EXERCICES – CHAPITRE 11

STRUCTURES ALGÉBRIQUES USUELLES

⋆ *application directe* ⋆⋆ *mise en œuvre* ⋆⋆⋆ *problème* ⋆⋆⋆⋆ *problème long, en autonomie*

Lois de composition interne

EXERCICE 1 ⋆

Pour chacune des lois suivantes, dire si elle est associative, si elle est commutative, si elle admet un élément neutre et, le cas échéant, déterminer les éléments inversibles. Chaque réponse négative sera justifiée par un contre-exemple explicite.

(a) Sur $\mathbb{R}$, la moyenne $x \star y = \dfrac{x+y}{2}$.

(b) Sur $\mathbb{R}_+$, puis sur $\mathbb{R}$, la loi $x \star y = \max(x, y)$.

(c) Sur $\mathcal{P}(E)$, où E est un ensemble non vide, la différence $A \star B = A \setminus B$.

(d) Sur $\mathbb{N}^*$, la loi $a \star b = a^b$.

(e) Sur $\mathbb{Z}$, la loi $a \star b = a + b + ab$.

EXERCICE 2 ⋆

On note $E = \{1, 2\}$ et $\mathcal{F}(E, E)$ l'ensemble des applications de E dans E. Ces applications sont l'identité id, l'échange s de 1 et 2, et les deux applications constantes c_1 et c_2, de valeurs 1 et 2.

1. Compléter la table de la composition, où la case de la ligne f et de la colonne g contient $f \circ g$.

$\circ$	id	s	c_1	c_2
id				
s				
c_1				
c_2				

2. Lire sur la table l'élément neutre, les éléments inversibles et un couple d'éléments qui ne commutent pas.

3. La remarque du cours qui suit la proposition 3 affirme que, dans la table d'un groupe fini, chaque élément apparaît une fois par ligne. Quelles lignes de cette table la vérifient ? Qu'en conclure ?

EXERCICE 3 ⋆⋆

Inverse à gauche, inverse à droite. Soit $\star$ une loi associative sur un ensemble E, d'élément neutre e.

1. Soit $x \in E$. On suppose qu'il existe a et b dans E tels que $a \star x = e$ et $x \star b = e$. Montrer que $a = b$, et que x est inversible.

2. Dans $(\mathcal{F}(\mathbb{N}, \mathbb{N}), \circ)$, on considère le décalage $d : n \mapsto n + 1$. Montrer que d admet une infinité d'applications g telles que $g \circ d = \mathrm{id}_{\mathbb{N}}$, mais aucune application h telle que $d \circ h = \mathrm{id}_{\mathbb{N}}$.

3. Expliquer pourquoi la question 2 ne contredit pas la question 1, ni la proposition 2 du cours.

EXERCICE 4 ⋆⋆

Éléments simplifiables. Soit E un ensemble ayant au moins deux éléments, et $f \in \mathcal{F}(E,E)$.

1. Montrer que f est simplifiable à gauche pour la composition, c'est-à-dire que $f\circ g = f\circ h$ entraîne $g = h$ pour tous g, h de $\mathcal{F}(E,E)$, si et seulement si f est injective.
2. Montrer de même que f est simplifiable à droite si et seulement si f est surjective.
3. En déduire que, si E est fini, un élément de $\mathcal{F}(E,E)$ simplifiable d'un côté l'est aussi de l'autre. Est-ce encore vrai si $E = \mathbb{N}$?

EXERCICE 5 ⋆⋆

Une table trompeuse. On munit l'ensemble $E = \{e,a,b,c,d,f\}$ de la loi $\star$ définie par la table suivante, où la case de la ligne x et de la colonne y contient $x \star y$.

$\star$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	c	b	f	d
b	b	c	d	f	e	a
c	c	b	f	d	a	e
d	d	f	e	a	c	b
f	f	d	a	e	b	c

1. Vérifier que la loi est commutative, que e est neutre, et que chaque élément apparaît exactement une fois dans chaque ligne et dans chaque colonne. En déduire que tout élément admet un unique symétrique, que l'on précisera.
2. Calculer $(b\star b)\star d$ et $b\star(b\star d)$. L'ensemble $(E,\star)$ est-il un groupe ?
3. Qu'en conclure sur la réciproque de la remarque du cours qui suit la proposition 3 ?

EXERCICE 6 ⋆⋆

Soit $\star$ une loi de composition interne sur un ensemble E, et

$$A = \{x \in E \mid \forall (y,z) \in E^2,\ x\star(y\star z) = (x\star y)\star z\}.$$

Montrer que A est stable par $\star$, et que la loi induite sur A est associative. Que vaut A lorsque $\star$ est la soustraction sur $\mathbb{Z}$?

EXERCICE 7 ⋆⋆⋆

L'argument d'Eckmann et Hilton. Soit X un ensemble muni de deux lois de composition interne $*$ et $\otimes$, admettant chacune un élément neutre, notés 1_* et $1_\otimes$, et telles que

$$\forall (a,b,c,d) \in X^4, \qquad (a\otimes b)*(c\otimes d) = (a*c)\otimes(b*d).$$

1. En choisissant bien a, b, c, d, montrer que $1_* = 1_\otimes$.
2. Montrer que les deux lois sont égales, puis qu'elles sont commutatives et associatives.
3. Vérifier que l'addition des réels, prise comme loi $*$ et comme loi $\otimes$, satisfait l'hypothèse. Peut-on prendre pour $*$ et $\otimes$ l'addition et la multiplication des réels ?

Groupes

EXERCICE 8 ⋆

Les ensembles suivants, munis de la loi indiquée, sont-ils des groupes ? Le cas échéant, sont-ils abéliens ?

(a) $\mathbb{Z}$, avec $a \star b = a + b + 1$;

(b) $\mathbb{Q}^*$, avec la division ;

(c) $\mathcal{F}(\mathbb{R}, \mathbb{R})$, avec l'addition ;

(d) les fonctions monotones de $\mathbb{R}$ dans $\mathbb{R}$, avec l'addition ;

(e) $\mathbb{U} \cup \{0\}$, avec la multiplication ;

(f) $\{-1, 1\}$, avec la multiplication ;

(g) $2\mathbb{Z}$, avec la multiplication ;

(h) $\mathcal{P}(E)$, avec la réunion.

