11 Structures algébriques usuelles

Cahier de calcul : $\varnothing$. **Banque CCINP :** $\varnothing$.

Lois de composition internes

Exercice 1 ●●○○ On pose, pour tous $x, y \in [0\,,1]$,

$$x \star y = x + y - xy.$$

1. Montrer que $([0\,,1], \star)$ est un magma associatif et commutatif avec élément neutre.
2. Quels sont les éléments inversibles de $([0\,,1], \star)$?

Exercice 2 ●●○○ Soit $(E, \leqslant)$ un ensemble totalement ordonné.

1. Montrer que $(x, y) \longmapsto \max\{x, y\}$ définit une loi de composition interne sur E.
2. Montrer que le magma $(E, \max)$ est associatif et commutatif.
3. À quelle condition nécessaire et suffisante $(E, \max)$ possède-t-il un élément neutre ?
4. Si $(E, \max)$ possède un élément neutre, quels sont ses éléments inversibles ?

Exercice 3 ●●○○ Soit E un ensemble et $\mathfrak{R}$ l'ensemble des relations binaires sur E. Pour tous $R, S \in \mathfrak{R}$, on définit la relation $R \star S$ sur E par

$$x(R \star S)y \iff \exists z \in E, \quad xRz \text{ et } zSy.$$

Par ailleurs, on associe à toute fonction $f \in E^E$ la relation R_f définie sur E par

$$xR_f y \iff y = f(x).$$

1. Montrer que $\star$ est associative, mais non commutative en général.
2. Simplifier $R_f \star R_g$, pour tous $f, g \in E^E$.
3. La loi $\star$ admet-elle un élément neutre ?

Exercice 4 ●●●○ **Oral X** Soit E un ensemble fini muni d'une loi de composition interne associative. Montrer qu'il existe $s \in E$ tel que $s^2 = s$.

Groupes

Exercice 5 ●●○○ Pour tous $(x, y), (x', y') \in \mathbb{R}^* \times \mathbb{R}$, on pose

$$(x, y) \star (x', y') = (xx', xy' + y).$$

1. Montrer que $(\mathbb{R}^* \times \mathbb{R}, \star)$ est un groupe. Est-il abélien ?
2. Simplifier $(x, y)^n$, pour tous $(x, y) \in \mathbb{R}^* \times \mathbb{R}$ et $n \in \mathbb{N}$.

Exercice 6 ●●○○

Déterminer l'ensemble des structures de groupe sur un ensemble de cardinal 3.

(Indication : on pourra utiliser les résultats de l'exercice 22).

Exercice 7 ●●○○ On considère les fonctions de $\mathbb{R}\backslash\{0, 1\} \longrightarrow \mathbb{R}\backslash\{0, 1\}$ définies par

$$a : x \longmapsto x, \qquad b : x \longmapsto 1 - x, \qquad c : x \longmapsto \frac{1}{x},$$

$$d : x \longmapsto \frac{x}{x-1}, \qquad e : x \longmapsto \frac{x-1}{x} \qquad \text{et} \qquad f : x \longmapsto \frac{1}{1-x}.$$

Montrer que $\{a, b, c, d, e, f\}$ est un sous-groupe de $(\mathfrak{S}(\mathbb{R}\backslash\{0, 1\}), \circ)$, dont on déterminera la table.

Exercice 8 ●●○○ **Transport de structure**

1. Soit G un groupe, E un ensemble et f une bijection de G sur E. On définit une loi interne $\star$ sur E en posant, pour tous $x, y \in E$,

$$x \star y = f\big(f^{-1}(x) f^{-1}(y)\big).$$

   Montrer que $(E, \star)$ est un groupe.
2. **a.** Montrer que

$$\forall x, y \in \mathbb{R}, \quad \operatorname{th}(x + y) = \frac{\operatorname{th} x + \operatorname{th} y}{1 + \operatorname{th} x \operatorname{th} y}.$$

   b. Pour tous $x, y \in \left]-1\,,1\right[$, on pose

$$x \oplus y = \frac{x + y}{1 + xy}.$$

   Montrer que l'on munit ainsi $(\left]-1\,,1\right[, \oplus)$ d'une structure de groupe abélien.

