\langle \frac{m}{n} \right\rangle$. 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 $m(n-1)! \in \mathrm{Z}$, ce qui prouve que l'ensemble $\left\{\frac{1}{n!}\,;\, n \in \mathbf{N}\right\}$ 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 $\mathrm{H} = \langle x \rangle$. 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 $\{p_i/q_i\}_{1 \leqslant i \leqslant r}$ avec $r \in \mathbf{N}^*$. Posons $q = q_1 q_2 \dots q_r$. Alors $q\mathrm{H}$ est un sous-groupe non nul de $\mathbf{Z}$. Il existe donc un entier $a > 0$ tel que $q\mathrm{H} = a\mathbf{Z}$, d'où $\mathrm{H} = (a/q)\mathbf{Z}$. 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 $g \circ g \circ \cdots \circ g$ de n fonctions g. Pour tout $z \in \widetilde{\mathbf{C}}$, on a $g^n(z) = z + n$, donc $g^n \neq \mathrm{id}_{\widetilde{\mathbf{C}}}$. 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 $z \in \widetilde{\mathbf{C}}$. Par suite, $h^n = \mathrm{id}_{\widetilde{\mathbf{C}}}$ si et seulement si $\alpha^n = 1$. Nous en déduisons que h est d'ordre fini dans $\mathscr{H}$ si et seulement si α est une racine de l'unité dans $\mathbf{C}$.

11. Déterminons l'ordre des matrices suivantes :

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

On note I la matrice identité.

Pour toute matrice $M \in GL(2,\mathbf{C})$ 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 $A^2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $A^4 = I$. La matrice A est d'ordre 4.

Ordre de B. En écrivons $B = I + \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ 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 $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, donc pour tout entier $k > 1$, on a $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^k = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. 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 $G = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$. Soit $n \geqslant 1$ 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

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

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

12. a) Soit

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

deux matrices de G. On trouve

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

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

L'application

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

est injective, donc le groupe G est infini.

Les matrices

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

sont des éléments de G tels que

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

donc le groupe G n'est pas abélien.

b) L'application $\varphi\colon \mathbf{R} \to \mathrm{G}$ 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 1er 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 $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ 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 $1\leqslant k\leqslant n-1$. Soit $d=\operatorname{pgcd}(k,n)$. Nous avons les équivalences

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

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

Remarque. Une conséquence immédiate est que x^k $(0\leqslant k<n)$ 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 $e=(xy)^{\omega m}=(x^m)^\omega y^{m\omega}=ey^{m\omega}=y^{m\omega}$ 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 démontration 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 $x^\omega = y^{-\omega} \in < x > \cap < y >= \{e\}$ 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 $o(x^3x^6) = o(e) = 1 < 3 = \text{ppcm}(3,6)$.

d) Les cycles $(\gamma_i)_{1\leqslant i\leqslant 9}$ 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 $(\gamma_i)_{1\leqslant i\leqslant 9}$.

21. *Permutation* σ_1. Les σ_1-orbites non pontuelles 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

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

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 $H \to S_{\mathbf{N}_5 \setminus \{1\}}$, $\sigma \mapsto \sigma\|_{\mathbf{N}_5 \setminus \{1\}}$ 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 $F = \{\sigma \in S_n \,;\, \sigma\|_{\mathbf{N}_r} \in S_{\mathbf{N}_r}\}$. Ainsi, si σ et τ sont deux permutations de F alors $(\sigma \circ \tau^{-1})(\mathbf{N}_r) = \mathbf{N}_r$. Par conséquent, F est un sous-groupe de S_n.

Ordre de F. Soit $\varphi : \mathbf{N}_n \setminus \mathbf{N}_r \to \mathbf{N}_{n-r}$ une bijection. Elle induit une bijection $S_{\mathbf{N}_n \setminus \mathbf{N}_r} \to S_{\mathbf{N}_{n-r}}$, $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$. Alors l'application

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

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

$$\left|S_{\mathbf{N}_r}\right| \times \left|S_{\mathbf{N}_{n-r}}\right| = r!\,(n-r)!.$$

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.