EXERCICE 9 ⋆

Sur $G = \mathbb{R} \setminus \{1\}$, on pose $x \star y = x + y - xy$.

1. Calculer $1 - x \star y$ en fonction de $1 - x$ et $1 - y$. En déduire que $\star$ est une loi de composition interne sur G.
2. Montrer que $\varphi : x \mapsto 1 - x$ est une bijection de G sur $\mathbb{R}^*$ qui vérifie $\varphi(x \star y) = \varphi(x)\varphi(y)$.
3. En déduire, sans autre calcul, que $(G, \star)$ est un groupe abélien, et déterminer son neutre et le symétrique de x.

EXERCICE 10 ⋆⋆

Le groupe affine. Sur $G = \mathbb{R}^* \times \mathbb{R}$, on définit la loi

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

1. Pour $(x, y) \in G$, on note $f_{x,y}$ l'application $t \mapsto xt + y$ de $\mathbb{R}$ dans $\mathbb{R}$. Vérifier que
$$f_{x,y} \circ f_{x',y'} = f_{(x,y)\star(x',y')}.$$
2. En déduire que $(G, \star)$ est un groupe, isomorphe au sous-groupe de $\mathfrak{S}_{\mathbb{R}}$ formé des bijections affines. Préciser le neutre et le symétrique de (x, y). Ce groupe est-il abélien ?
3. Pour $n \in \mathbb{N}^*$, calculer $(x, y)^n$, en distinguant les cas $x = 1$ et $x \neq 1$.

EXERCICE 11 ⋆⋆

Transport de structure.

1. Soit $(G, *)$ un groupe, E un ensemble et $f : G \to E$ une bijection. Montrer que la loi définie par $x \star y = f\big(f^{-1}(x) * f^{-1}(y)\big)$ fait de E un groupe, et que f est un isomorphisme de $(G, *)$ sur $(E, \star)$.
2. Montrer que, pour tous réels a et b,
$$\operatorname{th}(a + b) = \frac{\operatorname{th} a + \operatorname{th} b}{1 + \operatorname{th} a \operatorname{th} b}.$$
3. En déduire que la loi $x \star y = \dfrac{x + y}{1 + xy}$ fait de $]-1, 1[$ un groupe abélien isomorphe à $(\mathbb{R}, +)$.

En relativité restreinte, c'est la loi de composition des vitesses, exprimées en fraction de la vitesse de la lumière : la composée de deux vitesses inférieures à celle de la lumière lui reste inférieure.

EXERCICE 12 ⋆

Soit G un groupe dans lequel tout élément x vérifie $x^2 = e$. Montrer que G est abélien. Donner un exemple d'un tel groupe ayant au moins quatre éléments.

EXERCICE 13 ⋆⋆

Soit G un groupe, et x, y deux éléments de G tels que $x^3 = e$ et $xyx^{-1} = y^2$.

1. Montrer que, pour tout $k \in \mathbb{N}$, $(xyx^{-1})^k = xy^kx^{-1}$.
2. En déduire que $x^2yx^{-2} = y^4$, puis que $y^7 = e$.
3. On suppose de plus que $y^5 = e$. Montrer que $y = e$.

EXERCICE 14 ⋆⋆

Le centre d'un groupe. Soit G un groupe. On appelle *centre* de G l'ensemble

$$Z(G) = \{x \in G \mid \forall a \in G,\ ax = xa\}.$$

1. Montrer que $Z(G)$ est un sous-groupe abélien de G, et que $Z(G) = G$ si et seulement si G est abélien.
2. Déterminer le centre de $\mathfrak{S}_3$. On pourra s'inspirer de la démonstration de la proposition 5 du cours.

EXERCICE 15 ⋆

Dans chaque cas, dire si H est un sous-groupe du groupe G.

(a) $G = (\mathbb{Z}, +)$ et H est l'ensemble des entiers pairs, puis celui des entiers impairs.

(b) $G = (\mathbb{R}, +)$ et $H = [-1\,, +\infty[$.

(c) $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{Q}^*$.

(d) $G = (\mathbb{C}^*, \times)$ et $H = \{z \in \mathbb{C}^* \mid |z| \leqslant 1\}$.

(e) $G = \mathfrak{S}_E$ et $H = \{f \in G \mid f(a) = a\}$, où $a \in E$.

(f) $G = \mathfrak{S}_E$ et $H = \{f \in G \mid f(a) = b\}$, où a et b sont deux éléments distincts de E.

(g) $G = (\mathbb{Z} \times \mathbb{Z}, +)$ et $H = \{(k, k) \mid k \in \mathbb{Z}\}$. Ce sous-groupe est-il de la forme $H_1 \times H_2$, avec H_1 et H_2 sous-groupes de $\mathbb{Z}$?

EXERCICE 16 ⋆

1. Montrer que $\mathbb{U}_\infty = \{z \in \mathbb{C}^* \mid \exists n \in \mathbb{N}^*,\ z^n = 1\}$, ensemble des racines de l'unité, est un sous-groupe de $(\mathbb{C}^*, \times)$. Est-il égal à $\mathbb{U}$? On pourra considérer $\mathrm{e}^{\mathrm{i}\pi\sqrt{2}}$.
2. Montrer que $\mathbb{Q}[\sqrt{2}] \setminus \{0\}$, où $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$, est un sous-groupe de $(\mathbb{R}^*, \times)$.

EXERCICE 17 ⋆⋆

Les solutions entières de $x^2 - 3y^2 = 1$. On pose

$$H = \{x + y\sqrt{3} \mid x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}.$$

On admet que $\sqrt{3}$ est irrationnel, ce qui se démontre comme pour $\sqrt{2}$ au chapitre 7.

1. Montrer que tout élément de H est strictement positif. On comparera x et $|y|\sqrt{3}$.
2. Montrer que H est un sous-groupe de $(\mathbb{R}_+^*, \times)$.
3. Vérifier que $2 + \sqrt{3} \in H$, et en déduire que l'équation $x^2 - 3y^2 = 1$ a une infinité de solutions dans $\mathbb{N} \times \mathbb{Z}$. En donner trois.

EXERCICE 18 ⋆⋆

Réunion de sous-groupes. Soit G un groupe, et H, K deux sous-groupes de G.

1. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
2. En déduire qu'un groupe n'est jamais la réunion de deux sous-groupes distincts de lui-même.
3. Montrer que le groupe $(\mathcal{P}(\{1,2\}), \Delta)$ est la réunion de trois sous-groupes distincts de lui-même.

EXERCICE 19 ⋆

Soit G un groupe et $(H_n)_{n\in\mathbb{N}}$ une suite de sous-groupes de G, croissante pour l'inclusion.

1. Montrer que $\bigcup_{n\in\mathbb{N}} H_n$ est un sous-groupe de G.
2. On prend $G = \mathbb{U}$ et $H_n = \mathbb{U}_{2^n}$. Vérifier que la suite est croissante, et montrer que la réunion n'est pas $\mathbb{U}$ tout entier. On pourra utiliser la proposition 9 du cours.

EXERCICE 20 ⋆⋆⋆

Sous-groupe engendré par une partie. Soit G un groupe et X une partie de G. On note $\langle X\rangle$ l'intersection de tous les sous-groupes de G qui contiennent X.

1. Montrer que $\langle X\rangle$ est un sous-groupe de G contenant X, et qu'il est contenu dans tout sous-groupe contenant X.
2. Montrer que $\langle X\rangle$ est l'ensemble des produits $x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}$, où $n \in \mathbb{N}$, $x_i \in X$ et $\varepsilon_i \in \{-1,1\}$, avec la convention qu'un produit vide vaut e.
3. Déterminer le sous-groupe engendré par $\{4,6\}$ dans $(\mathbb{Z},+)$, par $\{\mathrm{i}\}$ dans $(\mathbb{C}^*,\times)$, et par $\{2,3\}$ dans $(\mathbb{Q}^*,\times)$.

EXERCICE 21 ⋆⋆

Périodes d'une fonction. Soit $f : \mathbb{R} \to \mathbb{R}$. On note $P(f)$ l'ensemble des réels T tels que l'on ait $f(x+T) = f(x)$ pour tout réel x : ce sont les périodes de f.

1. Montrer que $P(f)$ est un sous-groupe de $(\mathbb{R},+)$. Que vaut $P(\mathbf{1}_{\mathbb{Q}})$?
2. Soit $f : x \mapsto \cos\dfrac{\pi x}{12} + \sin\dfrac{\pi x}{8}$. Calculer $f'' + \dfrac{\pi^2}{64} f$, et en déduire que toute période de f est une période de $x \mapsto \cos\dfrac{\pi x}{12}$. Déterminer $P(f)$.
3. Par la même méthode, déterminer $P(g)$ pour $g : x \mapsto \cos x + \sin(\sqrt{2}\,x)$. La somme de deux fonctions périodiques est-elle toujours périodique ?

EXERCICE 22 ⋆

Traduire chacune des égalités suivantes en disant qu'une application est un morphisme entre deux groupes que l'on précisera. Déterminer ensuite le noyau et l'image de ce morphisme, et dire s'il est injectif, surjectif, ou s'il s'agit d'un isomorphisme.

(a) $\ln(xy) = \ln x + \ln y$;

(b) $|zz'| = |z|\,|z'|$;

(c) $\sqrt{xy} = \sqrt{x}\sqrt{y}$;

(d) $\overline{zz'} = \overline{z}\;\overline{z'}$;

(e) $\mathrm{e}^{\mathrm{i}(s+t)} = \mathrm{e}^{\mathrm{i}s}\mathrm{e}^{\mathrm{i}t}$;

(f) $(-1)^{m+n} = (-1)^m(-1)^n$.

EXERCICE 23 ⋆

Soit G un groupe. Montrer que l'application $x \mapsto x^2$ est un endomorphisme de G si et seulement si G est abélien. Même question pour $x \mapsto x^{-1}$.

EXERCICE 24 ⋆⋆

L'exponentielle complexe.

1. Justifier que exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, et déterminer son image et son noyau.
2. Soit $a \in \mathbb{C}^*$ et z_0 une solution de l'équation $e^z = a$. À l'aide du théorème 2 du cours, décrire l'ensemble de toutes les solutions. Résoudre ainsi $e^z = -2$.

EXERCICE 25 ⋆⋆

Morphismes de source $\mathbb{Z}$ ou $\mathbb{Q}$.

1. Soit G un groupe et f un morphisme de $(\mathbb{Z}, +)$ dans G. Montrer que $f(n) = f(1)^n$ pour tout $n \in \mathbb{Z}$. Réciproquement, montrer que, pour tout $x \in G$, il existe un unique morphisme f de $(\mathbb{Z}, +)$ dans G tel que $f(1) = x$.
2. Déterminer tous les endomorphismes du groupe $(\mathbb{Z}, +)$. Lesquels sont injectifs ? surjectifs ?
3. Soit f un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$, et $x \in \mathbb{Q}$. Montrer que $f(x)$ est divisible par 2^m pour tout $m \in \mathbb{N}$, et en déduire que f est nul.

EXERCICE 26 ⋆⋆

Automorphismes intérieurs. Soit G un groupe. Pour $a \in G$, on note $\tau_a : G \to G$ l'application $x \mapsto axa^{-1}$.

1. Montrer que τ_a est un automorphisme de G, et que $\tau_a \circ \tau_b = \tau_{ab}$ pour tous a, b de G.
2. En déduire que $\Phi : a \mapsto \tau_a$ est un morphisme de G dans le groupe $\mathfrak{S}_G$ des permutations de G, et que son image est un sous-groupe de $\mathfrak{S}_G$.
3. Montrer que le noyau de Φ est le centre $Z(G)$ défini à l'exercice 14. Le morphisme Φ est-il injectif lorsque $G = \mathfrak{S}_3$? lorsque G est abélien ?

EXERCICE 27 ⋆⋆

Groupes non isomorphes. Un isomorphisme transporte toute propriété exprimée à l'aide de la seule loi. En exploitant à chaque fois une telle propriété, montrer que les groupes suivants ne sont pas isomorphes.

(a) $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$. On cherchera les éléments x tels que $x^2 = e$.

(b) $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$. On cherchera les éléments x tels que $x^4 = e$.

(c) $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$. On cherchera les éléments qui sont le double d'un autre.

(d) $(\mathbb{R}^*, \times)$ et $(\mathbb{Q}^*, \times)$.