Exercice 9 ●○○○

Soit $p \in \mathbb{N}^*$. Montrer que l'ensemble

$$\left\{ \exp\left(\frac{2ik\pi}{p^n}\right) \,\middle|\, (k,n) \in \mathbb{Z} \times \mathbb{N} \right\}$$

est un sous-groupe de $\mathbb{C}^*$.

Exercice 10 ●○○○

Montrer que $\{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^*, \quad z^n = 1\}$ est un sous-groupe de $\mathbb{C}^*$.

Exercice 11 ●○○○

Soit $a, b \in \mathbb{N}^*$.
À quelle condition nécessaire et suffisante $\mathbb{U}_a$ est-il un sous-groupe de $\mathbb{U}_b$?

Exercice 12 ●●●○ — Groupe des similitudes et groupes diédraux

On note $\mathcal{S}$ l'ensembles des fonctions $z \longmapsto az+b$ et $z \longmapsto a\overline{z}+b$ sur $\mathbb{C}$, où $(a,b) \in \mathbb{C}^* \times \mathbb{C}$.

1. Montrer que $\mathcal{S}$ est un groupe pour la composition.
2. Soit $n \geqslant 2$. On note $\mathcal{D}_n$ l'ensemble $\{f \in \mathcal{S} \mid f(\mathbb{U}_n) \subset \mathbb{U}_n\}$.
   - **a.** Pourquoi la fonction $f|_{\mathbb{U}_n}$ est-elle bijective de $\mathbb{U}_n$ sur $\mathbb{U}_n$, pour tout $f \in \mathcal{D}_n$.
   - **b.** Montrer que $\mathcal{D}_n$ est un sous-groupe de $\mathcal{S}$, appelé le *groupe diédral de degré n*.
   - **c.** Montrer que $\mathcal{D}_n$ contient $\rho : z \longmapsto e^{2i\pi/n} z$ et $\sigma : z \longmapsto \overline{z}$.
   - **d.** Que vaut la somme des éléments de $\mathbb{U}_n$? En déduire que tout élément de $\mathcal{D}_n$ fixe 0.
   - **e.** Montrer que $\mathcal{D}_n = \left\{ \rho^k s^\varepsilon \,\middle|\, k \in [\![0\,, n-1]\!] \text{ et } \varepsilon \in \{0,1\} \right\}$.

Exercice 13 ●●●○

Soit E un ensemble fini non vide muni d'une opération interne $\star$ associative pour laquelle tout élément est régulier à droite et à gauche. Montrer que E est un groupe.

Exercice 14 ●●○○

Soit G un groupe. Montrer que G est abélien dans les deux situations suivantes :

1. Pour tout $x \in G$, $x^2 = 1_G$.
2. Tout élément de G peut être écrit comme un cube et, pour tous $x, y \in G$,
   $$(xy)^3 = x^3y^3.$$
   - **a.** Montrer que $x^3y^2 = y^2x^3$, pour tous $x, y \in G$.
   - **b.** En déduire que, pour tout $x \in G$, x^2 commute à tout élément de G.
   - **c.** Conclure.

Exercice 15 ●●○○ — Intersection et union de sous-groupes

Soit G un groupe.

1. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G, indexée par un ensemble I. Montrer que $\bigcap_{i\in I} H_i$ est un sous-groupe de G.
2.
   - **a.** Trouver deux sous-groupes de $\mathbb{R}^*$ dont la réunion n'est pas un sous-groupe de $\mathbb{R}^*$.
   - **b.** Soit H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
   - **c.** Soit $(H_n)_{n\in\mathbb{N}}$ une suite croissante de sous-groupes de G. Montrer que $\bigcup_{n\in\mathbb{N}} H_n$ est un sous-groupe de G.

Exercice 16 ●○○○ — Centre d'un groupe

Soit G un groupe.

1. Soit $x \in G$. On appelle *centralisateur de x dans G*, noté $C_G(x)$, l'ensemble des éléments de G qui commutent à x. Montrer que $C_G(x)$ est un sous-groupe de G.
2. On appelle *centre de G*, noté $Z(G)$, l'ensemble des éléments de G qui commutent à tout élément de G. Montrer que $Z(G)$ est un sous-groupe de G.

Exercice 17 ●●○○

Un sous-groupe d'un groupe produit est-il toujours le produit de deux sous-groupes ?

Exercice 18 ●●●○ — Sous-groupes additifs de $\mathbb{R}$ (un grand classique !)

1. Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$.
   - **a.** Justifier l'existence de $a = \inf\left(G \cap \mathbb{R}_+^*\right)$.
   - **b.** Montrer que si $a > 0$, alors $a \in G$ puis $G = a\mathbb{Z}$.
   - **c.** Montrer que si $a = 0$, alors G est dense dans $\mathbb{R}$.
2.
   - **a.** Soit $a, b \in \mathbb{R}^*$. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe dense de $\mathbb{R}$ si et seulement si $\dfrac{a}{b}$ est irrationnel.
   - **b.** En déduire que $\{\cos(n) \mid n \in \mathbb{N}\}$ est dense dans $[-1\,, 1]$.

Exercice 19 ●●○○ — Théorème de Lagrange dans le cas abélien

1. Soit G un groupe abélien fini et $g \in G$.
   - **a.** Montrer que l'application $x \longmapsto gx$ est une bijection de G sur G.
   - **b.** Montrer, en calculant de deux façons le produit $\prod_{x\in G}(gx)$, que $g^{|G|} = 1_G$.
2. Déterminer tous les sous-groupes finis de $\mathbb{C}^*$.

Exercice 20 ●●●○

Montrer que tout groupe fini de cardinal pair possède un élément $x \neq 1_G$ tel que $x^2 = 1_G$.

Exercice 21 ●●○○ Sous-groupes des automorphismes intérieurs

Soit G un groupe. Pour tout $g \in G$, on note σ_g l'application $x \longmapsto gxg^{-1}$ de G dans G.

1. Montrer que σ_g est un automorphisme de G, pour tout $g \in G$.
2. Montrer que l'application $\sigma : g \longmapsto \sigma_g$ est un morphisme de groupes de G dans $\mathrm{Aut}(G)$.
3. Montrer que $\mathrm{Ker}\,\sigma = Z(G)$, où $Z(G)$ est le centre de G (cf. exercice 16).

Exercice 22 ●●○○ Théorème de Cayley Soit G un groupe.

Pour tout $g \in G$, on note μ_g l'application $x \longmapsto gx$ de G dans G.

1. Montrer que, pour tous $g, g' \in G$, $\mu_{gg'} = \mu_g \circ \mu_{g'}$.
2. En déduire que l'application $g \longmapsto \mu_g$ est un morphisme de groupe injectif de G dans $\mathfrak{S}(G)$.

Exercice 23 ●●●○ Soit G et G' deux groupes isomorphes. Montrer qu'il en va de même de $\mathrm{Aut}(G)$ et $\mathrm{Aut}(G')$.

Exercice 24 ●●○○ Somme de caractères

Soit G un groupe fini et χ un morphisme de groupes de G dans $\mathbb{C}^*$. Calculer $\sum_{g \in G} \chi(g)$.

Exercice 25 ●●○○ Soit G un groupe. Montrer que l'application $x \longmapsto x^{-1}$ est un endomorphisme de G si et seulement si G est abélien.

Exercice 26 ●●●○

1. Soit G un groupe et $x \in G$. On pose $\langle x \rangle = \left\{ x^k \mid k \in \mathbb{Z} \right\}$.
   - **a.** Montrer que $\langle x \rangle$ est un sous-groupe de G.
   - **b.** Montrer que les endomorphismes de $\langle x \rangle$ sont exactement les $g \longmapsto g^n$, avec $n \in \mathbb{Z}$.
2. En déduire
   a. $\mathrm{Aut}(\mathbb{Z})$. **b.** $\mathrm{Aut}(\mathbb{Q})$. **c.** $\mathrm{Aut}(\mathbb{U}_n)$, pour tout $n \in \mathbb{N}^*$.

Exercice 27 ●●●○

1. Montrer que les groupes $\mathbb{R}$ et $\mathbb{R}_+^*$ sont isomorphes.
2. Montrer que les groupes $\mathbb{Q}$ et $\mathbb{Q}_+^*$ ne sont pas isomorphes.
   Indication : considérer $\sqrt{2}$.
3. Déterminer l'ensemble des morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Q}_+^*$.

Exercice 28 ●●○○ Oral ENS

Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Anneaux

Exercice 29 ●○○○ Montrer qu'un élément non nul d'un anneau commutatif est régulier pour la multiplication si et seulement s'il n'est pas un diviseur de 0.

Exercice 30 ●●○○ Démontrer que tout anneau intègre fini est un corps.

Exercice 31 ●●○○ Différence symétrique de deux ensembles

Soit E un ensemble. Pour toutes parties A et B de E, on définit la *différence symétrique de A et B*, notée $A \Delta B$, par

$$A \Delta B = (A \cup B) \backslash (A \cap B).$$

1. Illustrer cette définition par un schéma.
2. Que valent $A \Delta A$, $A \Delta \varnothing$ et $A \Delta \overline{A}$?
3. Exprimer $\mathbb{1}_{A \Delta B}$ en fonction de $\mathbb{1}_A$ et $\mathbb{1}_B$.
4. Montrer que $(\mathscr{P}(E), \Delta, \cup)$ est un anneau commutatif.
5. Déterminer $\mathrm{U}(\mathscr{P}(E))$. L'anneau $\mathscr{P}(E)$ est-il intègre ?
6. Soit F une partie de E. Montrer que $\mathscr{P}(F)$ est quasiment un sous-anneau de $\mathscr{P}(E)$. Quelle propriété fait défaut ?

Exercice 32 ●●○○ Anneau des entiers de Gauss

1. Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.
   - **a.** Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
   - **b.** Montrer que, pour tout $z \in \mathbb{Z}[i]$, $|z|^2 \in \mathbb{N}$.
   - **c.** En déduire $\mathcal{U}(\mathbb{Z}[i])$.
2. Même question avec $\mathbb{Z}[i\sqrt{2}] = \left\{ a + ib\sqrt{2} \mid a, b \in \mathbb{Z} \right\}$.

Exercice 33 ●○○○

Déterminer l'unique structure de corps sur un ensemble à deux éléments.

Exercice 34 ●●○○ Soit A un sous-anneau de $\mathbb{R}$.
Montrer que A est dense dans $\mathbb{R}$ si et seulement si $A \cap]0\,,1[= \varnothing$.

Exercice 35 ●●○○ Éléments nilpotents d'un anneau
Soit A un anneau. Un élément $x \in A$ est dit *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$.

1. Si A est intègre, montrer que 0_A est le seul élément nilpotent de A.
2. Montrer que la somme et le produit de deux éléments nilpotents de A qui COMMUTENT sont encore nilpotents.
3. Pour tout $x \in A$ nilpotent, montrer que $1_A - x$ est inversible et déterminer son inverse.
4. Plus généralement, que dire de la somme d'un élément nilpotent et d'un élément inversible qui commutent ?

Exercice 36 ●●●○ Un cas particulier du théorème de Jacobson†
Soit A un anneau. On appelle centre de A, noté $Z(A)$, l'ensemble des éléments de A qui commutent à tout élément de A (pour la multiplication bien sûr).

1. Montrer que $Z(A)$ est un sous-anneau de A.
2. On suppose que $x^3 = x$, pour tout $x \in A$.
   a. Montrer que
   $$\forall (x, y) \in A^2, \quad xy = 0 \implies yx = 0.$$
   b. Soit $x \in A$. On suppose que $x^2 = x$. Montrer que $x \in Z(a)$.
   Indication : on pourra étudier $x(y - xy)$, pour tout $y \in A$
   c. Montrer que, pour tout $x \in A$, $x^2 \in Z(A)$.
   d. En déduire que A est un anneau commutatif.

Exercice 37 ●●○○ Anneau de Boole
Soit A un *anneau de Boole*, *i.e.* un anneau non nul pour lequel $x^2 = x$, pour tout $x \in A$.

1. Montrer que A est commutatif.
2. Déterminer A dans le cas où A est intègre.
3. On définit une relation binaire $\preccurlyeq$ sur A en posant, pour tous $x, y \in A$,
   $$x \preccurlyeq y \iff yx = x.$$
   Montrer que $\preccurlyeq$ est une relation d'ordre.

†. Le théorème de Jacobson énonce plus généralement qu'un anneau A est commutatif dès lors que
$$\forall x \in A, \quad \exists\, n \geqslant 2, \quad x^n = x.$$

Exercice 38 ●●○○

1. Les anneaux $\mathbb{R}$ et $\mathbb{C}$ sont-ils isomorphes ?
2. Déterminer tous les endomorphismes d'anneau de $\mathbb{C}$ dont la restriction à $\mathbb{R}$ est la fonction identité.