CHAPITRE IV

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 $H \lhd G$, 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 $\overline{\alpha} \in \mathrm{Hom}\left(\frac{G}{H}, \frac{G}{H'}\right)$ tel que $\pi' \circ \alpha = \overline{\alpha} \circ \pi$ où $\pi : G \to \frac{G}{H}$ et $\pi' : G \to \frac{G}{H'}$ sont les épimorphismes canoniques. La remarque 4.33 permet de conclure immédiatement que $\overline{\alpha}$ 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

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

donc

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

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

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

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

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

Le 1er 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 $G_1 = \frac{\mathbf{Z}}{(4)}$, $H_1 = \langle \overline{2} \rangle$, $G_2 = D_2$ 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 $H_1 \lhd G_1$ et $H_2 \lhd G_2$. 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 $\Gamma \subset GL_3(\mathbf{K})$.

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 $GL_3(K)$.

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

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

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

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

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

Soit l'application $\psi : \Gamma \to \mathbf{K} \times \mathbf{K}$ 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 $\operatorname{Ker}\psi = Z(\Gamma)$. Le 1er théorème d'isomorphisme permet de conclure :

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

8. Nous savons déjà que $A_3 \lhd S_3$ (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 $k \in \mathbf{N}_3 \setminus \{i,j\}$. Alors $\gamma \circ \tau \circ \gamma^{-1} = (j,k) \notin H$, donc $H \not\lhd S_3$. 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 $H \lhd K$.

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 $H \not\lhd S_4$.

13. a) Le groupe $\frac{G}{H}$ est d'ordre n, donc pour tout $x \in G$, on a $\overline{x^n} = \overline{x}^n = \overline{e}$, c'est-à-dire $x^n \in H$.

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

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 $s(\sigma\circ\tau\circ\sigma^{-1}) = \sigma(s(\tau))$.

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, $id_E \in S_{(E)}$. 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 $\left|s(\sigma\circ\tau^{-1})\right| \leqslant |s(\sigma)| + |s(\tau)| < \infty$, 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 $\left|s(\tau \circ \sigma \circ \tau^{-1})\right| = |\tau(s(\sigma))| = |s(\sigma)| < \infty$, donc $S_{(E)} \lhd S_E$.

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 $(x_n)_{n\geqslant 0}$ d'éléménts 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 $(x_n)_{n\geqslant 0}$ 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 $\sigma\|_{s(\sigma)} \in S_{s(\sigma)}$. Notons n l'ordre de $\sigma\|_{s(\sigma)}$. 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 $\gamma = (\ldots, x_2, x_{-1}, x_0, x_1, x_2, \ldots)$ 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.

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 $g'^n = xg^nx^{-1}$ 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.

CHAPITRE V

Groupe opérant sur un ensemble

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

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

de sorte que

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

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

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

et

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

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

L'application

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

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

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

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

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

Le noyau de cette action est le sous-groupe

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

Le stabilisateur de 0 est le sous-groupe

$$\begin{aligned}\mathrm{G}_0&=\big\{\mathrm{M}(a,b,c)\in\mathrm{G}\,;\mathrm{M}(a,b,c)\cdot 0=0\big\}\\ &=\big\{\mathrm{M}(a,b,c)\in\mathrm{G}\,;\,b/c=0\big\}\\ &=\big\{\mathrm{M}(a,0,c)\in\mathrm{G}\big\},\end{aligned}$$

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

L'orbite de 0 est l'ensemble

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

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

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

Pour chaque $i \in \{1,\dots,r\}$, $\left|\Omega_{x_i}\right|$ divise $|G| = 15$, donc $\left|\Omega_{x_i}\right| \in \{3,5,15\}$. 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 $\{x_i\}_{1\leqslant i\leqslant r}$ une famille de représentants des G-orbites non ponctuelles. Supposons que E_G soit vide. On a alors

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

Pour chaque $i \in \{1,\dots,r\}$, $\left|\Omega_{x_i}\right|$ divise $|G| = 33$, donc $\left|\Omega_{x_i}\right| \in \{3,11,33\}$. 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 $i \notin \mathrm{supp}(\sigma)$, 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 $G_4 = \{e, (1,2,3), (1,3,2)\}$.