EXERCICE 28 ⋆⋆

Montrer que l'application $z \mapsto \left(\frac{z}{|z|}, |z|\right)$ est un isomorphisme du groupe $(\mathbb{C}^*, \times)$ sur le groupe produit $\mathbb{U} \times \mathbb{R}_+^*$. En déduire que $(\mathbb{C}^*, \times)$ est isomorphe au groupe produit $\mathbb{U} \times \mathbb{R}$, où $\mathbb{R}$ est muni de l'addition. Quelle écriture des nombres complexes non nuls cet isomorphisme traduit-il ?

EXERCICE 29 ⋆⋆

Soit G un groupe fini et f un morphisme de G dans $(\mathbb{C}^*, \times)$ qui n'est pas constant. On pose $S = \sum_{x \in G} f(x)$.

1. Soit $a \in G$ tel que $f(a) \neq 1$. Montrer que $x \mapsto ax$ est une bijection de G sur G, et en déduire que $f(a)S = S$. Conclure que $S = 0$.
2. Retrouver ainsi le résultat du chapitre 4 : pour $n \geqslant 2$ et $k \in \mathbb{Z}$ non multiple de n, la somme des z^k, pour $z \in \mathbb{U}_n$, est nulle.

EXERCICE 30 ⋆⋆⋆

Le théorème de Cayley. Soit G un groupe. Pour $g \in G$, on note $\sigma_g : G \to G$ l'application $x \mapsto gx$.

1. Montrer que σ_g est une permutation de G, et que $\sigma_g \circ \sigma_h = \sigma_{gh}$.
2. En déduire que $g \mapsto \sigma_g$ est un morphisme injectif de G dans $\mathfrak{S}_G$, puis que G est isomorphe à un sous-groupe d'un groupe de permutations.
3. Expliciter les trois permutations σ_g lorsque $G = \mathbb{U}_3$, en notant $j = \mathrm{e}^{2\mathrm{i}\pi/3}$.

Ce théorème, dû à Cayley en 1854, justifie que les groupes de permutations de Lagrange et de Galois contiennent, à isomorphisme près, tous les groupes.

EXERCICE 31 ⋆⋆⋆

Le théorème de Lagrange. Soit G un groupe fini et H un sous-groupe de G. On note card le nombre d'éléments, comme au chapitre 2.

1. On définit sur G la relation $x \sim y$ si et seulement si $x^{-1}y \in H$. Montrer que c'est une relation d'équivalence, et que la classe de x est $xH = \{xh \mid h \in H\}$.
2. Montrer que chaque classe a $\mathrm{card}(H)$ éléments. À l'aide du lemme des bergers du chapitre 2, en déduire que $\mathrm{card}(H)$ divise $\mathrm{card}(G)$.
3. Soit $x \in G$. Montrer, à l'aide du principe des tiroirs, qu'il existe deux entiers $0 \leqslant i < j$ tels que $x^i = x^j$, puis qu'il existe un plus petit entier $p \geqslant 1$ tel que $x^p = e$. Cet entier est appelé l'*ordre* de x.
4. Montrer que $\{e, x, \ldots, x^{p-1}\}$ est un sous-groupe de G à p éléments. En déduire que p divise $\mathrm{card}(G)$, puis que $x^{\mathrm{card}(G)} = e$.
5. Soit G un groupe dont le nombre d'éléments est un nombre premier q. Montrer que G est isomorphe à $(\mathbb{U}_q, \times)$.

EXERCICE 32 ⋆⋆

Noyau, image et nombre d'éléments. Soit $f : G \to G'$ un morphisme de groupes, G étant fini.

1. À l'aide du théorème 2 du cours et du lemme des bergers, montrer que
$$\text{card}(G) = \text{card}(\text{Ker}\, f) \times \text{card}(\text{Im}\, f).$$
2. Soit $n \in \mathbb{N}^*$. Déterminer l'image du morphisme $z \mapsto z^2$ de $\mathbb{U}_n$ dans lui-même, en distinguant selon la parité de n.
3. Soit G un groupe abélien fini ayant un nombre impair d'éléments. À l'aide de l'exercice 31, montrer que $x \mapsto x^2$ est un automorphisme de G, et en déduire que tout élément de G est un carré.

EXERCICE 33 ⋆⋆

Les sous-groupes de $\mathfrak{S}_3$. On note t_1, t_2, t_3 les trois permutations de $\{1,2,3\}$ qui échangent deux éléments et fixent le troisième, t_k fixant k, et c la permutation $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$.

1. Vérifier que $\mathfrak{S}_3 = \{\text{id}, c, c^2, t_1, t_2, t_3\}$, et dresser la table de la composition.
2. À l'aide du théorème de Lagrange de l'exercice 31, déterminer tous les sous-groupes de $\mathfrak{S}_3$.
3. Représenter le schéma des inclusions entre ces sous-groupes, à la manière de celui des $\mathbb{U}_d$ dans le cours, en indiquant dans chaque nœud le nombre d'éléments du sous-groupe.

Anneaux et corps

EXERCICE 34 ⋆

Dans chaque cas, dire si B est un sous-anneau de l'anneau A, muni des opérations usuelles.

(a) $A = \mathbb{Z}$ et $B = \mathbb{N}$, puis $B = 2\mathbb{Z}$.

(b) $A = \mathbb{R}^{\mathbb{N}}$, anneau des suites réelles muni des opérations terme à terme, et B est l'ensemble des suites convergentes, puis celui des suites de limite nulle, puis celui des suites bornées.

(c) $A = \mathcal{F}(\mathbb{R}, \mathbb{R})$ et B est l'ensemble des fonctions paires, puis celui des fonctions impaires, puis celui des fonctions continues.

(d) $A = \mathbb{R}$ et $B = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a,b) \in \mathbb{Z}^2\}$, puis $B = \{a + b\sqrt[3]{2} \mid (a,b) \in \mathbb{Z}^2\}$.

EXERCICE 35 ⋆⋆

Les rationnels à dénominateur impair. On note A l'ensemble des rationnels qui peuvent s'écrire $\dfrac{m}{n}$, avec $m \in \mathbb{Z}$ et n entier naturel impair.

1. Montrer que A est un sous-anneau de $\mathbb{Q}$.
2. Soit $x \in A$, écrit $x = \dfrac{m}{n}$ avec n impair. Montrer que la parité de m ne dépend pas de l'écriture choisie.
3. Montrer que x est inversible dans A si et seulement si m est impair. L'anneau A est-il un corps ?

EXERCICE 36 ⋆⋆

Soit A un anneau, et a, b deux éléments de A.

1. Montrer que $(a+b)^2 = a^2 + 2ab + b^2$ si et seulement si a et b commutent.
2. On suppose que $1-ab$ est inversible, d'inverse u. Montrer que $1-ba$ est inversible, et exprimer son inverse à l'aide de a, b et u. On cherchera cet inverse sous la forme $1+b\,v\,a$, avec $v \in A$ à déterminer.

EXERCICE 37 ⋆⋆

Les nombres duaux. Sur $\mathbb{R}^2$, on définit l'addition terme à terme et la multiplication

$$(a,b) \times (c,d) = (ac,\ ad+bc).$$

1. Montrer que $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, dont on précisera l'unité.
2. On note $1 = (1,0)$ et $\varepsilon = (0,1)$, et l'on identifie le réel a à $(a,0)$. Vérifier que $(a,b) = a + b\varepsilon$ et que $\varepsilon^2 = 0$. L'anneau est-il intègre ?
3. Déterminer les éléments inversibles, et l'inverse de $a+b\varepsilon$ lorsqu'il existe.
4. À l'aide du théorème 3 du cours, calculer $(a+b\varepsilon)^n$ pour $n \in \mathbb{N}^*$. En déduire que, pour toute fonction polynomiale $P : x \mapsto \sum_{k=0}^{d} c_k x^k$ à coefficients réels, on a $P(a+\varepsilon) = P(a) + P'(a)\varepsilon$.

La dernière égalité est le principe de la *dérivation automatique*, qu'utilisent les logiciels de calcul : on obtient la dérivée d'une fonction en calculant avec des nombres duaux.

EXERCICE 38 ⋆⋆⋆

Un anneau non commutatif. Soit $(G,+)$ un groupe abélien, et $\mathrm{End}(G)$ l'ensemble de ses endomorphismes. Pour f et g dans $\mathrm{End}(G)$, on note $f+g$ l'application $x \mapsto f(x)+g(x)$.

1. Montrer que $(\mathrm{End}(G), +, \circ)$ est un anneau, dont on précisera le zéro et l'unité. Où sert l'hypothèse que G est abélien ?
2. On prend $G = (\mathbb{Z}^2, +)$, et l'on considère les endomorphismes $s : (a,b) \mapsto (b,a)$, $p : (a,b) \mapsto (a,0)$ et $h : (a,b) \mapsto (0,a)$. Calculer $s \circ p$, $p \circ s$ et $h \circ h$. Que peut-on en conclure sur l'anneau $\mathrm{End}(\mathbb{Z}^2)$?
3. À l'aide de l'exercice 25, montrer que l'anneau $\mathrm{End}(\mathbb{Z})$ est isomorphe à l'anneau $\mathbb{Z}$.

Le chapitre 16 retrouvera l'anneau $\mathrm{End}(\mathbb{Z}^2)$ sous la forme d'un anneau de matrices.

EXERCICE 39 ⋆⋆

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

1. Montrer que, dans un anneau intègre, le seul élément nilpotent est 0. Donner un élément nilpotent non nul dans l'anneau de l'exercice 37, puis dans celui de l'exercice 38.
2. Soit x et y deux éléments de A tels que xy soit nilpotent. Montrer que yx est nilpotent.
3. Soit x et y deux éléments nilpotents qui commutent. Montrer que xy et $x+y$ sont nilpotents.
4. Dans l'anneau $\mathrm{End}(\mathbb{Z}^2)$, on considère $h : (a,b) \mapsto (0,a)$ et $k : (a,b) \mapsto (b,0)$. Montrer que h et k sont nilpotents, mais que ni $h+k$ ni $h \circ k$ ne le sont. Quelle hypothèse de la question 3 fait défaut ?
5. Soit x nilpotent, avec $x^n = 0$. Montrer que $1-x$ est inversible, et donner son inverse.

EXERCICE 40 ⋆⋆

Anneaux de Boole. Un anneau A est dit *de Boole* si $x^2 = x$ pour tout $x \in A$.

1. Montrer que, pour tout ensemble E, l'anneau $(\mathcal{P}(E), \Delta, \cap)$ du cours est de Boole.
2. Soit A un anneau de Boole. En développant $(x+x)^2$, montrer que $x + x = 0$ pour tout $x \in A$. En développant $(x+y)^2$, montrer que A est commutatif.
3. Montrer qu'un anneau de Boole intègre a exactement deux éléments. Pour quels ensembles E l'anneau $\mathcal{P}(E)$ est-il intègre ?
4. Soit X une partie de E, distincte de $\varnothing$ et de E. Montrer que $\{\varnothing, X, E \setminus X, E\}$ est le plus petit sous-anneau de $\mathcal{P}(E)$ contenant X.

EXERCICE 41 ⋆⋆

Les entiers d'Eisenstein. On note $j = \mathrm{e}^{2\mathrm{i}\pi/3}$ et $\mathbb{Z}[j] = \{a + bj \mid (a,b) \in \mathbb{Z}^2\}$.

1. Vérifier que $j^2 = -1 - j$, et en déduire que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.
2. Montrer que $|a + bj|^2 = a^2 - ab + b^2$ pour tous réels a et b.
3. En s'inspirant de l'étude de $\mathbb{Z}[\mathrm{i}]$ dans le cours, déterminer les éléments inversibles de $\mathbb{Z}[j]$, et reconnaître le groupe qu'ils forment.

EXERCICE 42 ⋆⋆⋆

Les inversibles de $\mathbb{Z}[\sqrt{2}]$. On note $A = \mathbb{Z}[\sqrt{2}]$, sous-anneau de $\mathbb{R}$ d'après l'exercice 34, et, pour $x = a + b\sqrt{2}$ avec a, b entiers, $\sigma(x) = a - b\sqrt{2}$ et $N(x) = x\,\sigma(x)$.

1. Justifier que σ est bien définie, que c'est un automorphisme de l'anneau A, puis que l'on a $N(xy) = N(x)N(y)$ et $N(x) = a^2 - 2b^2$, qui est un entier.
2. Montrer que x est inversible dans A si et seulement si $N(x) = \pm 1$.
3. Montrer que $1 + \sqrt{2}$ est inversible et que ses puissances sont deux à deux distinctes. Que peut-on en conclure sur $A^\times$? Comparer avec $\mathbb{Z}[\mathrm{i}]^\times$.
4. Montrer que, pour tout $k \in \mathbb{N}$, il existe un entier naturel a tel que $(1+\sqrt{2})^k = \sqrt{a} + \sqrt{a+1}$. Le vérifier pour $k = 2$ et $k = 3$.

EXERCICE 43 ⋆

Les anneaux commutatifs suivants sont-ils des corps ? Justifier chaque réponse.

(a) $\mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b \mid (a,b) \in \mathbb{Q}^2\}$, sous-anneau de $\mathbb{C}$;

(b) l'anneau $\mathbb{D}$ des nombres décimaux, puis l'anneau $\mathbb{Z}[\mathrm{i}]$;

(c) l'anneau des nombres duaux de l'exercice 37 ;

(d) l'anneau $\mathcal{F}(X, \mathbb{R})$, où X a au moins deux éléments ;

(e) l'anneau $(\mathcal{P}(E), \Delta, \cap)$, où E a un seul élément.

EXERCICE 44 ⋆⋆

Anneaux intègres finis.

1. Soit A un anneau intègre fini, et $a \in A \setminus \{0\}$. Montrer que l'application $x \mapsto ax$ est injective, puis, à l'aide du théorème 2 du chapitre 2, qu'elle est bijective. En déduire que A est un corps.
2. Soit $\mathbb{K}$ un corps fini. Déterminer les éléments x de $\mathbb{K}$ tels que $x = x^{-1}$. En regroupant chaque élément avec son inverse, en déduire que le produit de tous les éléments non nuls de $\mathbb{K}$ vaut -1.
3. Vérifier ce résultat sur le corps de l'exercice 43 (e).

EXERCICE 45 ⋆⋆⋆

Morphismes d'anneaux.

1. Soit A un anneau. Montrer qu'il existe un unique morphisme d'anneaux de $\mathbb{Z}$ dans A.
2. Montrer que le seul endomorphisme de l'anneau $\mathbb{Q}$ est l'identité.
3. Soit f un endomorphisme de l'anneau $\mathbb{R}$.
   (a) Montrer que $f(x) = x$ pour tout $x \in \mathbb{Q}$.
   (b) Montrer que $f(x) \geqslant 0$ pour tout $x \geqslant 0$, en écrivant x comme un carré. En déduire que f est croissante.
   (c) À l'aide de la densité de $\mathbb{Q}$ dans $\mathbb{R}$ (chapitre 7), montrer que $f = \mathrm{id}_{\mathbb{R}}$.
4. Déterminer les endomorphismes f de l'anneau $\mathbb{C}$ tels que $f(x) = x$ pour tout $x \in \mathbb{R}$.
5. Déterminer les automorphismes de l'anneau $\mathbb{Q}[\sqrt{2}]$. On montrera qu'un tel automorphisme envoie $\sqrt{2}$ sur $\sqrt{2}$ ou sur $-\sqrt{2}$.

Exercices de synthèse

EXERCICE 46 ⋆⋆

Vrai ou faux ? Justifier chaque réponse par une démonstration ou un contre-exemple.

1. Toute loi de composition interne associative admet un élément neutre.
2. Dans un groupe, $(xy)^{-1} = y^{-1}x^{-1}$ pour tous x et y.
3. Dans un groupe, si $x^2 = y^2$ et $x^3 = y^3$, alors $x = y$.
4. La réunion de deux sous-groupes d'un groupe est un sous-groupe.
5. Un endomorphisme injectif d'un groupe fini est un automorphisme.
6. Les groupes $(\mathbb{U}_4, \times)$ et $(\mathcal{P}(\{1,2\}), \Delta)$ sont isomorphes.
7. Dans un anneau, si $ab = 0$, alors $a = 0$ ou $b = 0$.
8. Tout sous-anneau d'un corps est un anneau intègre.
9. Le groupe des inversibles de $\mathbb{Z}[\mathrm{i}]$ est isomorphe au groupe des rotations du carré de l'introduction du cours.
10. Dans un anneau intègre fini, tout élément non nul est inversible.

EXERCICE 47 ⋆⋆

Les lois que respectent toutes les permutations. Soit E un ensemble non vide muni d'une loi de composition interne $\star$. On suppose que toute permutation σ de E respecte la loi, c'est-à-dire que

$$\forall (x, y) \in E^2, \qquad \sigma(x \star y) = \sigma(x) \star \sigma(y).$$

1. Vérifier que la loi définie par $x \star y = x$ possède cette propriété, quel que soit l'ensemble E.
2. On suppose dans cette question que E a au moins trois éléments. Montrer que $x \star x = x$ pour tout $x \in E$. On raisonnera par l'absurde, à l'aide d'une permutation qui échange deux éléments bien choisis et fixe tous les autres.
3. On suppose désormais la loi $\star$ commutative. Soit x et y deux éléments distincts de E. En utilisant la permutation qui échange x et y, montrer que $x \star y \notin \{x, y\}$. En déduire que E ne peut pas avoir exactement deux éléments.

4. La loi étant toujours commutative, montrer que E ne peut pas avoir quatre éléments ou plus. Conclure que E a un ou trois éléments.

5. On prend $E = \{a, b, c\}$. Montrer qu'il existe une unique loi commutative sur E que respectent toutes les permutations, et dresser sa table. Est-elle associative ? Admet-elle un élément neutre ?

EXERCICE 48 ⋆⋆

Ce que les idempotents savent des intervalles. Un élément p d'un anneau A est dit *idempotent* si $p^2 = p$; par exemple, 0 et 1 sont idempotents. Pour une partie D de $\mathbb{R}$, on note $\mathcal{C}(D)$ l'ensemble des fonctions continues de D dans $\mathbb{R}$.

1. Montrer que $\mathcal{C}(D)$ est un sous-anneau de $\mathcal{F}(D, \mathbb{R})$, et que les idempotents de l'anneau $\mathcal{F}(D, \mathbb{R})$ sont les fonctions indicatrices $\mathbf{1}_X$, où X décrit $\mathcal{P}(D)$.

2. Soit I un intervalle de $\mathbb{R}$. À l'aide du théorème des valeurs intermédiaires, montrer que les seuls idempotents de l'anneau $\mathcal{C}(I)$ sont 0 et 1.

3. Montrer que l'anneau $\mathcal{C}(\mathbb{R}^*)$ possède exactement quatre idempotents. Plus généralement, pour $n \in \mathbb{N}$, on note $D_n = \mathbb{R} \setminus \{1, 2, \dots, n\}$, avec $D_0 = \mathbb{R}$. Déterminer le nombre d'idempotents de l'anneau $\mathcal{C}(D_n)$.

4. Soit $f : A \to B$ un isomorphisme d'anneaux. Montrer que f induit une bijection de l'ensemble des idempotents de A sur celui de B. En déduire que les anneaux $\mathcal{C}(D_n)$, pour $n \in \mathbb{N}$, sont deux à deux non isomorphes ; en particulier, $\mathcal{C}(\mathbb{R})$ et $\mathcal{C}(\mathbb{R}^*)$ ne sont pas isomorphes.

5. On note $g : \mathbb{R} \to \mathbb{R}^*$ l'application définie par $g(x) = x + 1$ si $x \in \mathbb{N}$, et $g(x) = x$ sinon. Montrer que g est bijective, puis que $\varphi \mapsto \varphi \circ g$ est un isomorphisme de l'anneau $\mathcal{F}(\mathbb{R}^*, \mathbb{R})$ sur l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$. Quelle hypothèse fait la différence avec la question 4 ?

EXERCICE 49 ⋆⋆⋆

Les groupes à quatre éléments. Soit G un groupe à quatre éléments, de neutre e. On utilise le théorème de Lagrange et la notion d'ordre de l'exercice 31.

1. Quels sont les ordres possibles des éléments de G ?

2. On suppose que G possède un élément x d'ordre 4. Montrer que $G = \{e, x, x^2, x^3\}$, puis que G est isomorphe à $(\mathbb{U}_4, \times)$.

3. On suppose que G ne possède aucun élément d'ordre 4. Montrer que $x^2 = e$ pour tout $x \in G$, que G est abélien, puis que $G = \{e, a, b, ab\}$ pour deux éléments a et b bien choisis. Dresser la table de G, et montrer que G est isomorphe à $(\mathcal{P}(\{1, 2\}), \Delta)$.

4. Conclure : combien y a-t-il de groupes à quatre éléments, à isomorphisme près ? Sont-ils tous abéliens ?

5. Montrer de même que tout groupe ayant 2, 3 ou 5 éléments est isomorphe à un $\mathbb{U}_n$. Quel est le plus petit nombre d'éléments d'un groupe non abélien ?

EXERCICE 50 ⋆⋆⋆

Combien faut-il de générateurs ? Pour un groupe fini G, on appelle *rang* de G, et l'on note $r(G)$, le plus petit nombre d'éléments d'une partie X de G telle que $\langle X \rangle = G$, avec la notation de l'exercice 20. On utilise le théorème de Lagrange de l'exercice 31.

1. Justifier que $r(G)$ est bien défini, et que $r(G) = 0$ si et seulement si $G = \{e\}$. Montrer que $r(\mathbb{U}_n) = 1$ pour $n \geqslant 2$, puis que $r(\mathfrak{S}_3) = 2$, avec les notations de l'exercice 33.

2. Soit H un sous-groupe de G distinct de G, et $x \in G \setminus H$. Montrer que le sous-groupe $K = \langle H \cup \{x\} \rangle$ a au moins $2\,\mathrm{card}(H)$ éléments.

3. En déduire que $2^{r(G)} \leqslant \text{card}(G)$ pour tout groupe fini G. On construira, tant que c'est possible, une suite de sous-groupes $H_0 = \{e\}$, H_1, H_2, ... obtenus en ajoutant à chaque fois un élément.
4. Soit E un ensemble à d éléments, avec $d \geqslant 1$. Dans le groupe $(\mathcal{P}(E), \Delta)$, montrer que le sous-groupe engendré par k parties $A_1, \dots, A_k$ a au plus 2^k éléments. En déduire que $r(\mathcal{P}(E)) = d$: l'inégalité de la question 3 est une égalité.
5. On note $j = \mathrm{e}^{2\mathrm{i}\pi/3}$. Montrer que le groupe produit $\mathbb{U}_2 \times \mathbb{U}_3$ est de rang 1, en calculant les puissances de $(-1, j)$, alors que le groupe produit $\mathbb{U}_2 \times \mathbb{U}_2$ est de rang 2.

EXERCICE 51 ⋆⋆⋆

Un point fixe commun. On note G le groupe des bijections affines $t \mapsto at + b$ de $\mathbb{R}$ dans $\mathbb{R}$, avec $a \neq 0$, étudié à l'exercice 10. Soit Γ un sous-groupe de G tel que tout élément de Γ admette au moins un point fixe.

1. Montrer qu'un élément de Γ distinct de l'identité a un unique point fixe, et qu'il n'est pas une translation.
2. Soit $f : t \mapsto at + b$ et $g : t \mapsto a't + b'$ deux éléments de G. Montrer que le coefficient de t dans $f \circ g \circ f^{-1} \circ g^{-1}$ vaut 1.
3. En déduire que deux éléments quelconques de Γ commutent.
4. Soit f et g deux éléments de Γ distincts de l'identité, et ω le point fixe de f. Montrer que $g(\omega)$ est un point fixe de f, et conclure que les éléments de Γ ont un point fixe commun.

EXERCICE 52 ⋆⋆⋆

Les nombres constructibles à la règle et au compas. Le plan est muni d'un repère orthonormé, et l'on part des deux points $O(0,0)$ et $I(1,0)$. On ajoute des points par étapes : à chaque étape, on peut tracer une droite passant par deux points distincts déjà obtenus, ou un cercle centré en un point déjà obtenu et passant par un autre point déjà obtenu, et l'on ajoute les points d'intersection de deux droites ou cercles distincts ainsi tracés. Un point est dit *constructible* s'il est obtenu au terme d'un nombre fini d'étapes, et une droite ou un cercle est constructible s'il est tracé à partir de points constructibles. On note K l'ensemble des réels qui sont l'abscisse ou l'ordonnée d'un point constructible. On admet les constructions classiques suivantes : si A, B et M sont trois points constructibles, avec $A \neq B$, la perpendiculaire et la parallèle à (AB) passant par M sont des droites constructibles.

1. Montrer que les deux axes du repère sont des droites constructibles. Soit $x \in \mathbb{R}$. Montrer que les points $(x,0)$, $(-x,0)$ et $(0,x)$ sont constructibles dès que l'un d'eux l'est, puis que $x \in K$ si et seulement si le point $(x,0)$ est constructible.
2. Soit x et y deux éléments de K. Montrer que le point (x,y) est constructible, puis que $x+y$ et $x-y$ appartiennent à K.
3. Soit x et y deux éléments non nuls de K, et J le point $(0,1)$. En traçant la parallèle à la droite qui joint I au point $(0,y)$ passant par le point $(x,0)$, montrer que $xy \in K$. De même, en traçant la parallèle à la droite qui joint le point $(x,0)$ au point J passant par I, montrer que $\dfrac{1}{x} \in K$. En déduire que K est un sous-corps de $\mathbb{R}$ qui contient $\mathbb{Q}$.
4. Soit $a > 0$ un élément de K. On note $A(-1,0)$ et $B(a,0)$. Montrer que le cercle de diamètre $[AB]$ est constructible, et qu'il coupe l'axe des ordonnées en un point $H(0,h)$ tel que $h^2 = a$. En déduire que $\sqrt{a} \in K$ pour tout élément positif a de K.
5. On rappelle que $\cos\dfrac{2\pi}{5} = \dfrac{\sqrt{5}-1}{4}$ (exercice 41 de la feuille du chapitre 4). Montrer que les cinq points
$$M_k\Big(\cos\frac{2k\pi}{5}, \sin\frac{2k\pi}{5}\Big), \qquad 0 \leqslant k \leqslant 4,$$
sommets d'un pentagone régulier, sont constructibles.

Réciproquement, les coordonnées d'un point d'intersection s'obtiennent en résolvant une équation du premier ou du second degré : tout élément de K se calcule à partir des rationnels par des additions, des soustractions, des multiplications, des divisions et des extractions de racines carrées. C'est le point de départ de la démonstration, publiée par Pierre-Laurent Wantzel en 1837, de l'impossibilité de la duplication du cube : le nombre $\sqrt[3]{2}$ n'appartient pas à K.

EXERCICE 53 ⋆⋆⋆⋆

Les sous-groupes de $(\mathbb{R},+)$. Soit H un sous-groupe de $(\mathbb{R},+)$, non réduit à $\{0\}$.

1. Montrer que $H\cap]0\,,+\infty[$ est non vide, et qu'il admet une borne inférieure $\alpha\geqslant 0$.
2. On suppose $\alpha>0$.
   (a) Montrer que $\alpha\in H$. On raisonnera par l'absurde, en trouvant deux éléments g et h de H tels que $\alpha<h<g<2\alpha$, puis en considérant $g-h$.
   (b) Soit $x\in H$. En introduisant $k=\lfloor x/\alpha\rfloor$, montrer que $x=k\alpha$. Conclure que $H=\alpha\mathbb{Z}$.
3. On suppose $\alpha=0$. Montrer que, pour tout $\varepsilon>0$, H contient un élément de $]0\,,\varepsilon[$, puis que H rencontre tout intervalle ouvert non vide : H est dense dans $\mathbb{R}$.
4. Soit a et b deux réels non nuls. Montrer que $a\mathbb{Z}+b\mathbb{Z}=\{am+bn\mid(m,n)\in\mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{R}$, et qu'il est dense dans $\mathbb{R}$ si et seulement si $\dfrac{a}{b}$ est irrationnel.
5. On admet que π est irrationnel. Montrer que $\mathbb{Z}+2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$, puis que l'ensemble $\{\cos n\mid n\in\mathbb{N}\}$ est dense dans $[-1\,,1]$.

Le chapitre 12 utilisera le même raisonnement pour décrire les sous-groupes de $\mathbb{Z}$: ce sont les $n\mathbb{Z}$, et l'on en tirera le PGCD.

Les six derniers exercices sont des problèmes à traiter en autonomie : l'énoncé fixe le but, et c'est à vous de trouver le chemin. Pour une partie finie X, on note $|X|=\mathrm{card}(X)$ son nombre d'éléments.

EXERCICE 54 ⋆⋆⋆⋆

Soit G un groupe qui possède un nombre fini de sous-groupes. Montrer que G est fini.

EXERCICE 55 ⋆⋆⋆⋆

Soit A et B deux parties d'un groupe fini G. On suppose $|A|+|B|>|G|$.

1. Montrer que $G=\{ab\mid a\in A,\ b\in B\}$.
2. Montrer que la question précédente devient fausse si on remplace, dans l'hypothèse, l'inégalité stricte par une inégalité large.

EXERCICE 56 ⋆⋆⋆⋆

Soit G un groupe fini non abélien. On note $Z(G)=\{x\in G\mid\forall y\in G,\ xy=yx\}$ son centre.

1. Montrer que $|G|\geqslant 4\,|Z(G)|$.
2. Montrer que la probabilité pour deux éléments de G de commuter est $\leqslant\dfrac{5}{8}$, c'est-à-dire que

$$\frac{|\{(x,y)\in G^2\mid xy=yx\}|}{|G|^2}\leqslant\frac{5}{8}.$$

EXERCICE 57 ⋆⋆⋆⋆

Soit H un sous-groupe strict d'un groupe fini G. On note, pour $x \in G$, $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.

1. Montrer que la relation $\sim$ définie sur G par

$$\forall (x_1, x_2) \in G^2, \qquad x_1 \sim x_2 \iff x_1 H x_1^{-1} = x_2 H x_2^{-1}$$

est une relation d'équivalence, et que son nombre de classes est $\leqslant \dfrac{|G|}{|H|}$.

2. En déduire $\bigcup_{x \in G} xHx^{-1} \neq G$.

EXERCICE 58 ⋆⋆⋆⋆

Soit A un anneau tel que $\forall (x, y) \in A^2$, $xy = \pm yx$. Montrer que A est commutatif.

EXERCICE 59 ⋆⋆⋆⋆

Soit $\mathbb{K}$ un corps. Montrer que les groupes $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \cdot)$ ne sont pas isomorphes, où $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.