Exercice 39 ●○○○ Déterminer les endomorphismes de l'anneau $\mathbb{Z}$.

Exercice 40 ●●○○ Oral X Soit $E = \left\{a + b\sqrt{2} \;\middle|\; (a, b) \in \mathbb{Q}^2\right\}$.
Montrer que E est un sous-corps de $\mathbb{C}$ et en déterminer tous les automorphismes.

Indications

Exercice 13. On pourra utiliser la propriété suivante : si E est un ensemble fini et si $f \in E^E$, alors f est bijective si et seulement si elle est injective.

Exercice 17. Non. Il suffit donc d'exhiber un contre-exemple.

Exercice 18. Pour la question **1**, penser à la division euclidienne dans $\mathbb{R}$ (exemple 41 du chapitre 9) et s'inspirer de l'exemple 41 du cours. En **1.b**, on pourra notamment raisonner par l'absurde et examiner ce qu'il se passe dans $G \cap \left]a\,,2a\right[$.

Exercice 20. On pourra considérer la relation binaire $\sim$ sur G définie par

$$x \sim y \iff x = y \text{ ou } x = y^{-1}$$

et commencer par vérifier qu'il s'agit d'une relation d'équivalence, puis s'intéresser aux classes d'équivalence.

Exercice 24. Les applications de l'exercice 22 suggèrent des changements d'indice dans la somme.

Exercice 28. **3.** Un tel morphisme est de la forme $r \longmapsto a^r$, avec $a \in \mathbb{Q}_+^*$.

Exercice 30. Considérer l'application $x \longmapsto ax$ pour un élément a non nul.

Exercice 37. **1.** Que dire de $(1+x)^2$ et $(x+y)^2$ pour $x, y \in A$.

Éléments de réponses

Exercice 1. **1.** Le neutre est 0. **2.** 0 est le seul élément inversible.

Exercice 2. **3.** E possède un minimum. **4.** Le neutre est le seul élément inversible.

Exercice 3. **2.** $R_f \star R_g = R_{g\circ f}$. **3.** $=$.

Exercice 5. **2.** $\left(x^n, \frac{x^n-1}{x-1}y\right)$.

Exercice 7.

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	a	e	d	b
d	d	e	f	a	b	c
e	e	d	b	c	f	a
f	f	c	d	b	a	e

Exercice 11. a divise b.

Exercice 19. **2.** Les $\mathbb{U}_n$ avec $n \in \mathbb{N}^*$.

Exercice 24. $\displaystyle\sum_{g\in G} \chi(g) = \begin{cases} \operatorname{Card}(G) & \text{si } \chi = \widetilde{1} \\ 0 & \text{sinon.} \end{cases}$

Exercice 26. **2.a** $\operatorname{Aut}((\mathbb{Z},+)) = \{\mathrm{Id}_\mathbb{Z}, -\mathrm{Id}_\mathbb{Z}\}$ et $(\operatorname{Aut}((\mathbb{Z},+)),\circ) \simeq (U(\mathbb{Z}),\times)$.
2.b $\operatorname{Aut}((\mathbb{Q},+)) = \left\{x \longmapsto ax \;\middle|\; a \in \mathbb{Q}^*\right\}$ et $(\operatorname{Aut}((\mathbb{Q},+)),\circ) \simeq (\mathbb{Q}^*,\times)$.
2.c $\operatorname{Aut}((\mathbb{U}_n,\times)) = \{\omega \longmapsto \omega^a \mid a \in [\![0\,,n-1]\!] \text{ et } a \wedge n = 1\}$.

Exercice 27. **1.** Considérer exp ou ln. **3.** Le seul morphisme est le morphisme trivial.

Exercice 28. Il y a seulement la fonction nulle.

Exercice 32. **1.c** $\mathrm{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. **2.c** $\mathrm{U}\big(\mathbb{Z}[i\sqrt{2}]\big) = \{\pm 1\}$.

Exercice 38. **1.** Non. **2.** $\mathrm{Id}_\mathbb{C}$ et $z \longmapsto \overline{z}$.

Exercice 39. $\mathrm{Id}_\mathbb{Z}$.

Exercice 40. Id_E et $a + b\sqrt{2} \longmapsto a - b\sqrt{2}$.