5. Pour toute matrice $M = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in \Gamma$, 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

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

— les quatre demi-droites

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

— 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 $H \lhd G$, 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 $\pi \circ \sigma \circ \pi^{-1} \in \mathrm{H}_y$. Il s'ensuit que $\pi \mathrm{H}_x \pi^{-1} \subseteq \mathrm{H}_y$, d'où $\mathrm{o}(\mathrm{H}_x) \leqslant \mathrm{o}(\mathrm{H}_y)$. Par symétrie, l'inégalité opposée est également vraie, donc $\mathrm{o}(\mathrm{H}_y) = \mathrm{o}(\mathrm{H}_x)$. La conclusion vient du théorème 5.19 et de la proposition 2.15 :

$$|\Omega_x| = \mathrm{o}(\mathrm{H}) / \mathrm{o}(\mathrm{H}_x) = \mathrm{o}(\mathrm{H}) / \mathrm{o}(\mathrm{H}_y) = \left|\Omega_y\right|.$$

b) Supposons que $\mathrm{H} = (e)$, ce que l'énoncé n'exclut pas. Les H-orbites de N_n sont donc toutes ponctuelles. Puisque $n \geqslant 2$, nous en déduisons que H n'est pas transitif sur $\mathbf{N}_n$.

Supposons maintenant que $\mathrm{H} \neq (e)$. Puisque les H-orbites forment une partition de $\mathbf{N}_n$, le nombre d'orbites r, leur cardinal m ainsi que n sont liés par la relation $rm = n$. Étant donné que n est premier, on a $r = 1$. Autrement dit, le groupe H opère transitivement sur N_n.

10. a) — Remarquons que $\mathrm{G}_\mathrm{X} = \bigcap_{x \in \mathrm{X}} \mathrm{G}_x$ et que pour tout $x \in \mathrm{X}$, on a $\mathrm{G}_{gx} = g\mathrm{G}_x g^{-1}$ (théorème 5.18). Il s'ensuit que

$$\mathrm{G}_{g\mathrm{X}} = \bigcap_{x \in \mathrm{X}} \mathrm{G}_{gx} = \bigcap_{x \in \mathrm{X}} g\mathrm{G}_x g^{-1} = g\left(\bigcap_{x \in \mathrm{X}} \mathrm{G}_x\right) g^{-1} = g\mathrm{G}_\mathrm{X} g^{-1}.$$

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

b) Bien entendu, G_X, égal à l'intersection des sous-groupes $\{\mathrm{G}_x ; x \in \mathrm{X}\}$, 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 $\mathscr{P}(\mathrm{E})$ décrite à la question précédente.

Enfin, pour tout $g \in \mathrm{G}^*_\mathrm{X}$, on a $g\mathrm{G}_\mathrm{X} g^{-1} = \mathrm{G}_{g\mathrm{X}} = \mathrm{G}_\mathrm{X}$, donc $\mathrm{G}_\mathrm{X} \lhd \mathrm{G}^*_\mathrm{X}$.

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

11. On a

$$\operatorname{Ker}\varphi = \bigcap_{i=1}^{k} \operatorname{Ker}\pi_i = \bigcap_{i=1}^{k} \mathrm{G}_i = \left\{ g \in \mathrm{G} \,;\, gx = x \text{ pour tout } x \in \bigcup_{i=1}^{k} \mathrm{X}_i = \mathrm{E} \right\}.$$

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

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

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

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

Comme $\left|\Omega_{x_i}\right|$ divise o(G) pour tout $i \in \{1, \ldots, k-1\}$, on a $\left|\Omega_{x_i}\right| \geqslant p$. Par conséquent, $\mathrm{o(G)} \geqslant 1 + (k-1)p$. On a l'inégalité $\mathrm{o(G)}/p < k$ et p divise l'ordre de G, d'où $\mathrm{o(G)}/p \leqslant k-1$, puis $\mathrm{o(G)} \leqslant (k-1)p$. L'encadrement

$$1 + (k-1)p \leqslant \mathrm{o(G)} \leqslant (k-1)p,$$

entraînant $1 \leqslant 0$, nous en déduisons que $\mathrm{Z(G)} \neq (e)$.

17. a) Il est clair que pour tout $(a, a') \in \mathrm{X}^2$ tel que $a \neq a'$, on a $\mathrm{S}(a, \cdot) \cap \mathrm{S}(a', \cdot) = \emptyset$. Par construction, $\mathrm{S}(a, \cdot) \subseteq \mathrm{S}$ pour tout $a \in \mathrm{X}$, d'où l'inclusion $\cup_{a \in \mathrm{X}} \mathrm{S}(a, \cdot) \subseteq \mathrm{S}$. Comme $(a, b) \in \mathrm{S}(a, \cdot)$ pour tout $(a, b) \in \mathrm{S}$, nous avons l'inclusion réciproque, d'où l'égalité $\mathrm{S} = \cup_{a \in \mathrm{X}} \mathrm{S}(a, \cdot)$. 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,

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

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

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

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

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

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

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

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

$$\sum_{g\in G} \left|F(g)\right| = t\,|G| .$$

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

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

CHAPITRE VI

Groupes finis. Théorèmes de Sylow

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.

12. Pour tout $g \in G$, on a $gHg^{-1} \subseteq gKg^{-1} = K$ et $\left|gHg^{-1}\right| = |H|$, 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 $H \lhd K$, il vient $gHg^{-1} = H$. Ainsi nous avons prouvé que $H \lhd G$.

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.

CHAPITRE VII

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 $Z(K) \lhd G$ (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 $K \lhd G$, on déduit $LKL^{-1} \subseteq K$, puis $LK \subseteq KL$. De même, $L \lhd G$ implique $KL \subseteq LK$, si bien que $LK = KL$. La proposition 1.47 permet de conclure.

Montrons que l'application

$$\varphi : K \times L \to KL, (k, l) \mapsto kl$$

est un isomorphisme de groupes.

Vérifions que $kl = lk$ pour tout $(k, l) \in K \times L$. Nous savons que

$$K \lhd G \text{ et } L \lhd G \implies K \cap L \lhd G \text{ et } K \cap L \leqslant K.$$

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

$$\varphi(k, l)\varphi(k', l') = klk'l' = kk'll' = \varphi(kk', ll') = \varphi((k, l)(k', l')).$$

Par construction, φ est clairement surjectif. Enfin, soit $(k,l) \in \mathrm{K} \times \mathrm{L}$ tel que $\varphi(k,l) = e$, c'est-à-dire $kl = e$. Alors $k = l^{-1} \in \mathrm{K} \cap \mathrm{L}$ et $l = k^{-1} \in \mathrm{K} \cap \mathrm{L}$, si bien que $(k,l) = (e,e)$; l'homomorphisme φ est injectif.

En résumé, le sous-groupe KL est isomorphe au groupe $\mathrm{K} \times \mathrm{L}$.

c) Soit H un sous-groupe normal de $\mathbf{Z}$ différent de (0). Il existe $n \in \mathbf{N}^*$ tel que $\mathrm{H} = n\mathbf{Z}$. Soit $\mathrm{H}' = 2n\mathbf{Z}$. Alors $\mathrm{H}' \lhd \mathbf{Z}$ et $\mathrm{H}' < \mathrm{H}$ avec $\mathrm{H}' \neq (0)$. 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.