TD 11
Structures algébriques

1 Exercices corrigés en classe

Exercice 1. *Sous-groupes de* $\mathbb{R}$. Soit H un sous-groupe de $(\mathbb{R},+)$, $H \neq \{0\}$. Soit $a = \inf(H \cap \mathbb{R}_+^*)$.

1. Justifier l'existence de a.

Correction. Comme H est non trivial, il possède un élément non nul, x_0. Donc x_0 ou $-x_0$ est strictement positive, donc $H \cap \mathbb{R}_+^*$ est non vide. Minoré par 0, il possède une borne inférieure a.

2. Montrer que si $a = 0$, alors H est dense dans $\mathbb{R}$.

Correction. Soit x dans $\mathbb{R}$, $\varepsilon > 0$. Par définition de l'inf, on dispose de $h \in H$ tel que $0 < h < \varepsilon$. Mais alors,

$$\left\lfloor \frac{x}{h} \right\rfloor \leqslant \frac{x}{h} \leqslant \left\lfloor \frac{x}{h} \right\rfloor + 1,$$

donc

$$h\left\lfloor \frac{x}{h} \right\rfloor \leqslant x \leqslant h\left(\left\lfloor \frac{x}{h} \right\rfloor + 1\right),$$

donc, en particulier, $0 \leqslant x - h\left\lfloor \frac{x}{h} \right\rfloor \leqslant \varepsilon$, et $h\left\lfloor \frac{x}{h} \right\rfloor \in H$, donc H est dense dans $\mathbb{R}$.

3. Montrer que si $a > 0$, alors $H = a\mathbb{Z} = \{ka, k \in \mathbb{Z}\}$.

Correction. Si $a > 0$, montrons que $a \in H$. Si ce n'était pas le cas, on disposerait de x, y dans H^2 tels que $a < x < y < a + \frac{a}{2}$ (définition de la borne inférieure). Mais alors $y - x \in H$ et $0 < y - x < \frac{a}{2}$, contredit le fait que $a = \inf H \cap \mathbb{R}_+^*$.
Donc $a \in H$.
Ensuite, par récurrence immédiate et stabilité par $x \mapsto -x$, $a\mathbb{Z} \subset H$.
Enfin, si $x \in H$, on écrit $x = a\frac{x}{a} = a\left(\left\lfloor \frac{x}{a} \right\rfloor + \left\{\frac{x}{a}\right\}\right)$. Comme $a\left\lfloor \frac{x}{a} \right\rfloor \in H$, $a\left\{\frac{x}{a}\right\} \in H$. Mais $0 \leqslant \left\{\frac{x}{a}\right\} < 1$ donc

$$0 \leqslant a\left\{\frac{x}{a}\right\} < a.$$

Si $\left\{\frac{x}{a}\right\} \neq 0$, alors on aurait un élément de $H \cap \mathbb{R}_+^*$ strictement inférieur à a, absurde. Donc $\left\{\frac{x}{a}\right\} = 0$, donc $x = a\left\lfloor \frac{x}{a} \right\rfloor$. Donc $x \in a\mathbb{Z}$.
D'où l'inclusion réciproque et l'égalité.

Application Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Un réel T est appelé *période* de f si

$$\forall x \in \mathbb{R},\ f(x+T) = f(x).$$

4. Montrer que l'ensemble des périodes de f est un sous-groupe de $(\mathbb{R}, +)$.
5. Soit f une fonction continue admettant 3 et $\sqrt{2}$ comme périodes. Montrer que f est constante.

Exercice 2. *Quelques questions indépendantes sur les morphismes de groupes*. Soit $(G, *)$ un groupe.

1. À quelle condition $x \mapsto x^{-1}$ est-il un morphisme de groupes ?
2. À quelle condition $x \mapsto x^2$ est-il un morphisme de groupes ?
3. Démontrer que pour tout a dans G, $x \mapsto a * x * a^{-1}$ est un automorphisme de G. *Les automorphismes de ce type sont appelés automorphismes intérieurs de G.* À quelle condition cet automorphisme est-il l'identité ?

Exercice 3. ●○○ Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}$$

Décomposer σ en produits de cycles à supports disjoints, en produit de transpositions, la signature de σ, et calculer σ^{100}. Faire de même avec ρ.

Correction. On remarque que $\sigma = (1\ 3\ 4\ 6) \circ (2\ 5) = \tau_{13}\tau_{34}\tau_{46}\tau_{25}$. Alors $\varepsilon(\sigma) = 1$. De plus on remarque que $\sigma^4 = \mathrm{Id}$ (et que les puissances plus petites ne donnent pas l'identité). On en déduit que $\sigma^{100} = (\sigma^4)^{25} = \mathrm{Id}$.
De même, $\rho = (1\ 4\ 7\ 8) \circ (2\ 6\ 5) \circ (3\ 9) = \tau_{14}\tau_{47}\tau_{78}\tau_{26}\tau_{65}\tau_{39}$, donc $\varepsilon(\rho) = 1$ et $\rho^{12} = \mathrm{Id}$. Donc $\rho^{100} = \rho^{8\times 12+4}$ donc $\rho^{100} = \rho^4 = (2\ 6\ 5)$.

Exercice 4. ●●○ Soit $n \geqslant 3$. Soient $a \neq b \in \{1, \dots n\}$ et soit $\sigma \in S_n$. Déterminer $\sigma \circ (a\ b) \circ \sigma^{-1}$. Généraliser en remplaçant $(a\ b)$ par un cycle quelconque, puis par une permutation quelconque.

Correction. On montre que $\rho = \sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$.
Soit k dans $[\![1, n]\!]$.

- Si $\sigma^{-1}(k) \notin \{a, b\}$, alors $(a\ b) \circ \sigma^{-1}(k) = \sigma^{-1}(k)$, donc $\rho(k) = \sigma \circ \sigma^{-1}(k) = k$.
- Si $\sigma^{-1}(k) = a$, i.e. $k = \sigma(a)$, alors $(a\ b) \circ \sigma^{-1}(k) = (a\ b)(a) = b$, donc $\rho(k) = \sigma(b)$, i.e. $\rho(\sigma(a)) = \sigma(b)$.
- De même, si $k = \sigma(b)$, alors $\rho(k) = \sigma(a)$.

Donc ρ est la transposition qui échange $\sigma(a)$ et $\sigma(b)$.

Exercice 5. *Quelques sous-anneaux de $\mathbb{C}$.* ●○○

1. Montrer que l'ensemble des entiers de Gauss $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Correction. (a) Déjà $\mathbb{Z}[i] \neq \emptyset$ car $1 = 1 + 0.i$ est dans $\mathbb{Z}[i]$.
(b) Ensuite, si x et y sont dans $\mathbb{Z}[i]$, alors on dispose de $(a, b, c, d) \in \mathbb{Z}^4$ tels que $x = z + ib$ et $y = c + id$. Alors
i. $x - y = (a - c) + i(b - d)$

ii. $x \times y = (a+ib)(c+id) = (ac-bd)+i(bc+ad) \in \mathbb{Z}[i]$.

Donc $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

---

2. Montrer que l'ensemble $\mathbb{Z}[j] = \{a+jb, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Correction. (a) Déjà $\mathbb{Z}[j] \neq \emptyset$ car $1 = 1 + 0.j$ est dans $\mathbb{Z}[j]$.

(b) Ensuite, si x et y sont dans $\mathbb{Z}[j]$, alors on dispose de $(a,b,c,d) \in \mathbb{Z}^4$ tels que $x = z+jb$ et $y = c+jd$. Alors

i. $x - y = (a-c) + j(b-d)$

ii. $x \times y = (a+jb)(c+jd) = ac + j(bc+ad) + j^2bd$. Mais $j^2 + j + 1 = 0$ donc $j^2 = -1 - j$, donc

$$x \times y = ac + j(bc+ad) + (-1-j)bd = (ac-bd) + j(bc+ad-bd) \in \mathbb{Z}[j].$$

Donc $\mathbb{Z}[j]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Exercice 6. *Éléments nilpotents d'un anneau : utile pour les chapitres de matrices*. Soit $(A, +, \times)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe n dans $\mathbb{N}$ tel que $x^n = 0_A$.

1. Si $A = \mathscr{M}_2(\mathbb{R})$, l'ensemble des matrices carrées de taille 2×2 à coefficients dans $\mathbb{R}$, donner un élément nilpotent de A.

On revient au cas général.

1. Démontrer qu'un élément nilpotent n'est pas inversible.

2. Démontrer que si x et y sont deux éléments nilpotents tels que $x \times y = y \times x$, alors $x \times y$ et $x + y$ sont nilpotents.

3. Démontrer que si x est un élément nilpotent, alors $1_A - x$ est inversible.

Exercice 7. ●●○ Soit a un élément de $\mathbb{Q}$ et α une racine de l'équation $x^2 = a$. Montrer que l'ensemble $\mathbb{Q}[\alpha] = \{q + \alpha r, (q,r) \in \mathbb{Q}^2\}$ muni des lois $+$ et $\times$ est un corps.

Correction. Montrons qu'il s'agit d'un sous-anneau de $\mathbb{R}$, et que chaque élément non nul admet un inverse.

- $\mathbb{Q}[\alpha] \neq \emptyset$ car $0 \in \mathbb{Q}[\alpha]$.
- Si x et y sont dans $\mathbb{Q}[\alpha]$, on dispose de q, r, q', r' quatre rationnels tels que $x = q + \alpha r$ et $y = q' + \alpha r'$.
  - Montrons que $x - y \in \mathbb{Q}[\alpha]$.
  $$x - y = q + \alpha r - (q' + \alpha r') = (q - q') + \alpha(r - r') \in \mathbb{Q}[\alpha].$$
  - Montrons que $xy \in \mathbb{Q}[\alpha]$.
  $$\begin{aligned} xy &= (q + \alpha r)(q' + \alpha r') \\ &= qq' + \alpha r q' + \alpha r' q + \alpha^2 rr' \\ &= (qq' + arr') + \alpha(rq' + r'q). \end{aligned}$$
  Or, $qq' + arr' \in \mathbb{Q}$ et $rq' + r'q \in \mathbb{Q}$, donc $xy \in \mathbb{Q}[\alpha]$.

- Soit enfin x non nul dans $\mathbb{Q}[\alpha]$. Son inverse dans $\mathbb{R}$ est $\frac{1}{x}$ Montrons que $\frac{1}{x} \in \mathbb{Q}[\alpha]$. On dispose de q et r rationnels tels que $x = q + r\alpha$. Alors

$$\frac{1}{x} = \frac{1}{q + r\alpha}$$

Alors soit $\alpha \in \mathbb{Q}$ et c'est gagné, soir $\alpha \notin \mathbb{Q}$ et alors ni $q + r\alpha$, ni $q - r\alpha$ ne sont nuls et

$$\begin{aligned}\frac{1}{x} &= \frac{q - r\alpha}{(q + r\alpha)(q - r\alpha)} \\ &= \frac{q}{q^2 - ar^2} + \alpha \frac{-r}{q^2 - ar^2},\end{aligned}$$

et $\frac{q}{q^2 - ar^2} \in \mathbb{Q}$, $\frac{-r}{q^2 - ar^2} \in \mathbb{Q}$, donc $\frac{1}{x} \in \mathbb{Q}[\alpha]$.

Donc $\mathbb{Q}[\alpha]$ est un corps.

Stratégie pour les autres exercices. Ici, trois stratégies :

- vous avez trouvé le cours trop théorique, et vous voulez vous coller au programme officiel : il faut bien apprendre les définitions, refaire les exemples de cours, et faire les exercices 8, 10, 11, 22, 26.
- vous avez bien compris les définitions, les morphismes : faites les exercices 11, 12, 19, 23, 26, 27.
- vous trouvez ces notions vraiment simples : en plus des exercices précédents, les exercices 16, 21, 20 ! Les exercices 24 et 31 sont aussi de niveaux très solides !

2 Groupes

Exercice 8. *Lois de groupe sur* $\mathbb{R}$. ◐○○

1. Montrer que $\mathbb{R}$ muni de la loi $*$ définie par

$$\forall (x, y) \in \mathbb{R}^2,\ x * y = \sqrt[3]{x^3 + y^3},$$

est un groupe abélien.

Correction. Déjà, $*$ est bien une loi de composition interne, car pour tous x et y réels, $\sqrt[3]{x^3 + y^3}$ est réel.
On remarque aussi qu'elle est commutative : cela nous évitera de faire le double des vérifications pour l'élément neutre et l'inverse.
Ensuite, on montre que $*$ est associative : soit $(x, y, z) \in \mathbb{R}^3$. Alors

$$x * (y * z) = \sqrt[3]{x^3 + (y * x)^3 x} = \sqrt[3]{x^3 + \left(\sqrt[3]{y^3 + z^3}\right)^3} = \sqrt[3]{x^3 + y^3 + z^3} = (x * y) * z,$$

d'où l'associativité.
De plus, 0 est l'élément neutre pour $*$: en effet, pour tout x réel, $x * 0 = \sqrt[3]{x^3 + 0} = \sqrt[3]{x^3} = x$.
Enfin, pour tout x dans $\mathbb{R}$, $x * (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0$, donc x admet un inverse pour $+$.
Donc $(\mathbb{E}, *)$ est bien un groupe.

2. $\mathbb{R}$ muni de la loi $\star$ définie par

$$\forall (x,y) \in \mathbb{R}^2,\ x \star y = \sqrt{x^2+y^2}$$

est-il un groupe ?

Correction. Non ! Cette loi ne munit pas $\mathbb{R}$ d'une structure de groupe, simplement parce que les nombres strictement négatifs n'ont de neutre $\star$! Si $x = -1$, alors pour tout $y \in \mathbb{R}$, $x \star y = \sqrt{(-1)^2+y^2} \geqslant 0$, donc pour tout $y \in \mathbb{R}$, $x \star y \neq x$.

Exercice 9. *Groupe des similitudes.* ●○○
Montrer que l'ensemble des similitudes directes non dégénérées est un groupe pour la loi de composition.

Correction. On considère $(\mathcal{S}, \circ)$ où $\mathcal{S}$ est l'ensemble des similitudes directes. On sait par définition que si $f \in \mathcal{S}$, il existe a et b des complexes tels que f associe à tout point d'affixe z le point M' d'affixe $z' = az + b$. Si f est non dégénérée, $a \neq 0$.

- Montrons que $\circ$ est une loi de composition interne. Soient φ et ψ deux similitudes directes. Alors on dispose de a, b, a', b' quatre complexes, avec $a \neq 0$, $a' \neq 0$, tels que φ associe à tout $M(z)$ le point d'affixe $az+b$ et ψ associe à tout $M(z)$ le point d'affixe $a'z+b$. Alors $\varphi \circ \psi$ associe à $M(z)$ le point d'affixe $a(a'z+b')+b = aa'z + (ab'+b)$, avec $aa' \neq 0$. Donc $\varphi \circ \psi$ est une similitude directe non dégénérée.
- Montrons que $\circ$ est associative (le plus embêtant). Soient φ, ψ, θ trois similitudes, a, a', a'', b, b', b'' les coefficients correspondants et $M(z)$ un point. Alors l'affixe de $(\varphi \circ \psi) \circ \theta(M)$ est

  $$aa'(a''z+b'') + (ab'+b) = aa'a''z + aa'b'' + ab' + b,$$

  et celle de $\varphi \circ (\psi \circ \theta)(M)$ est

  $$a(a'a''z + a'b'' + b') + b = aa'a''z + aa'b'' + ab' + b,$$

  d'où l'associativité.
- L'identité est clairement l'élément neutre pour $\circ$.
- Soit $\varphi \in \mathcal{S}$, a et b ses coefficients. Cherchons un inverse pour φ. Pour ce faire, on cherche a', b' tels que $\forall z, aa'z + (ab'+b) = z$. Posons $a' = \dfrac{1}{a}$ (possible car φ non dégénérée), et $b' = -\dfrac{b}{a}$. Alors si ψ envoie $M(z)$ sur M' d'affixe $a'z+b$, on a bien $\varphi \circ \psi = \psi \circ \varphi = \mathrm{Id}$.

Donc $(\mathcal{S}, \circ)$ est un groupe.

Exercice 10. ◐○○
Montrer que l'ensemble $\{z \in \mathbb{C}^*,\ \exists n \in \mathbb{N}^*, z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Correction. Nommons $\mathcal{U}$ l'ensemble considéré.

- $\mathcal{U}$ n'est pas vide car $1 \in \mathcal{U}$.
- Soient z et z' dans $\mathcal{U}$. Alors on dispose de n et m dans $\mathbb{N}$ tels que $z^n = 1$ et $z'^m = 1$. Alors

$$\left(\frac{z}{z'}\right)^{mn} = \frac{z^{mn}}{z'^{mn}} = \frac{(z^n)^m}{(z'^m)^n} = \frac{1}{1} = 1,$$

  donc $\dfrac{z}{z'} \in \mathcal{U}$.

Donc $\mathcal{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exercice 11. *Sous-groupes classiques d'un groupe.* ●◐○
Cet exercice doit vous paraître redondant : la deuxième question est incluse dans la première, la troisième dans un exercice déjà fait. Dès que vous vous en rendez compte, passez à autre chose.
Soit $(G, \cdot)$ un groupe.

1. Soit A une partie de G. On note $C(A) = \{x \in G,\ \forall a \in A, x \cdot a = a \cdot x\}$ (centralisateur de A). Montrer que $C(A)$ est un sous-groupe de G.

Correction. Utilisons la caractérisation des sous-groupes.

- Déjà $C(A) \neq \emptyset$ car 1_G appartient à $C(A)$.
- Soient ensuite x et y dans $C(A)$. Montrons que $x \cdot y^{-1}$ appartient à $C(A)$.
  Soit $a \in A$.
  Montrons que $y^{-1} \cdot a = a \cdot y^{-1}$. On sait que

$$y.a = a.y$$

  Composons cette égalité à gauche par y^{-1}. On obtient

$$y^{-1}.y.a = y^{-1}.a.y,$$
$$\text{i.e.}\quad a = y^{-1}.a.y$$

  Composons à droite par y^{-1} pour obtenir

$$a.y^{-1} = y^{-1}.a.y.y^{-1} = y^{-1}.a.1_G = y^{-1}.a$$

  D'où l'égalité souhaitée.
  On en déduit donc que

$$x.y^{-1}.a = x.a.y^{-1} = a.x.y^{-1} \text{ car } x \in C(A).$$

  Donc $x.y^{-1} \in C(A)$. D'où le résultat.

---

2. On appelle centre de G l'ensemble $Z(G) = \{x \in G,\ \forall y \in G, x \cdot y = y \cdot x\}$. Montrer que $Z(G)$ est un sous-groupe de G, et même qu'il est distingué dans G, c'est-à-dire que

$$\forall x \in Z(G), \forall y \in G, y \cdot x \cdot y^{-1} \in Z(G).$$

Correction. $Z(G) = C(G)$ donc $Z(G)$ est un sous-groupe de G. Soient x dans $Z(G)$ et y dans $Z(G)$. Alors $yxy^{-1} = xyy^{-1}$ car $y \in G$ et x commute avec y. Donc $yxy^{-1} = x \in Z(G)$. D'où le résultat souhaité !

---

3. On suppose G abélien. On dit qu'un élément x de G est **de torsion** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

Correction. Appelons T l'ensemble des éléments de torsion de G. Alors

- T est non vide car $e \in T$,
- soient x et y dans T. Alors on dispose de n et m dans $\mathbb{N}^*$ tels que $x^n = e$ et $y^m = e$. Alors

$$\begin{aligned}(x * y^{-1})^{nm} &= x^{nm} * (y^{-1})^{nm} \text{ car } G \text{ est abélien} \\ &= (x^n)^m * (y^m)^{-n} \\ &= e^m * e^{-n} = e,\end{aligned}$$

donc $x * y^{-1} \in T$.

Donc T est un sous-groupe de G.

Exercice 12. ●●○ Soit $(G, *)$ un groupe. On note, si A et B sont deux sous-groupes de G, $AB = \{a * b,\ a \in A,\ b \in B\}$. Démontrer que AB est un sous-groupe de G si, et seulement si $AB = BA$.

Correction. $\boxed{\Rightarrow}$ Supposons que AB est un sous-groupe, et montrons que $AB = BA$. Soit x dans AB. Alors $x^{-1} \in AB$. Donc on dispose de a dans A et b dans B tels que $x^{-1} = a * b$. Donc $x = b^{-1} * a^{-1} \in BA$. Donc $AB \subset BA$.
De même, $BA \subset AB$, d'où l'égalité.

$\boxed{\Leftarrow}$ Supposons que $AB = BA$, et montrons que AB est un sous-groupe de G.

— Déjà, $e \in A$, $e \in B$, donc $e * e = e \in AB$.

— Soient ensuite x et y dans AB. Alors on peut écrire $x = a * b$ et $y = a' * b'$ où $(a, a') \in A^2$ et $(b, b') \in B^2$. Mais alors $x * y^{-1} = a * b * b'^{-1} * a'^{-1}$.
Or, $b * b'^{-1} \in B$ (B est un sous-groupe) donc $b * b'^{-1} * a'^{-1} \in BA = AB$. Donc on dispose de a'' et b'' dans A et B tels que $b * b'^{-1} * a'^{-1} = a'' * b''$. Donc $x * y^{-1} = a * a'' * b'' \in AB$.

Donc AB est un sous-groupe de G.

Exercice 13. *Groupe dont tous les éléments sont d'ordre 2.* ●●○ Soit $(G, *)$ un groupe fini tel que pour tout x dans G, $x^2 = e$ (où e désigne le neutre de G).

1. Démontrer que G est abélien.

2. Soit H un sous-groupe strict de G et $x \notin H$. On note $xH = \{x * h,\ h \in H\}$. Démontrer que $H \cup xH$ est un sous-groupe de G. Si H contient p éléments, combien $H \cup xH$ contient-il d'éléments ?

3. ●●● En déduire que le cardinal de G est une puissance de 2.

Exercice 14. ●●◐ Soit E un ensemble de cardinal n.

Correction. Il y a un point de vue qui permet de trivialiser l'exercice : c'est celui des tables ! Une loi de composition interne se décrit entièrement par une table de composition, avec une double entrée : si $a_1, \dots, a_n$ sont les éléments de E, le produit $a_i \star a_j$ se lit avec le coefficient (i, j) de la table

1. (a) Combien peut-on définir de lois de composition internes sur E ?

Correction. Choisir une loi de composition interne, c'est choisir un tableau rempli avec un élément de E dans chaque case, d'où n^{n^2} choix possibles.

(b) Combien sont commutatives ?

Correction. Choisir une loi de composition interne, c'est choisir un tableau rempli avec un élément de E dans chaque case, tel que la case (i, j) et la case (j, i) soient égales, i.e. c'est choisir les éléments du triangle supérieur, d'où $n^{\frac{n(n+1)}{2}}$ choix possibles.

(c) Combien possèdent un élément neutre ?

Correction. Choisir une loi de composition interne avec un élément neutre, c'est choisir un élément a_{i_0} de E tel que pour tout i, $a_{i_0}a_i = a_i a_{i_0} = a_i$. D'où la ligne et la colonne i_0 imposées, d'où $n^{(n-1)^2}$ choix possibles.

2. (a) Combien peut-on définir de relations binaires sur E ?

Correction. Encore une fois, utilisons les tables. Une relation binaire se décrit entièrement par une table de composition, avec une double entrée : si $a_1, \dots, a_n$ sont les éléments de E, on remplit la case (i, j) avec 0 si les éléments ne sont pas en relation, 1 si c'est le cas. On peut donc définir 2^{n^2} relations binaires.

(b) Combien sont réflexives ?

Correction. Une relation réflexive est une relation pour laquelle pour tout x, $s\mathcal{R}x$. Elle se code en imposant la diagonale à 1. D'où 2^{n^2-n} possibilités.

(c) Combien sont symétriques ?

Correction. Une relation symétrique revient à prendre une table symétrique, d'où $2^{\frac{n(n+1)}{2}}$ possibilités.

Exercice 15. *Relation de conjugaison.* ●◐○ Soit G un groupe. On définit la relation $\sim$ sur G par

$$\forall (x,y) \in G,\ (x \sim y) \Leftrightarrow (\exists g \in G, x = gyg^{-1}).$$

Montrer que $\sim$ est une relation d'équivalence sur G.
Lorsque G est abélien, quelles sont les classes de conjugaison ?

Correction. Montrons que la relation $\sim$ vérifie les trois hypothèses définissant une relation d'équivalence.

- $\sim$ est réflexive.
  Soit $x \in G$. Alors $x = 1_G x 1_G^{-1}$, donc $x \sim x$.
- $\sim$ est symétrique.
  Soient (x,y) tels que $x \sim y$. Alors on dispose de g dans G tel que $x = gyg^{-1}$. Alors $y = g^{-1}xg = g^{-1}x(g^{-1})^{-1}$, donc $y \sim x$.
- $\sim$ est transitive.
  Soient (x,y,z) tels que $x \sim y$ et $y \sim z$. Alors on dispose de g et h dans G tels que

  $$x = gyg^{-1} \text{ et } y = hzh^{-1}.$$

  Alors

  $$x = g(hzh^{-1})g^{-1} = (gh)z(h^{-1}g^{-1}) = (gh)z(gh)^{-1}.$$

  Donc $x \sim z$. Donc $\sim$ est transitive.

$\sim$ est donc une relation d'équivalence. Lorsque G est abélien, $\forall (g,y) \in G^2, gyg^{-1} = y$, donc les classes d'équivalence sont des points.

Exercice 16. ●●●

1. Déterminer tous les sous-groupes finis de $(\mathbb{C}^*, \times)$.

Correction. (remarque : cet exercice se simplifie encore avec le théorème de Lagrange, qui dit que le cardinal d'un sous-groupe divise le cardinal du groupe).
Soit G un tel groupe, n son cardinal, $a_1, \dots, a_n$ ses éléments. Déjà tous ses éléments sont de module 1 : en effet si on avait $a \in G$ de module différent de 1, la suite $(|a|^k)_{k\in\mathbb{N}}$ tendrait soit vers 0, soit vers $+\infty$, et G contiendrait une infinité d'éléments, ce qui est absurde.
Soit a dans G. Alors l'ensemble $\{a^k, k \in \mathbb{N}\}$ est inclus dans G, donc fini, donc il existe k_0 et k_1 dans $\mathbb{N}$ tel que $a^{k_0} = a^{k_1}$ (principe des tiroirs). Donc il existe ℓ tel que $a^\ell = 1$. Donc pour tout k il existe ℓ_k tel que $a_k^{\ell_k} = 1$.
Donc en posant $L = \text{ppcm}(\ell_1, \dots, \ell_k)$, on a pour tout k $a_k^L = 1$, donc G est un sous-groupe de $\mathbb{U}_L$.
Notre but est donc de démontrer qu'en fait, G est $\mathbb{U}_n$.
Pour cela, on utilise le fait que

$$\varphi : \left| \begin{array}{l} \mathbb{Z} \to \mathbb{U}_L \\ m \mapsto e^{\frac{2im\pi}{L}} \end{array} \right.$$

est un morphisme. Donc $\varphi^{-1}(G)$ est un sous-groupe de $\mathbb{Z}$. Donc, par le cours, il est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}^*$. Donc G est engendré par un seul élément, de la forme $e^{\frac{2i\alpha\pi}{L}}$. Or, si $M = \dfrac{L}{a \wedge L}$ et $b = \dfrac{a}{a \wedge L}$, G est engendré par $e^{\frac{2i\pi a}{M}}$, où $a \wedge M = 1$, i.e. $G = \mathbb{U}_M$ (on a vu dans le cours que si $a \wedge M = 1$, alors $e^{\frac{2i\alpha\pi}{M}}$ engendrait $\mathbb{U}_M$). Comme $\text{Card}(G) = n$, on en déduit que $G = \mathbb{U}_n$.

Soit A une partie de $\mathbb{C}$. On dit que A est compacte si de toute suite d'éléments à valeurs dans A, on peut extraire une sous-suite de A qui converge **DANS** A.

2. Les parties suivantes de $\mathbb{C}$ sont-elles compactes : $\mathbb{R}$, $\{z \in \mathbb{C},\ |z| \leqslant 1\}$, $\{z \in \mathbb{C},\ |z| < 1\}$, $\{a + ib,\ (a,b) \in \mathbb{Q}^2\}$?

Correction.
- $\mathbb{R}$ n'est pas compacte car $(n)_{n\in\mathbb{N}}$ est une suite d'éléments à valeurs dans $\mathbb{R}$ dont aucune sous-suite ne converge.
- $A = \{z \in \mathbb{C},\ |z| \leqslant 1\}$ est compact, car si $(u_n) \in A^{\mathbb{N}}$, alors (u_n) est bornée donc d'après le théorème de BW, on dispose de φ extractrice telle que $(u_{\varphi}(n))_{n\in\mathbb{N}}$ converge vers $\ell \in \mathbb{C}$. Mais $\forall n,\ |u_n| \leqslant 1$ donc $|\ell| \leqslant 1$, donc $\ell \in A$.
- $B = \{z \in \mathbb{C},\ |z| < 1\}$ n'est pas compacte : si pour tout n, $u_n = 1 - \dfrac{1}{n}$, alors $(u_n) \in B^{\mathbb{N}}$ et toute suite extraite de (u_n) tend vers $1 \notin B$.
- $\mathbb{Q}[i] = \{a + ib,\ (a,b) \in \mathbb{Q}^2\}$ n'est pas compacte. Si $x \in \mathbb{R} \setminus \mathbb{Q}$, on dispose de (u_n) suite de rationnels convergeant vers x. Donc $(u_n) \in \mathbb{Q} \subset \mathbb{Q}[i]$ mais toute suite extraite de (u_n) tend vers $x \notin \mathbb{Q}[i]$.

---

3. ●●● Déterminer tous les sous-groupes compacts de $(\mathbb{C}^*, \times)$.

Correction. Déjà $\mathbb{U}$ et les $\mathbb{U}_n$ sont clairement tous compacts. (le vérifier, mais ce n'est pas compliqué !).
Ensuite, si H est un sous-groupe compact de $(\mathbb{C}^*, \times)$, alors par le même argument que précédemment, on aurait une suite (u_n) dont la suite des modules tendrait vers $+\infty$, et donc H ne serait pas compact (toute suite extraite de (u_n) aurait sa suite des modules tendant vers $+\infty$ donc ne pourrait pas converger.
Donc $H \subset \mathbb{U}$.
C'est là la grosse difficulté !
Tous les éléments de H sont de la forme $e^{i\theta}$. Soit $\varphi : \left|\begin{array}{l}\mathbb{R} \to \mathbb{U} \\ \theta \mapsto e^{i\theta}\end{array}\right.$ φ est clairement un morphisme surjectif. Alors $A = \varphi^{-1}(H)$ est un sous-groupe de $\mathbb{R}$, donc, soit de la forme $a\mathbb{Z}$, soit dense :

(a) si A est dense dans $\mathbb{R}$, alors
- ou bien $A = \mathbb{R}$, donc $H = \varphi(\mathbb{R}) = \mathbb{U}$.
- ou bien $A \neq \mathbb{R}$. Alors on dispose de $x \in \mathbb{R}$ tel que $x \notin A$. Donc $\varphi(x) \notin H$. Mais on dispose de $(u_n) \in A^{\mathbb{N}}$ tel que $u_n \to x$. Donc, par continuité de l'exponentielle complexe, $\varphi(u_n) \to \varphi(x) \notin \mathbb{U}$, alors que pour tout n, $\varphi(u_n) \in H$. Donc H n'est pas compact !

(b) sinon , $A = a\mathbb{Z}$ avec $a \in \mathbb{R}$.

- si $\frac{a}{2\pi} \in \mathbb{Q}$, alors écrivons $a = 2\pi\frac{p}{q}$. Alors pour tout x dans A, $qx \in 2\pi\mathbb{Z}$ donc $\varphi(qx) = 1$, i.e. $\varphi(x)^q = 1$, i.e. $H \subset \mathbb{U}_q$. Donc H est un sous-groupe fini de $\mathbb{C}$ et on est ramenés à la question précédente !
- sinon, $\frac{a}{2\pi} \notin \mathbb{Q}$, donc si l'on regarde le sous-groupe $a\mathbb{Z} + 2\pi\mathbb{Z}$, c'est un sous-groupe de $\mathbb{R}$ qui ne peut pas s'écrire comme un $b\mathbb{Z}$ (sinon on aurait m tel que $a = bm$ et n tel que $2\pi = bn$, i.e. $\frac{a}{2\pi} \in \mathbb{Q}$, absurde). Donc ce sous-groupe est dense ! Soit alors $y \notin H$, et x un antécédent de y par φ. Par densité de $a\mathbb{Z} + 2\pi\mathbb{Z}$, on dispose de $(u_n) \in A^{\mathbb{N}}$ et $(v_n) \in 2\pi\mathbb{Z}^{\mathbb{N}}$ tels que $u_n + v_n \to x$. Donc $\varphi(u_n + v_n) \to y$, mais $\varphi(u_n + v_n) = e^{iu_n}e^{iv_n} = e^{iu_n}$ car $v_n \in 2\pi\mathbb{Z}$. Donc $\varphi(u_n) \in H$ pour tout n et $\varphi(u_n) \to y \notin H$, i.e. H n'est pas compact !

Finalement, les seuls sous-groupes compacts de $\mathbb{C}$ sont $\mathbb{U}$ et les $\mathbb{U}_n$ avec $n \in \mathbb{N}$.

---

3 Morphismes, parties génératrices

Exercice 17. *Morphismes sur $\mathbb{Z}$, sur $\mathbb{Q}$.* ●●○

1. Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$. Préciser, à chaque fois, le noyau et l'image de ce morphisme.

Correction. On sait que $\mathbb{Z}$ est engendré par 1 : $\forall n \in \mathbb{Z},\ n = n.1$. Si φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$, on en déduit alors que pour tout n dans $\mathbb{Z}$, $\varphi(n) = n\varphi(1)$. Donc :

- si $\varphi(1) = 0$, alors $\ker(\varphi) = \mathbb{Z}$ et $\mathrm{Im}(\varphi) = \{0\}$,
- sinon, φ est injectif et $\mathrm{Im}(\varphi) = \varphi(1)\mathbb{Z}$.

---

2. Quels sont les automorphismes de groupe de $(\mathbb{Z}, +)$?

Correction. Les automorphismes de $(\mathbb{Z}, +)$ sont les morphismes bijectifs de $(\mathbb{Z}, +)$. Étant donnée l'image d'un morphisme de $(\mathbb{Z}, +)$, les seuls automorphismes sont $\pm\mathrm{Id}_{\mathbb{Z}}$.

---

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

Correction. Il n'y en a pas beaucoup... Le morphisme nul fonctionne, montrons que c'est le seul. Supposons par l'absurde qu'il existe φ un morphisme non nul de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. Notons $a = \varphi(1)$. Sans perte de généralité, on peut supposer $a > 0$.
Posons $x = \frac{1}{a+1}$. Alors $\varphi(x) \in \mathbb{Z}$ et $\varphi(1) = \varphi((a+1)x) = (a+1)\varphi(x)$.
Mais $\varphi(x) \in \mathbb{Z}$ et, comme $\varphi(1) > 0$, $\varphi(x) > 0$. Donc $\varphi(x) \geqslant 1$, donc

$$\varphi(1) = (a+1)\varphi(x) \geqslant a + 1,$$

absurde car $\varphi(1) = a$. Donc $\varphi(1) = 0$ et φ est le morphisme nul.

Exercice 18. ●●○ On munit $\mathbb{Z}^2$ de la loi $+$ (addition coordonnée par coordonnée). On considère un morphisme φ de $(\mathbb{Z},+)$ dans $(\mathbb{Z}^2,+)$.

1. Démontrer que pour tout k dans $\mathbb{Z}$, $\varphi(k)=k\varphi(1)$.
2. Démontrer que φ ne peut pas être un isomorphisme.

Exercice 19. ●●◐ Un **isomorphisme** de groupes est un morphisme de groupes bijectif. Deux groupes sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre.
Démontrer que $(\mathbb{Q},+)$ et $(\mathbb{Q}^*,\times)$ ne sont pas isomorphes.

Correction. Supposons que $(\mathbb{Q},+)$ et $(\mathbb{Q}^*,\times)$ soient isomorphes, soit $\varphi:(\mathbb{Q},+)\to(\mathbb{Q}^*,\times)$ un isomorphisme. Soit x un antécédent de 2 par φ. Notons $y=\frac{x}{2}$. Alors $\varphi(2y)=\varphi(y)^2$, donc $\varphi(x)=\varphi(y)^2$, i.e. $2=\varphi(y)^2$, avec $\varphi(y)\in Q$. Donc $\varphi(y)=\pm\sqrt{2}$, donc $\pm\sqrt{2}$ serait rationnel, absurde !
Donc $(\mathbb{Q},+)$ et $(\mathbb{Q}^*,\times)$ ne sont pas isomorphes.

Exercice 20. *Nombre de morphismes d'un groupe.* ●●● Soit $(G,\cdot)$ un groupe fini à n éléments.

1. Soit H une partie génératrice de G à p éléments. Montrer qu'il y a au plus n^p morphismes de G.

Correction. Écrivons $H=\{h_1,\dots,h_p\}$. Alors pour tout x de G, on dispose de $s\in\mathbb{N}$, $(\alpha_1,\dots,\alpha_s)\in H^s$, $(\varepsilon_1,\dots,\varepsilon_s)\in\{-1,1\}^s$ tels que

$$x=\alpha_1^{\varepsilon_1}\cdot\dots\cdot\alpha_s^{\varepsilon_s}.$$

Si φ est un morphisme de G, alors

$$\varphi(x)=\varphi(\alpha_1)^{\varepsilon_1}\cdot\dots\cdot\varphi(\alpha_s)^{\varepsilon_s}.$$

Donc φ est **entièrement déterminé par ses images des éléments de H.**
Or, pour chaque élément de H, il y a au plus n images possibles. Comme il y a p éléments dans H, il y a au plus n^p choix d'automorphismes possibles.

2. Démontrer que G admet une partie génératrice qui possède moins de $\lceil\log_2(n)\rceil$ éléments, où $\lceil\cdot\rceil$ désigne la partie entière supérieure.

Correction. Soit x_1 dans G tel que $x_1\neq e$ (où e est le neutre de G). Considérons $H_1=\langle x_1\rangle$. Alors H_1 a au moins 2 éléments.
Si $H_1\neq G$, soit $x_2\notin H_1$. Alors si l'on définit $x_2H_1=\{x_2y,\ y\in H_1\}$, on montre facilement que $x_2H_1\cap H_1=\emptyset$ (sinon on disposerait de y et y' dans H_1 tels que $y=x_2y'$ donc $x_2=y\cdot y'^{-1}$ serait dans H_1). Donc, comme $\langle x_1,x_2\rangle$ contient H_1 et x_2H_1, donc il possède au moins 4 éléments.
On poursuit ainsi, en prenant $x_3\notin\langle x_1,x_2\rangle$, etc. jusqu'à arriver à p tel que $H_p=\langle x_1,\dots,x_p\rangle$

soit égal à G. Alors $H_p = G$ et H_p possède au moins 2^p éléments.
Or, le plus petit q tel que $n \leqslant 2^p$, vérifie

$$q_0 - 1 < \log_2(n) \leqslant q_0,$$

i.e. $q_0 = \lceil \log_2(n) \rceil$. Mais comme H_p possède **au moins** 2^p éléments, cela signifie que $p \leqslant q_0$, i.e. $p \leqslant \lceil \log_2(n) \rceil$.

---

3. En déduire que G possède au plus $n^{\lceil \log_2(n) \rceil}$ morphismes.

Correction. On a vu en question précédente que G possédait une partie génératrice d'au plus $\lceil \log_2(n) \rceil$ éléments. Donc, par la première question, il admet au plus

$$n^{\lceil \log_2(n) \rceil} \text{ morphismes,}$$

ce qui était exactement le résultat à démontrer !

Exercice 21. ●●● Soit G un groupe abélien de cardinal supérieur ou égal à 2. Un élément μ de G est dit *mou* si pour toute partie H génératrice de G, $H \setminus \{\mu\}$ est génératrice de G. On note M l'ensemble des éléments mous de G.

1. Démontrer que M est un sous-groupe de G. On l'appelle sous-groupe de Frattini de G.

Correction. **Notons $*$ la loi de G et e son neutre.** Déjà e est dans M. En effet, si H est une partie génératrice de G, alors H n'est pas réduite au neutre (sinon elle ne pourrait pas engendrer tout G). Donc on dispose de $x \in H$ tel que $x \neq e$. Donc $\langle H \setminus \{e\} \rangle$ contient x, donc contient $x * x^{-1} = e$. Donc $\langle H \setminus \{e\} \rangle$ contient H, donc e est mou.
Ensuite, soient x et y dans M.
Soit H génératrice de G, et posons $K = H \setminus \{x * y^{-1}\}$. Alors, comme $\langle K, x * y^{-1} \rangle = \langle H \rangle = G$, $\langle K, x * y^{-1} \rangle = \langle K, x * y^{-1}, x, y \rangle$. Mais $x * y^{-1}$ est engendré par x et y, donc

$$\langle K, x * y^{-1} \rangle = \langle K, x * y^{-1}, x, y \rangle = \langle K, x, y \rangle = \langle K, x \rangle = \langle K \rangle ,$$

les deux dernières égalités venant du fait que y, puis x sont mous.

---

2. Dans cette question, $G = (\mathbb{Z}, +)$. Montrer que l'ensemble des éléments mous de G est $\{0\}$.

Correction. On montre que seul 0 est mou dans $\mathbb{Z}$. Soit en effet n dans $\mathbb{Z}^*$. Alors on remarque très facilement que $\langle n, n+1 \rangle = \mathbb{Z}$, pour la simple et bonne raison que $n + 1 - n = 1$, donc $\langle n, n+1 \rangle$ contient 1, donc contient le sous-groupe engendré par 1, c'est-à-dire $\mathbb{Z}$.

---

3. Dans cette question, $G = (\mathbb{Q}, +)$. On va montrer que tout rationnel est mou. Soit $r = \dfrac{p}{q}$ dans $\mathbb{Q}$ et H une partie génératrice de $\mathbb{Q}$, $K = H \setminus \{r\}$.

(a) Si $r \notin H$, conclure immédiatement que K est génératrice.

Correction. C'est évident car $K = H$.

On suppose alors que $r \in H$.

(b) Démontrer que $H \setminus \{r\}$ n'est pas vide.

Correction. Sinon toute fraction serait multiple de $\frac{p}{q}$, absurde !

(c) Posons K le sous-groupe engendré par $H \setminus \{r\}$. Soit $A = qK = \{qx, x \in K\}$

i. Démontrer qu'il existe $d \in \mathbb{N}^*$ tel que $A \cap \mathbb{Z} = d\mathbb{Z}$.

Correction. Déjà A est un sous-groupe de $\mathbb{Q}$ et $A \cap \mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$ contenu dans $\mathbb{Z}$, donc c'est un sous-groupe de $\mathbb{Z}$. Donc on dispose de d dans $\mathbb{N}^*$ tel que $A \cap \mathbb{Z} = d\mathbb{Z}$.

ii. Démontrer qu'il existe $k \in \mathbb{N}$, $u \in \mathbb{Z}$, $(n_1, \dots, n_k) \in \mathbb{Z}^k$, $(r_1, \dots, r_k) \in (H \setminus \{r\})^k$ tels que

$$\frac{1}{qd} = ur + n_1 r_1 + \cdots + n_k r_k,$$

puis démontrer que

$$1 - qdur \in d\mathbb{Z}.$$

Correction. La première égalité vient du fait que H est génératrice de $\mathbb{Q}$. Puis la seconde vient du fait que $qdur = dup \in \mathbb{Z}$ donc $1 - qdur \in \mathbb{Z}$. Mais on a aussi

$$1 - qdur = qd(n_1 r_1 + \cdots + n_k r_k) \in A,$$

donc $1 - qdur \in A \cap \mathbb{Z} = d\mathbb{Z}$.

iii. Démontrer que $d = 1$ et conclure.

Correction. On en déduit que d divise $1 - qdur$ donc d divise 1. Donc $d = 1$. Donc A contient tous les éléments de $\mathbb{Z}$ donc 1, donc on dispose de $s \in H \setminus \{r\}$ tel que $qs = 1$ donc $s = \frac{1}{q}$. Donc $r = ps \in \langle K \rangle$, donc $\langle K \rangle = \langle K \cup \{x\} \rangle$ donc $\langle K \rangle = \langle H \rangle$ donc x est mou.

4 Groupe symétrique

Exercice 22. ●◐○ Soit E un ensemble contenant au moins trois éléments. Montrer que S_E n'est pas commutatif.

Correction. Nommons x, y et z trois éléments distincts de E. Soit φ l'application qui échange x et y et laisse fixes tous les autres éléments. Soit ψ l'application qui échange x et z et laisse fixes tous les autres éléments. Alors

$$\varphi \circ \psi(x) = \varphi(z) = z,$$

et

$$\psi \circ \varphi(x) = \psi(y) = y.$$

Donc $\varphi \circ \psi \neq \psi \circ \varphi$, donc S_E n'est pas commutatif.

Exercice 23. ●●◐

1. Démontrer que le centre (défini comme en 11) de $\mathcal{S}_n$ est trivial (i.e. égal à $\{\mathrm{Id}\}$) pour $n \geqslant 3$). *On pourra utiliser l'exercice 4*

Correction. Soit σ tel que $\forall s \in S_n,\ \sigma \circ s \circ \sigma^{-1} = s$. Alors pour tous a et b de $[\![1, n]\!]$, $(\sigma(a)\ \sigma(b)) = (a, b)$. Donc si $n = 2$, S_n est commutatif, si $n \geqslant 3$, soient a, b, c trois entiers distincts. Alors $(\sigma(a)\ \sigma(b)) = (a, b)$, i.e. $\sigma(a) = a$ ou b, et $(\sigma(a)\ \sigma(c)) = (a, c)$ donc $\sigma(a) = a$ ou c, donc $\sigma(a) = a$, et ce pour tout a, donc $\sigma = \mathrm{Id}$.

2. Démontrer que le centre de $\mathcal{A}_n$ est trivial pour $n \geqslant 4$.

Correction. Soit $n \geqslant 4$, et σ dans le centre de $\mathcal{A}_n$. Soient a, b, c, d quatre entiers distincts. Alors $\sigma \circ (a\ b\ c) \circ \sigma^{-1} = (a\ b\ c)$, et, par le même raisonnement que précédemment, $\sigma \circ (a\ b\ c) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b)\ \sigma(c))$ donc

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

De même,

$$\{\sigma(a), \sigma(b), \sigma(d)\} = \{a, b, d\},$$

et

$$\{\sigma(a), \sigma(c), \sigma(d)\} = \{a, c, d\},$$

donc, en intersectant les trois ensembles, $\sigma(a) = a$. On montre ainsi que pour tout entier x, $\sigma(x) = x$ donc $\sigma = \mathrm{Id}$.
Remarque : si $n = 3$, on remarque que $\mathcal{A}_3 = \{\mathrm{Id}, \rho, \rho^2\}$ avec $\rho = (1\ 2\ 3)$, donc $\mathcal{A}_3$ est cyclique, donc abélien, donc est son propre centre.

Exercice 24. ●●● Vous venez d'obteir ce jeu de taquin dans votre paquet de céréales. Où est l'arnaque ?

4	1	3
5	2	7
8	6	

Correction. À toute position du taquin on associe une permutation de $[\![1,8]\!]$, en identifiant des positions comme $\begin{array}{|c|c|c|}\hline 4&1&3\\\hline 5&2&7\\\hline 8&6&\\\hline\end{array}$ et $\begin{array}{|c|c|c|}\hline 4&1&3\\\hline 5&2&7\\\hline 8&&6\\\hline\end{array}$ (qui correspondent à la permutation $\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&3&5&2&7&8&6\end{pmatrix}$ dans notre cas). Le déplacement d'un carré correspond soit à la permutation Id dans le cas d'un déplacement horizontal, soit à un un 3-cycle lors d'un déplacement vertical. Dans tous les cas, le déplacement d'un carré ne change pas la signature. Or, la signature de $\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&3&5&2&7&8&6\end{pmatrix}$ est -1 car la permutation s'écrire $(1452)\circ(678)$, donc on ne pourra jamais retrouver la position $\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5&6\\\hline 7&8&\\\hline\end{array}$, de signature 1.

Exercice 25. ●●● Soit E un ensemble de cardinal n. On appelle dérangement de E toute permutation de E sans point fixe. On note d_p le nombre de dérangements d'un ensemble à p éléments.

1. Montrer que $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$.

Correction. Soit $S_{n,k}$ l'ensemble des permutations ayant $n-k$ points fixes. Choisir une permutation avec k points fixes, c'est choisir d'abord $n-k$ points fixes, i.e. $\binom{n}{n-k} = \binom{n}{k}$ possibilités, puis choisir une permutation sans point fixe sur les points restants, i.e. d_k possibilités. Donc $|S_{n,k}| = \binom{n}{k} d_k$, donc, comme S_n est la réunion disjointe de tous les $S_{n,k}$, on a $|S_n| = \sum_{k=0}^{n} |S_{n,k}|$, donc $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$.

---

2. Démontrer la formule d'inversion de Pascal : soit f une fonction définie sur $\mathbb{N}$, soit g définie pour tout n par $g(n) = \sum_{k=0}^{n} \binom{n}{k} f(k)$. Montrer que pour tout entier naturel n, $f(n) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} g(k)$.

Correction. Calculons $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}g(k)$:

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}g(k)=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\sum_{j=0}^{k}\binom{k}{j}f(j)=\sum_{k=0}^{n}\sum_{j=0}^{k}(-1)^{n-k}\binom{n}{k}\binom{k}{j}f(j)$$
$$=\sum_{j=0}^{n}\sum_{k=j}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{j}f(j).$$

Or, $\binom{n}{k}\binom{k}{j}=\frac{n!}{k!(n-k)!}\frac{k!}{j!(k-j)!}=\frac{n!}{(n-k)!j!(k-j)!}=\binom{n}{j}\binom{n-j}{n-k}$, d'où

$$\begin{aligned}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}g(k)&=\sum_{j=0}^{n}\sum_{k=j}^{n}(-1)^{n-k}\binom{n}{j}\binom{n-j}{n-k}f(j)\\&=\sum_{j=0}^{n}\binom{n}{j}f(j)\sum_{k=j}^{n}(-1)^{n-k}\binom{n-j}{k-j}\\&=_{\ell=k-j}\sum_{j=0}^{n}\binom{n}{j}f(j)\sum_{\ell=0}^{n-j}(-1)^{n-k}\binom{n-j}{\ell}\\&=\sum_{j=0}^{n}\binom{n}{j}f(j)(1-1)^{n-j}=\sum_{j=0}^{n}\binom{n}{j}f(j)\delta_{nj}=\binom{n}{n}f(n)=f(n),\end{aligned}$$

d'où le résultat demandé.

---

3. En déduire une formule pour d_n.

Correction. On en déduit, par la formule d'inversion, que

$$d_n=\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k!=\sum_{k=0}^{n}(-1)^{n-k}\frac{n!}{(n-k)!}=_{\ell=n-k}n!\sum_{k=0}^{n}\frac{(-1)^{\ell}}{\ell!}.$$

---

4. Quelle est la limite de la proportion $\frac{d_n}{n!}$ des dérangements de E parmi les permutations de E quand n tend vers $+\infty$?

Correction. La proportion de dérangements est alors $\frac{d_n}{n!}$, i.e. $\sum_{k=0}^{n}\frac{(-1)^{\ell}}{\ell!}$, elle converge donc vers $\frac{1}{e}$.

---

5 Anneaux et corps

Exercice 26. *Anneau des dyadiques*. ●●○ On définit le sous-ensemble A de $\mathbb{Q}$ par

$$A = \left\{ \frac{p}{2^n}, p \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

1. Montrer que A est un sous-anneau de $\mathbb{Q}$. Est-il intègre ? Tout élément de A est-il inversible pour $\times$?

Correction. Montrons que A est un sous-anneau de $\mathbb{Q}$.

- A est un sous-groupe de $\mathbb{Q}$
  - $A \neq \emptyset$ car $0 \in A$.
  - Soient x et y deux éléments de A. Alors on dispose de p et q dans $\mathbb{Z}$, de n et m dans $\mathbb{N}$ tels que $x = \frac{p}{2^n}$ et $y = \frac{q}{2^m}$. Alors
$$x - y = \frac{2^m x - 2^n y}{2^{n+m}} \in A.$$
- A est stable par multiplication. Soient x et y deux éléments de A. Alors on dispose de p et q dans $\mathbb{Z}$, de n et m dans $\mathbb{N}$ tels que $x = \frac{p}{2^n}$ et $y = \frac{q}{2^m}$. Alors
$$xy = \frac{pq}{2^{m+n}} \in A.$$

Donc A est un sous-anneau de $\mathbb{Q}$. Il est intègre car $\mathbb{Q}$ est intègre. Cependant il n'est pas inversible pour $\times$: $3 \in A$ mais son inverse dans $\mathbb{Q}$ est $\frac{1}{3}$ qui ne peut pas s'écrire comme $\frac{q}{2^n}$ (si c'était le cas, on aurait $2^n = 3q$, i.e. $v_3(2^n) \geqslant 1$, absurde.

---

2. