DU L3 VERS LE M1

Table des matières

1. Quelques rappels

1.1. La notion de groupe.

Définitions 1.1. ◇ Un *groupe* est la donnée d'une paire $(\mathrm{G}, *)$ où G est un ensemble et

$$*\colon \mathrm{G} \times \mathrm{G} \to \mathrm{G}$$

est une loi de composition telle que les trois propriétés suivantes sont satisfaites :
(Unité) il existe un élément $e \in \mathrm{G}$ tel que $e * g = g * e = g$ pour tout $g \in \mathrm{G}$;
(Inverse) pour tout $g \in \mathrm{G}$, il existe $h \in \mathrm{G}$ tel que $g * h = h * g = e$;
(Associativité) pour tous g, h, k dans G, on a $(g * h) * k = g * (h * k)$.

◇ Si de plus on a $g * h = h * g$ pour tous g, h dans G, on dit que le groupe G est *abélien*.
◇ Le cardinal $|\mathrm{G}|$ (fini ou infini) d'un groupe G est appelé *ordre* du groupe.

Remarque 1.1. Un groupe n'est jamais vide.

Lemme 1.1. *Soit* G *un groupe.*
◇ *L'élément unité* e *de* G *tel que* $e * g = g * e = g$ *pour tout* $g \in \mathrm{G}$ *est unique.*
◇ *Pour tout* $g \in \mathrm{G}$, *l'élément* $h \in \mathrm{G}$ *tel que* $g * h = h * g = e$ *est unique.*

Démonstration. ◇ Soient e et e' des éléments unités de G. Alors on a $e' = e * e' = e$.
◇ Soient h et h' deux éléments de G tels que $g * h = h * g = e$ et $g * h' = h' * g = e$. Alors

$$h' = h' * e = h' * (g * h) = (h' * g) * h = e * h = h.$$

□

Définition 1.2. Soient G un groupe et g un élément de G. L'unique élément h de G tel que $g * h = h * g = e$ est appelé *inverse* de g dans G.

Lemme 1.2. *Soit* G *un groupe.*
◇ *Si* g *appartient à* G, *alors* $(g^{-1})^{-1} = g$.
◇ *Si* g *et* h *appartiennent à* G, *alors* $(g * h)^{-1} = h^{-1} * g^{-1}$.
◇ *Si* $(g_i)_{1 \leqslant i \leqslant n}$ *sont des éléments de* G, *alors* $(g_1 * g_2 * \ldots * g_n)^{-1} = g_n^{-1} * g_{n-1}^{-1} * \ldots * g_1^{-1}$.

Démonstration. ◇ En effet, on a $g * g^{-1} = g^{-1} * g = e$ donc $(g^{-1})^{-1} = g$.
◇ On calcule $(g * h)(h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * g^{-1} = e$ et $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * h = e$.
◇ Par récurrence en utilisant le premier point.

□

Corollaire 1.3. *L'application* φ: G $\to$ G, $g \mapsto g^{-1}$ *est bijective.*

Démonstration. Il suffit de montrer que φ est son propre inverse. Mais pour tout $g \in$ G, nous avons $(\varphi \circ \varphi)(g) = \varphi(\varphi(g)) = \varphi(g^{-1}) = (g^{-1})^{-1} = g$. □

Exemples 1.1. ◇ Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes abéliens.
◇ Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la loi $\times$ sont des groupes abéliens.
◇ L'ensemble $\mathrm{GL}(n, \mathbb{R})$ des matrices réelles inversibles de taille n est un groupe pour la multiplication des matrices. Il est non abélien si et seulement si $n \geqslant 2$.
◇ L'ensemble $\mathrm{GL}(V)$ des endomorphismes bijectifs d'un $\mathbb{R}$-espace vectoriel V est un groupe pour la composition. Il est non abélien si et seulement si $\dim V \geqslant 2$.
◇ L'ensemble $\mathcal{S}_n$ des permutations de l'ensemble $[1, n]$ est un groupe pour la composition. Son ordre est $n!$. Il est non abélien si et seulement si $n \geqslant 3$.
◇ L'ensemble des rotations planes de centre O forme un groupe pour la composition. Il est abélien.
◇ Soit E un ensemble. L'ensemble $\mathcal{S}_E$ des bijections de E dans E est un groupe pour la composition.

Dans la suite nous noterons généralement multiplicativement : $(g, h) \mapsto gh$ les lois de groupe, l'élément neutre est alors noté e ou id, l'inverse de g est noté g^{-1}. Cette « règle » a une exception majeure, celle du groupe $\mathbb{Z}$, ses sous-groupes et ses quotients ainsi que des groupes additifs des corps et des espaces vectoriels qui sont notés additivement.

1.2. **Morphisme de groupes.**

Définitions 1.3. Soient G et G′ deux groupes.

- ◇ Un *morphisme de groupes* de G dans G′ est une application $\varphi\colon \mathrm{G} \to \mathrm{G}'$ telle que $\varphi(gh) = \varphi(g)\varphi(h)$ pour tous g et h dans G. L'ensemble des morphismes de groupes de G dans G′ est noté $\mathrm{Hom}(\mathrm{G}, \mathrm{G}')$.
- ◇ Un morphisme de groupes $\varphi\colon \mathrm{G} \to \mathrm{G}'$ est appelé *isomorphisme de groupes* si φ est bijective. L'ensemble des morphismes de groupes de G dans G′ est noté $\mathrm{Isom}(\mathrm{G}, \mathrm{G}')$.
- ◇ Lorsque G′ est égal à G, un morphisme de groupes est appelé *endomorphisme de groupes*. L'ensemble des endomorphismes de groupes de G dans lui-même est noté $\mathrm{End}(\mathrm{G})$.
- ◇ Lorsque G′ est égal à G, un isomorphisme de groupes est appelé *automorphisme de groupes*. L'ensemble des automorphismes de groupes de G dans lui-même est noté $\mathrm{Aut}(\mathrm{G})$.

  Un exemple d'automorphisme est fourni par les *automorphismes intérieurs* ; un tel automorphisme i_g est donné pour $g \in \mathrm{G}$ par la formule $i_g(x) = gxg^{-1}$.
- ◇ Le *noyau* d'un morphisme de groupes $\varphi\colon \mathrm{G} \to \mathrm{H}$ est le sous-groupe de G défini par
$$\ker \varphi = \big\{ g \in \mathrm{G} \,|\, \varphi(g) = e \big\}.$$
  L'image de φ est aussi un sous-groupe de H, noté $\mathrm{im}\,\varphi$.

Lemme 1.4. *Soient $\varphi\colon \mathrm{G} \to \mathrm{G}'$ un isomorphisme de groupes et $\varphi^{-1}\colon \mathrm{G}' \to \mathrm{G}$ l'inverse de φ. Alors φ^{-1} est un morphisme de groupes.*

Démonstration. Soient x et y dans G′. Posons $g = \varphi^{-1}(x)$ et $h = \varphi^{-1}(y)$. Comme φ est un morphisme de groupes, nous avons $\varphi(gh) = \varphi(g)\varphi(h) = xy$. En particulier $\varphi^{-1}(xy) = gh = \varphi^{-1}(x)\varphi^{-1}(y)$. □

Proposition 1.5. *Soit $\varphi\colon \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Alors :*

- ◇ $\varphi(e_{\mathrm{G}}) = e_{\mathrm{G}'}$;
- ◇ $\varphi(g^{-1}) = \varphi(g)^{-1}$ *pour tout* $g \in \mathrm{G}$;
- ◇ $\varphi(g^n) = \varphi(g)^n$ *pour tout* $g \in \mathrm{G}$ *et tout* $n \in \mathbb{Z}$.

Démonstration.

- ◇ Nous avons $\varphi(e_{\mathrm{G}}) = \varphi(e_{\mathrm{G}}e_{\mathrm{G}}) = \varphi(e_{\mathrm{G}})\varphi(e_{\mathrm{G}})$ et en multipliant (à gauche ou à droite) par $\varphi(e_{\mathrm{G}})^{-1}$ nous avons $\varphi(e_{\mathrm{G}}) = e_{\mathrm{G}'}$.
- ◇ Nous avons $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_{\mathrm{G}}) = e_{\mathrm{G}'} = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. Nous avons donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.

◇ Pour $n = 0$ c'est le premier point. Pour $n \geqslant 1$, nous procédons par récurrence sur n. Pour $n \leqslant -1$, nous procédons par récurrence sur $|n| = -n$ en utilisant le second point.

□

Exemples 1.2. ◇ L'application $\log\colon (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ est un isomorphisme de groupes.
◇ L'application $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est l'isomorphisme de groupes réciproque de log.
◇ L'application $\det\colon \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}$ est un morphisme de groupes surjectif (et non injectif) si et seulement si $n \geqslant 2$.
◇ L'application $\varphi\colon (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $\varphi(x) = \exp(2\mathbf{i}\pi x)$ est un morphisme de groupes non injectif et non surjectif.
◇ L'application $\varphi\colon (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ définie par $\varphi(z) = z^n$ est un morphisme surjectif mais non injectif de groupes.

Proposition 1.6. *Soient $\varphi\colon \mathrm{G} \to \mathrm{G}'$ et $\psi\colon \mathrm{G}' \to \mathrm{G}''$ deux morphismes de groupes. Alors $\psi \circ \varphi\colon \mathrm{G} \to \mathrm{G}''$ est un morphisme de groupes.*

Démonstration. Pour tous g et h dans G nous avons

$$(\psi \circ \varphi)(gh) = \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = (\psi \circ \varphi)(g)(\psi \circ \varphi)(h).$$

□

Corollaire 1.7. *Soit* G *un groupe, alors* $(\mathrm{Aut}(\mathrm{G}), \circ)$ *est un groupe* (*c'est un sous-groupe de* $(\mathcal{S}_\mathrm{G}, \circ)$).

Démonstration. L'identité est un automorphisme de groupes. Nous venons de voir que la composée de deux automorphismes de groupes est encore un automorphisme de groupes. Enfin, nous avons vu que l'inverse d'un automorphisme de groupes est un automorphisme de groupes. □

1.3. **Sous-groupes.**

Définition 1.4. Soit G un groupe. Un sous-ensemble $\mathrm{H} \subset \mathrm{G}$ est appelé *sous-groupe* de G s'il vérifie les trois conditions suivantes :
◇ e appartient à H ;
◇ si g appartient à H, alors g^{-1} appartient à H ;
◇ si g, h appartiennent à H, alors gh appartient à H.

Remarques 1.2.
- ◇ On vérifie aisément que si H ⊂ G est un sous-groupe, alors H muni du produit de G est un groupe.
- ◇ Si on oublie la seconde condition de l'énoncé ci-dessus, alors H n'est pas nécessairement un sous-groupe de G (par exemple $H = \mathbb{N} \subset G = \mathbb{Z}$).

Soit G un groupe.
- ◇ Les sous-ensembles $\{e\}$ et G forment toujours des sous-groupes de G. Ils sont appelés *sous-groupes triviaux* de G.
- ◇ Un sous-groupe H ⊂ G tel que H ≠ G est appelé *sous-groupe propre* de G.

Proposition 1.8. *Soient* G *un groupe et* H ⊂ G *un sous-ensemble de* G*. Alors* H *est un sous-groupe de* G *si et seulement si les deux conditions suivantes sont satisfaites :*
- ◇ H *est non vide ;*
- ◇ *si* g*,* h *appartiennent à* H*, alors* gh^{-1} *appartient à* H*.*

Démonstration. Commençons par supposer que H est un sous-groupe de G. Alors $e \in H$ et H est non vide. De plus, si g, h appartiennent à H, alors h^{-1} appartient à H et donc gh^{-1} appartient à H. Réciproquement, si H satisfait les deux conditions ci-dessus, montrons que c'est un sous-groupe. Montrons que e appartient à H. Soit $g_0 \in H$ un élément quelconque (c'est possible car H est non vide). Alors on a $e = g_0 * g_0^{-1} \in H$. Soit $h \in H$ montrons que h^{-1} appartient à H. Comme e appartient à H on a $h^{-1} = e * h^{-1} \in H$. Finalement, si g, h appartiennent à H, montrons que $g * h$ appartient à H. Par ce qui précède, h^{-1} appartient à H donc $g * h = g * (h^{-1})^{-1}$ appartient à H. □

Exemples 1.3.
- ◇ Les sous-ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$.
- ◇ Les sous-ensembles $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.
- ◇ Le sous-ensemble $\{1, -1\}$ de $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{Q}^*, \times)$.
- ◇ Le sous-ensemble $O(n, \mathbb{R}) = \left\{A \in GL(n, \mathbb{R}) \,|\, A^{-1} = {}^tA\right\}$ où ${}^tA$ désigne la transposé de A est un sous-groupe de $GL(n, \mathbb{R})$.
- ◇ Le sous-ensemble $\mathrm{Aff}_+(\mathbb{R}^2)$ défini par
$$\mathrm{Aff}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in GL(2, \mathbb{R}) \,|\, a^2 + b^2 \neq 0 \right\}$$
est un sous-groupe de $GL(2, \mathbb{R})$.
- ◇ Le sous-ensemble $\mathrm{Isom}_+(\mathbb{R}^2)$ défini par
$$\mathrm{Isom}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in GL(2, \mathbb{R}) \,|\, a^2 + b^2 = 1 \right\}$$
est un sous-groupe de $\mathrm{Aff}_+(\mathbb{R}^2)$ et de $GL(2, \mathbb{R})$.

Lemme 1.9. *Soit* G *un groupe.*
- ◇ *Si* H *et* K *sont des sous-groupes de* G*, alors* $\mathrm{H} \cap \mathrm{K}$ *est un sous-groupe de* G*.*
- ◇ *Plus généralement, si* $(\mathrm{H}_\lambda)_{\lambda\in\Lambda}$ *est une famille de sous-groupes de* G*, alors l'intersection* $\bigcap_{\lambda\in\Lambda} \mathrm{H}_\Lambda$ *est un sous-groupe de* G*.*

Démonstration. La première assertion est une conséquence de la seconde. Nous montrons la seconde. Notons $\mathrm{K} = \bigcap_{\lambda\in\Lambda} \mathrm{H}_\lambda$. Il suffit de montrer que K est non vide et que pour tous g, h dans K, on a gh^{-1} appartient à K. Puisque H_λ est un sous-groupe, e appartient à H_λ pour tout λ et donc e appartient à K et K est non vide. Soient maintenant g et h deux éléments de K. Alors g, h appartiennent à H_λ pour tout λ et donc gh^{-1} appartient à H_λ pour tout λ et donc gh^{-1} appartient à K. □

Définitions 1.5. Le cardinal d'un groupe fini est aussi appelé son *ordre*.

Si p est un nombre premier, on appelle *p-groupe* un groupe dont le cardinal est une puissance de p.

Si g est un élément de G, alors l'*ordre* de g est le plus petit entier $n > 0$ (s'il en existe) qui vérifie $g^n = 1$. C'est aussi l'ordre du sous-groupe engendré par g.

Définitions 1.6. Si H est un sous-groupe d'un groupe G, on appelle *classe à gauche* de l'élément $a \in \mathrm{G}$ relativement à H le sous-ensemble

$$a\mathrm{H} = \big\{g \in \mathrm{G} \,|\, g = ah,\, h \in \mathrm{H}\big\};$$

on définit de même les *classes à droite* Ha.

Les classes à gauche forment une partition de G. Leur ensemble est noté G/H ; ce n'est pas un groupe en général.

Définition 1.7. Le cardinal de G/H est appelé l'*indice* de H dans G et est noté $[\mathrm{G} : \mathrm{H}]$.

Lorsque le groupe est fini, la considération des classes à gauche conduit à l'énoncé suivant :

Théorème 1.10 (Théorème de Lagrange)**.** *Si* H *est un sous-groupe du groupe fini* G*, l'ordre de* H *et l'indice de* H *dans* G *divisent l'ordre de* G*.*

Plus précisément nous avons

$$|\mathrm{G}| = |\mathrm{H}| \left|\mathrm{G}/\mathrm{H}\right| = |\mathrm{H}|\,[\mathrm{G} : \mathrm{H}].$$

. *En particulier l'ordre d'un élément $g \in \mathrm{G}$ divise l'ordre de* G.

Définition 1.8. Le groupe des bijections (ou permutations) d'un ensemble E s'appelle le *groupe symétrique* de E et est noté $\mathcal{S}_E$.

Si E et E' ont même cardinal les groupes symétriques associés sont isomorphes. Lorsque $E = \{1, 2, \ldots, n\}$, avec $n \in \mathbb{N}$, nous posons $\mathcal{S}_E = \mathcal{S}_n$ et nous parlons du groupe symétrique standard. L'ordre de ce groupe est $n!$.

Définitions 1.9. Le groupe symétrique contient des permutations remarquables : les *cycles* d'ordre k. Un tel cycle est noté $\sigma = (a_1\ a_2\ \ldots\ a_k)$ avec les $a_i \in E$, distincts et la notation signifie que

$$\begin{cases} \sigma(a) = a \text{ si } a \text{ n'est pas l'un des } a_i \\ \sigma(a_i) = a_{i+1} \text{ où l'indice est pris modulo } k \end{cases}$$

Un tel cycle est un élément d'ordre k, c'est-à-dire vérifie $\sigma^k = \mathrm{id}$).
Pour $k = 2$ nous parlons de *transpositions*.

Le groupe symétrique $\mathcal{S}_n$ est muni d'un morphisme surjectif, appelé *signature*, et noté $\mathrm{sgn}\colon \mathcal{S}_n \to \{1, -1\}$ que l'on peut définir de multiples façons mais dont nous retenons les propriétés suivantes :

- ◇ si τ est une transposition, alors $\mathrm{sgn}(\tau) = -1$,
- ◇ plus généralement si σ est un cycle d'ordre k, alors $\mathrm{sgn}(\sigma) = (-1)^{k+1}$.

Le noyau de sgn est formé des permutations paires (c'est-à-dire les permutations s qui vérifient $\varepsilon(s) = 1$) ; c'est un groupe d'ordre $\frac{n!}{2}$, appelé *groupe alterné* et noté $\mathcal{A}_n$.

1.4. Générateurs d'un groupe.

Proposition-Définition 1.11. *Soient* G *un groupe et* $A \subset \mathrm{G}$ *une partie de* G.
Il existe un plus petit sous-groupe H *de* G *contenant* A. *On dit que* H *est le sous-groupe engendré par* A *ou que les éléments de* A *sont des générateurs de* H. *On note* $\mathrm{H} = \langle A \rangle$.

Démonstration. L'existence de H peut se voir de deux manières :

- ◇ nous considérons tous les sous-groupes de G contenant A (cet ensemble contient au moins G tout entier) et leur intersection convient (d'après le Lemme 1.9 c'est un groupe) ;
- ◇ supposons A non vide (sinon $\mathrm{H} = \{\mathrm{id}\}$), posons $A^{-1} = \left\{x \in \mathrm{G} \,|\, x^{-1} \in A\right\}$ et

$$\mathrm{H} = \left\{a_1 a_2 \ldots a_n \,|\, n \in \mathbb{N},\ a_i \in A \cup A^{-1}\right\}.$$

Alors H est un groupe, contient A et est évidemment le plus petit possible.

□

Exemples 1.4. ◇ Groupes monogènes et cycliques.

Un groupe G engendré par un élément a est dit *monogène*. Il est isomorphe[1] à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier n. Dans le second cas G est *cyclique*. En particulier si $|\mathrm{G}| = p$ est un nombre premier, G n'a pas de sous-groupe non trivial (en vertu du théorème de Lagrange). Ainsi si $a \in \mathrm{G} \smallsetminus \{\mathrm{id}\}$, le groupe G coïncide avec $\langle a \rangle$ donc est cyclique et $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z}$.

◇ Groupes symétrique et alterné.

- Les transpositions engendrent $\mathcal{S}_n$; plus précisément les transpositions (1 2), (1 3), …, ($n-1$ n) engendrent $\mathcal{S}_n$ (on peut le voir par récurrence sur n). On peut même vérifier que la transposition (1 2) et le n-cycle (1 2 3 … n) engendrent $\mathcal{S}_n$.
- Les cycles d'ordre 3 engendrent $\mathcal{A}_n$ pour $n \geqslant 3$. En effet le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et nous avons les formules

$$(a\ b)(b\ c) = (a\ b\ c),$$

$$(a\ b)(a\ c) = (a\ c\ b),$$

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d).$$

Notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$.

1.5. **Sous-groupes distingués.**

Définition 1.10. Soient G un groupe et H un sous-groupe de G. Le sous-groupe H est *distingué* dans G s'il est invariant par automorphisme intérieur, c'est-à-dire si

$$\forall\, a \in \mathrm{G} \quad \forall\, h \in \mathrm{H} \quad aha^{-1} \in \mathrm{H}.$$

On note alors $\mathrm{H} \triangleleft \mathrm{G}$.

Remarques 1.3. ◇ La condition ci-dessus équivaut à : pour tout $a \in \mathrm{G}$ nous avons $a\mathrm{H} = \mathrm{H}a$, c'est-à-dire l'égalité des classes à droite et à gauche modulo H.

◇ Si $\varphi\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, son noyau $\ker\varphi$ est un sous-groupe distingué de G et $\operatorname{im}\varphi \simeq \mathrm{G}/\ker\varphi$.

◇ Réciproquement si G est un groupe, si H est un sous-groupe distingué de G, alors le quotient G/H, ensemble des classes à gauche (ou à droite), est muni d'une structure de groupe et nous avons un morphisme surjectif $p\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ de noyau H.

◇ Enfin on définit une *suite exacte* :

$$1 \longrightarrow \mathrm{N} \xrightarrow{\ i\ } \mathrm{G} \xrightarrow{\ p\ } \mathrm{H} \longrightarrow 1,$$

ici N, G et H désignent des groupes et i, p des morphismes ; la suite est dite *exacte* si

1) i est injectif,
2) p est surjectif,
3) $\operatorname{im} i = \ker p$.

Lorsque les groupes sont abéliens et notés additivement nous écrivons les suites exactes avec des 0 :

$$0 \longrightarrow \mathrm{N} \longrightarrow \mathrm{G} \longrightarrow \mathrm{H} \longrightarrow 0.$$

1. Considérer le morphisme surjectif $\varphi\colon \mathbb{Z} \to \mathrm{G}$, $n \mapsto a^n$.

Exemples 1.5. ◇ Les groupes {id} et G sont toujours des sous-groupes distingués de G.
◇ Si G est abélien, alors tout sous-groupe de G est distingué dans G.
◇ Étudions le groupe $\mathcal{S}_3$ qui a 6 éléments :

$$\mathrm{id}, \qquad \tau_c = (a\ b), \qquad \tau_b = (a\ c), \qquad \tau_a = (b\ c), \qquad \sigma = (a\ b\ c), \qquad \sigma^2 = \sigma^{-1} = (a\ c\ b).$$

Le groupe $\mathcal{S}_3$ contient un sous-groupe distingué d'ordre 3, le sous-groupe $\langle\sigma\rangle = \{1, \sigma, \sigma^2\} = \mathcal{A}_3$, isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et nous avons la suite exacte

$$1 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{S}_3 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

Notons que les sous-groupes $\tau_a = \{\mathrm{id}, \tau_a\}$ etc ne sont pas distingués, en effet

$$\sigma\tau_a\sigma^{-1} = \tau_{\sigma(a)} = \tau_b.$$

Définition 1.11. Un groupe $\mathrm{G} \neq \mathrm{id}$ est *simple* si ses seuls sous-groupes distingués sont {id} et G.

Exemples 1.6. ◇ Le groupe $\mathbb{Z}/p\mathbb{Z}$ est simple si et seulement si p est premier.
◇ Le groupe $\mathcal{A}_n$ est simple dès que $n \geqslant 5$.

L'intérêt des sous-groupes distingués est de permettre le « dévissage » des groupes : si G est un groupe et si H est un sous-groupe distingué de G, on peut essayer de ramener l'étude de G à celle de H et du quotient G/H (si G est fini, ces groupes sont d'ordre plus petit).

La classification des groupes simples finis a été achévée en 1981 (*voir* [Pui82]).

Les groupes classiques fournissent beaucoup d'exemples de groupes simples.

1.6. **Centre et commutateurs.** Soit G un groupe. Donnons deux sous-groupes distingués de G qui existent toujours mais peuvent être triviaux : le centre et le groupe dérivé.

1.6.1. *Le centre.*

Définition 1.12. Le *centre* du groupe G est le sous-groupe de G formé des éléments qui commutent à tous les autres

$$Z(\mathrm{G}) = \big\{a \in \mathrm{G} \,|\, \forall\, g \in \mathrm{G},\ ag = ga\big\}.$$

Le centre $Z(\mathrm{G})$ de G est un sous-groupe distingué de G, c'est même un *sous-groupe caractéristique* de G (c'est-à-dire invariant par tout automorphisme).

Exemples 1.7. ◇ Si G est abélien, alors $Z(\mathrm{G}) = \mathrm{G}$.

◇ Si $\mathrm{G} = \mathcal{S}_n$, avec $n \geqslant 3$, alors $Z(\mathrm{G}) = \{\mathrm{id}\}$. En effet, soit σ un élément non trivial de G ; alors $\sigma(i) = j \neq i$ pour un certain i. Soit $k \neq i$, j et $\tau = (j\ k)$. Alors

$$\sigma\tau(i) = \sigma(i) = j \qquad\qquad \tau\sigma(i) = \tau(j) = k$$

donc $\sigma\tau \neq \tau\sigma$ et σ n'appartient pas au centre de G.

◇ Soit $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions. La multiplication est définie par la règle des signes et des formules

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

Alors $Z(\mathbb{H}_8) = \{\mathrm{id}, -\mathrm{id}\}$ est non trivial.

1.6.2. *Les commutateurs.*

Définitions 1.13. Soit G un groupe.

Soient x et y deux éléments de G. Le commutateur de x et y est l'élément $xyx^{-1}y^{-1}$ de G. Il est noté $[x, y]$. Il est appelé ainsi car il est trivial si et seulement si x et y commutent.

Le *groupe dérivé* $D(\mathrm{G})$ est le sous-groupe engendré par les commutateurs de G.

Le groupe $D(\mathrm{G})$ est un sous-groupe distingué de G, c'est même un sous-groupe caractéristique de G. En effet si φ est un automorphisme de G, alors

$$\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1},$$

et les commutateurs sont conservés. Notons que $\mathrm{G}/D(\mathrm{G})$ est abélien, c'est même le plus grand quotient abélien de G et ceci caractérise $D(\mathrm{G})$.

Exemples 1.8. ◇ Si G est abélien, alors $D(\mathrm{G}) = \{\mathrm{id}\}$.

◇ Si $\mathrm{G} = \mathcal{S}_3$, alors $D(\mathrm{G}) = \{\mathrm{id}, \sigma, \sigma^2\}$.

◇ Si $\mathrm{G} = \mathbb{H}_8$, alors $D(\mathrm{G}) = \{\mathrm{id}, -\mathrm{id}\}$.

◇ Si $\mathrm{G} = \mathcal{A}_5$, alors $D(\mathrm{G}) = \mathcal{A}_5$.

2. Exercices

Exercice 1

Donner un exemple de groupe non abélien.

Exercice 2

Donner un exemple de groupe contenant exactement 3 éléments.

Exercice 3

Quelle est la loi naturelle qui permet de munir l'ensemble $\mathbb{C}^*$ des complexes non nuls d'une structure de groupe ? Quel est l'ordre de $\mathbf{i}$ pour cette loi ? Quel est l'ordre de 2 ?

Exercice 4
Si R est un rectangle (non carré), donner la liste des isométries du plan préservant ce rectangle. Cet ensemble est-il un groupe ?

Exercice 5
Donner un exemple de groupe d'ordre fini, abélien et non cyclique.

Exercice 6
Soit $\sigma \in \mathcal{S}_8$ le produit de cycles suivant

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

Calculer la décompositon canonique de σ.

Exercice 7
Soit T un triangle équilatéral de sommets A, B et C et soit $\mathrm{Isom}(T) = \left\{\mathrm{id},\ s_A,\ s_B,\ s_C,\ r_{\frac{2\pi}{3}},\ r_{-\frac{2\pi}{3}}\right\}$ le groupe des isométries du plan préservant ce triangle.
Expliciter un isomorphisme du groupe $\mathrm{Isom}(T)$ vers le groupe symétrique $\mathcal{S}_3$.

Exercice 8
Soit T un triangle équilatéral de sommets A, B et C et soit $\mathrm{Isom}(T) = \left\{\mathrm{id},\ s_A,\ s_B,\ s_C,\ r_{\frac{2\pi}{3}},\ r_{-\frac{2\pi}{3}}\right\}$ le groupe des isométries du plan préservant ce triangle.
Si $\mathrm{H} = \left\{\mathrm{id},\ s_A\right\}$, donner un exemple d'élément $g \in \mathrm{Isom}(T)$ tel que les classes à gauche et à droite de g soient distinctes, *i.e.* $g\mathrm{H} \neq \mathrm{H}g$.

Exercice 9
Calculer l'ordre de la permutation $\sigma \in \mathcal{S}_{10}$ suivante

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

Exercice 10
Donner une permutation $\sigma \in \mathcal{S}_6$ telle que $\sigma \circ (1\ 3\ 5) \circ \sigma^{-1} = (2\ 4\ 6)$.

Exercice 11
Donner la liste des classes de conjugaison avec leur cardinal pour le groupe alterné $\mathcal{A}_5$.

Exercice 12
Donner un exemple de deux groupes d'ordre 8 non abéliens et non isomorphes.

Exercice 13
Parmi les ensembles suivants lesquels sont des groupes pour l'opération donnée ?

(1) $\mathbb{Q}^*$, $+$;
(2) $\mathbb{Q}^*$, $\cdot$;
(3) $\mathbb{Z}/n\mathbb{Z}$, $\cdot$;
(4) $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $\cdot$;
(5) $\left\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\right\}$, $\cdot$;
(6) $\left\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 0\right\}$, $+$.

Exercice 14
Parmi les groupes suivants lesquels sont abéliens ?

(1) $\mathbb{R}[x]_{\leqslant 8}$, $+$ (les polynômes de degré $d \leqslant 8$ dans une variable x à coefficients réels) ;
(2) $\mathrm{GL}(n, \mathbb{R})$, $\cdot$ (les matrices inversibles de taille $n \times n$ à coefficients réels) ;
(3) $\mathcal{S}_4$, $\circ$.

Exercice 15
Lesquels des ensembles A sont des sous-groupes du groupe G donné ?

(1) $A = \mathbb{R}[x]_8$, $+$ (les polynômes de degré 8) et $\mathrm{G} = \mathbb{R}[x]_{\leqslant 8}$, $+$;
(2) $A = 100\mathbb{Z}$ et $\mathrm{G} = 10\mathbb{Z}$;
(3) $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}/100\mathbb{Z}$;
(4) $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}$.

Exercice 16
Quels sont les éléments de $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$?

(1) $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
(2) $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
(3) $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$;
(4) $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$.

Exercice 17
Pour quelles opérations parmi l'addition $+$ et la multiplication $\cdot$ l'ensemble suivant est-il un groupe ?

(1) $\mathbb{Z}$;
(2) $\mathbb{C}$;
(3) $\mathbb{C}^*$;
(4) $\mathbb{Z}/8\mathbb{Z}$;
(5) $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$;
(6) $\mathbb{Z}/7\mathbb{Z}$;
(7) $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$;
(8) $\{1, -1\}$.

Exercice 18

(1) Quel est l'ordre de 0 dans $\mathbb{Z}$?
(2) Quel est l'ordre de 1 dans $\mathbb{Z}$?
(3) Quel est l'ordre de 2 dans $\mathbb{Z}$?
(4) Quel est l'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$?
(5) Quel est l'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$?

(6) Quel est l'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?

(7) Quel est l'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$?

(8) Quel est l'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?

Exercice 19

Compléter pour obtenir un énoncé correct : Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

(1) k divise l'ordre de G ;

(2) l'ordre de x divise k ;

(3) k divise l'ordre de x.

Exercice 20

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

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

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

(3) $\langle g \rangle = \mathrm{G}$.

Exercice 21

Quelles sont les implications correctes ?

(1) Si G est un groupe abélien, alors G est cyclique ;

(2) Si G est un groupe cyclique, alors G est abélien ;

(3) Si G est d'ordre p, avec p un nombre premier, alors G est cyclique ;

(4) Si G est d'ordre fini et cyclique, alors G est d'ordre premier.

Exercice 22

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

(1) (3 2 4) ;

(2) id ;

(3) (2 4 3)(1) ;

(4) (1)(2)(3)(4).

Exercice 23

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

(1) 9 ;

(2) 11 ;

(3) 12 ;

(4) 24.

Exercice 24

Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. Parmi les énoncés suivants lesquels sont vrais ?

(1) Dans D_8 il y a 4 réflexions et 4 rotations ;

(2) Dans D_8 il y a exactement 4 éléments d'ordre 2 ;

(3) Dans D_8 il y a exactement 4 éléments d'ordre 4.

Exercice 25

Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Parmi les énoncés suivants lesquels sont corrects ?

(1) $G = D_{10}$;

(2) $G = D_5$;

(3) Si $x \in G$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;

(4) Si $x \in G$ est d'ordre 2, alors x préserve exactement deux sommets de $\mathcal{P}$;

(5) Dans G, il y a des éléments d'ordre 1, 2 et 5 ;

(6) Dans G, il y a des éléments d'ordre 1, 2, 5 et 10.

Exercice 26

Soit $(G, *) = (\mathbb{Z}, +)$, $H = 4\mathbb{Z}$ et $g = 3$. Alors $g * H$ est égal à :

(1) $3 + 4\mathbb{Z}$;

(2) $12\mathbb{Z}$;

(3) $\{\ldots, -1, 3, 7, 11, \ldots\}$;

(4) $-5 * H$.

Exercice 27

Soient G un groupe et H un sous-groupe distingué de G. Parmi les énoncés suivants lesquels sont corrects ?

(1) $\forall\, g \in G, \forall\, h \in H$, on a $ghg^{-1} \in H$;

(2) $\forall\, g \in G, \forall\, h \in H$, on a $g^{-1}hg \in H$;

(3) $\forall\, g \in G, \forall\, h \in H$, on a $hgh^{-1} \in H$;

(4) $\forall\, g \in G, \forall\, h \in H$, on a $h^{-1}gh \in H$.

Exercice 28

Soient G un groupe et H un sous-groupe propre de G. Parmi les énoncés suivants lesquels sont corrects ?

(1) En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.

(2) Si H est distingué dans G, alors les classes à gauche dans G suivant H sont des sous-groupes de G ;

(3) En général, il y a autant de classes à gauche que de classes à droite ;

(4) Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;

(5) Soit $g \in G$. Si H est distingué dans G, alors $gH = Hg$.

Exercice 29

Soit G un groupe. Parmi les énoncés suivants lesquels sont corrects ?

(1) Si G n'est pas abélien, alors G a au moins un sous-groupe propre (*i.e.* distinct de $\{e_{\mathrm{G}}\}$ et de G) qui n'est pas distingué dans G ;

(2) Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ;

(3) Si G est abélien et H est un sous-groupe propre de G, alors G/H est abélien ;

(4) Si G n'est pas abélien et H est un sous-groupe distingué propre de G, alors G/H n'est pas abélien ;

(5) Si G est cyclique et H est un sous-groupe de G, alors G/H est cyclique ;

(6) Si G n'est pas cyclique et H est un sous-groupe de G, alors G/H n'est pas cyclique.

Exercice 30

Soient G un groupe et H un sous-groupe de G. Parmi les énoncés suivants lesquels sont corrects ?

(1) Si l'ordre de G est infini, alors le nombre de classes à gauche dans G suivant H est infini ;

(2) Si l'ordre de G est infini et l'ordre de H est infini, alors le nombre de classes à gauche dans G suivant H est infini ;

(3) Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini ;

(4) Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de H ;

(5) Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G.

Exercice 31

Pour l'action $\cdot$ donnée du groupe G sur l'ensemble A, déterminer :

(1) l'élément $\overline{1} \cdot \overline{3}$ si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation ;

(2) l'élément $\overline{5} \cdot \overline{1}$ si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation ;

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

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

Exercice 32

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

(1) L'élément $g \cdot a$ à quel ensemble appartient-il ?

(2) Si $g = e_{\mathrm{G}}$, alors que vaut $g \cdot a$?

(3) Est-ce que l'orbite de a est un sous-ensemble de A ou de G ?

(4) Est-ce que le stabilisateur de a est un sous-ensemble de A ou de G ?

(5) De quel ensemble est-ce que le noyau de l'action est un sous-groupe ?

Exercice 33

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$. Les assertions suivantes sont-elles vraies ou fausses ?

(1) Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$;

(2) Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$;

(3) L'orbite de a est un groupe ;

(4) Le stabilisateur de g est un groupe ;

(5) Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ;

(6) L'action est transitive si et seulement s'il n'y a qu'une seule orbite ;

(7) Le stabilisateur de g est un sous-groupe distingué de G.

Exercice 34
Soit G un groupe. Soient a, b deux éléments de G d'ordre fini. Le groupe engendré par a et b est-il fini ?

Exercice 35
Dans le lemme chinois expliciter rapidement comment on construit l'isomorphisme.

Exercice 36
Donner un exemple de groupe fini simple.

3. Éléments de correction

Solution 1
Le groupe $\mathrm{GL}(2,\mathbb{R})$ des matrices inversibles à coefficients réels n'est pas abélien. En effet

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

mais

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

Un autre exemple était donné par le groupe $\mathrm{Isom}(T)$ des isométries du plan préservant un triangle équilatéral ou encore par le groupe symétrique $\mathcal{S}_3$, c'est-à-dire le groupe contenant les six bijections de l'ensemble $\{1, 2, 3\}$.

Solution 2
Le groupe $\mathbb{Z}/3\mathbb{Z}$ des entiers modulo 3 muni de l'addition. En effet $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

Un autre exemple est donné par le groupe des rotations préservant un triangle équilatéral

$$\mathrm{Isom}^{+}(T) = \{\mathrm{id}, r_{2\pi/3}, r_{-2\pi/3}\}$$

ou encore le groupe

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

des racines cubiques de l'unité.

Solution 3

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

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

Solution 4

L'ensemble en question est bien un groupe pour la composition ; en effet il s'agit d'un sous-groupe du groupe des isométries du plan.

Notons O le centre du rectangle, c'est-à-dire l'intersection de deux diagonales. La liste éléments de $\text{Isom}(R)$ consiste en les 4 isométries suivantes : l'identité, la rotation d'angle π centrée en O et les deux symétries axiales dont les axes passent par les milieux des côtés opposés.

Solution 5

Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ convient.

On peut aussi prendre le groupe des isométries préservant un rectangle qui est en fait isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution 6

La décomposition canonique de σ est

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

Solution 7

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

Solution 8

Par exemple $g = S_B$ convient car

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

et $s_B \circ s_A \neq s_A \circ s_B$ sont deux rotations d'angles opposés.

Notons que le choix de g n'est pas unique : $g = S_C$, $g = r_{2\pi/3}$ ou $g = r_{-2\pi/3}$ convient aussi.

Solution 9

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

Solution 10

Nous avons

$$\sigma \circ (1\ 3\ 5) \circ \sigma^{-1} = (\sigma(1)\ \sigma(3)\ \sigma(5))$$

donc $\sigma = (1\ 2)(3\ 4)(5\ 6)$ convient. Notons que le choix de σ n'est pas unique.

Solution 11

Le groupe $\mathcal{A}_5$ admet 5 classes de conjugaison :

- ◇ la classe de l'identité, de cardinal 1 ;
- ◇ la classe des 3-cycles, de cardinal 20 ;
- ◇ la classe des doubles transpositions, de cardinal 15 ;
- ◇ deux classes de 5-cycles, chacune de cardinal 12.

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

Solution 12

Le groupe diédral D_8 (le groupe des isométries préservant un carré) est non abélien d'ordre 8.

Le groupe des quaternions $\mathbb{H}_8$ engendré par les matrices

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

est également non abélien d'ordre 8.

Ces deux groupes ne sont pas isomorphes ; ils ne contiennent pas le même nombre d'éléments d'ordre 2 : le groupe D_8 en contient 5 alors que $\mathbb{H}_8$ n'en contient qu'un seul.

Solution 13

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

sont des groupes.

Remarque sur le 4. : ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \smallsetminus \{\overline{0}\}, \cdot$ n'est pas un groupe en général. Si n est premier, alors ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \smallsetminus \{\overline{0}\} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}{}^{*}$ est un groupe.

Remarque sur le 6. : l'opération + n'est pas interne. Soient

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad\qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix};$$

nous avons

$$\det A = 0 \qquad \det B = 0 \qquad \det A + B = 1 \neq 0.$$

Solution 14

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

Solution 15

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

Remarque sur le 3. : ${}^{\mathbb{Z}}\!/_{10\mathbb{Z}} \not\subseteq {}^{\mathbb{Z}}\!/_{100\mathbb{Z}}$.

Remarque sur le 4. : ${}^{\mathbb{Z}}\!/_{10\mathbb{Z}} \not\subseteq \mathbb{Z}$.

Solution 16

(1) $\overline{1}, \overline{3}, \overline{5}, \overline{7}$;
(2) $\overline{3}, \overline{5}, \overline{7}, \overline{9}$

sont les éléments de $\left({}^{\mathbb{Z}}\!/_{8\mathbb{Z}}\right)^*$.

Solution 17

(1) $\mathbb{Z}, +$;
(2) $\mathbb{C}, +$;

(3) $\mathbb{C}^*, \cdot$;

(4) $\mathbb{Z}/8\mathbb{Z}, +$;

(5) $\left(\mathbb{Z}/8\mathbb{Z}\right)^*, \cdot$;

(6) $\mathbb{Z}/7\mathbb{Z}, +, \cdot$;

(7) $\left(\mathbb{Z}/7\mathbb{Z}\right)^*, \cdot$;

(8) $\{1, -1\}, \cdot$

sont des groupes.

Solution 18

(1) L'ordre de 0 dans $\mathbb{Z}$ est : 1.

(2) L'ordre de 1 dans $\mathbb{Z}$ est : ∞.

(3) L'ordre de 2 dans $\mathbb{Z}$ est : ∞.

(4) L'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$ est : 2.

(5) L'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.

(6) L'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 1.

(7) L'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.

(8) L'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 3.

Solution 19

Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

2. l'ordre de x divise k.

Remarque sur l'assertion 1. : rappelons que $g^k = e$, $k \in \mathbb{N}^*$, si et seulement si l'ordre $o(g)$ de g divise k. Le théorème de Lagrange assure que $o(g) = |\langle g \rangle|$ divise $|\mathrm{G}|$. Si $k = o(g) + |\mathrm{G}|$, alors

$$g^k = g^{o(g)+|\mathrm{G}|} = g^{o(g)} g^{|\mathrm{G}|} = ee = e$$

mais $k = o(g) + |\mathrm{G}|$ ne divise pas $|\mathrm{G}|$.

Solution 20

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

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

Solution 21

Les assertions correctes sont :

2. Si G est un groupe cyclique, alors G est abélien ; en effet si G est cyclique, il existe $g \in \mathrm{G}$ tel que $\mathrm{G} = \langle g \rangle$. Soient a et b dans G, ils s'écrivent aussi g^ℓ et g^k, ℓ, $k \in \mathbb{Z}$ et

$$ab = g^\ell g^k = g^{\ell+k} = g^{k+\ell} = g^k g^\ell = ba.$$

3. Si G est d'ordre p, avec p un nombre premier, alors G est cyclique. En effet soit $g \in \mathrm{G} \setminus \{e\}$. Le théorème de Lagrange assure que l'ordre de g divise p. Puisque p est premier, l'ordre de g est p et g est un générateur de G.

Remarque sur le 1. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, c'est un groupe abélien, non cyclique.

Remarque sur le 4. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z}$, c'est un groupe d'ordre fini et cyclique mais 4 n'est pas premier.

Solution 22

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

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

Solution 23

L'ordre de l'élément (1 3)(2 4 5)(6 9 8 7) dans $\mathcal{S}_{11}$ est 12. En effet l'élément (1 3)(2 4 5)(6 9 8 7) a pour décomposition en cycles à supports disjoints (1 3)(2 4 5)(6 9 8 7). De plus

$$o\big((1\ 3)\big) = 2 \qquad o\big((2\ 4\ 5)\big) = 3 \qquad o\big((6\ 9\ 8\ 7)\big) = 4$$

L'ordre de (1 3)(2 4 5)(6 9 8 7) est $\mathrm{ppcm}(2, 3, 4) = 12$.

Solution 24

Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. L'énoncé suivant est vrai :

1. Dans D_8 il y a 4 réflexions et 4 rotations.

Les autres assertions sont fausses. En effet id, r, r^2 et r^3 sont des rotations alors que s, sr, sr^2 et sr^3 sont des réflexions. Les éléments d'ordre 2 sont les réflexions et r^2. Les éléments d'ordre 4 sont r et r^3.

Solution 25

Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Les énoncés suivants sont corrects :

1. $\mathrm{G} = \mathrm{D}_{10}$;
3. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;
5. Dans G, il y a des éléments d'ordre 1, 2 et 5.

Solution 26

Soit $(\mathrm{G}, *) = (\mathbb{Z}, +)$, $\mathrm{H} = 4\mathbb{Z}$ et $g = 3$. Alors $g * \mathrm{H}$ est égal à :

1. $3 + 4\mathbb{Z}$;
3. $\{\ldots, -1, 3, 7, 11, \ldots\}$;
4. $-5 * \mathrm{H}$.

Solution 27

Soient G un groupe et H un sous-groupe distingué de G. Les énoncés suivants sont corrects :

1. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$;
2. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $g^{-1}hg \in \mathrm{H}$.

Solution 28

Soient G un groupe et H un sous-groupe propre de G. Les énoncés suivants sont corrects :

1. En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.
3. En général, il y a autant de classes à gauche que de classes à droite ;
4. Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;
5. Soit $g \in \mathrm{G}$. Si H est distingué dans G, alors $g\mathrm{H} = \mathrm{H}g$.

Solution 29

Soit G un groupe. Les énoncés suivants sont corrects :

2. Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ; cela découle de la définition de sous-groupe distingué.
3. Si G est abélien et H est un sous-groupe propre de G, alors G/H est abélien ; En effet soient $g_1\mathrm{H}$ et $g_2\mathrm{H}$ deux éléments de G/H, alors
$$\begin{aligned} g_1\mathrm{H} \cdot g_2\mathrm{H} &= g_1g_2\mathrm{H} \text{ (définition de cette opération)} \\ &= g_2g_1\mathrm{H} \text{ (car G est abélien)} \\ &= g_2\mathrm{H} \cdot g_1\mathrm{H} \text{ (définition de cette opération)} \end{aligned}$$
5. Si G est cyclique et H est un sous-groupe de G, alors G/H est cyclique. En effet soit x un générateur de G. Soit $g\mathrm{H}$ un élément de G/H. Il existe $k \in \mathbb{Z}$ tel que $g = x^k$ donc $g\mathrm{H} = x^k\mathrm{H} = (x\mathrm{H})^k$. Ainsi $x\mathrm{H}$ est un générateur de G/H.

L'assertion 1. est fausse. Le groupe des quaternions $\mathbb{H}_8$ n'est pas abélien et n'a pas de sous-groupe propre qui n'est pas distingué.

L'assertion 4. est fausse. Considérons par exemple les groupes $\mathrm{G} = \mathrm{D}_8$ et $\mathrm{H} = \langle r \rangle$, alors $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$ et donc G/H est abélien.

L'assertion 6. est fausse. Considérons par exemple les groupes $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{H} = \langle(\overline{1}, \overline{0})\rangle$. Le groupe G n'est pas cyclique mais $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$ est cyclique.

Solution 30

Soient G un groupe et H un sous-groupe de G. Les énoncés suivants sont corrects :

3. Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini. En effet les classes à gauche forment une partition de G. Toute classe à gauche suivant H est en bijection avec H. S'il n'y avait qu'un nombre fini de classes à gauche suivant H, alors G serait fini.
5. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G. Cela découle du théorème de Lagrange.

L'assertion 1. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

L'assertion 2. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

Solution 31

(1) Si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{1} \cdot \overline{3}$ est $\overline{1} + \overline{3} = \overline{4}$;

(2) si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{5} \cdot \overline{1}$ est $\overline{5}$;

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

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

Solution 32

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

(1) L'élément $g \cdot a$ appartient à A.

(2) Si $g = e_{\mathrm{G}}$, alors $g \cdot a = a$.

(3) L'orbite de a est un sous-ensemble de A.

(4) Le stabilisateur de a est un sous-ensemble de G ?

(5) Le noyau de l'action est un sous-groupe de G.

Solution 33

Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

(1) Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$; faux : écrire a^{-1} n'a pas de sens.

(2) Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$; vrai : si $g \cdot a = b$, alors $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot b$ soit $(g^{-1}g) \cdot a = g^{-1} \cdot b$ ou encore $a = g^{-1}b$.

(3) L'orbite de a est un groupe ; faux : les orbites forment une partition de A, ce sont des ensembles sans structure.

(4) Le stabilisateur de g est un groupe ; vrai.

(5) Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ; vrai.

(6) L'action est transitive si et seulement s'il n'y a qu'une seule orbite ; vrai.

(7) Le stabilisateur de g est un sous-groupe distingué de G ; faux.

Solution 34

Non (considérer par exemple le groupe G des permutations de $\mathbb{Z}$ engendré par $f(x) = -x$ et $g(x) = 1 - x$. Alors $f \circ f = \mathrm{id}$, $g \circ g = \mathrm{id}$ mais $f \circ g \colon x \mapsto x - 1$ donc $(f \circ g)^n \colon x \mapsto x - n$. Le groupe G contient donc tous les éléments de la forme $x \mapsto x - n$ avec n dans $\mathbb{Z}$. En particulier il est infini.

Solution 35

Lemme chinois. *Si p et q sont premiers entre eux, alors*
$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Soit $\overline{n}$, respectivement $\widehat{n}$, respectivement $\dot{n}$ la classe de n modulo pq, respectivement p, respectivement q. Considérons le morphisme
$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$
Il est injectif car $\mathrm{pgcd}(p, q) = 1$. On conclut grâce à l'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$.

Solution 36

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

Références

[Pui82] L. Puig. La classification des groupes finis simples : bref aperçu et quelques conséquences internes. In *Bourbaki Seminar, Vol. 1981/1982*, volume 92 of *Astérisque*, pages 101–128. Soc. Math. France, Paris, 1982. With the collaboration of Michel Broué.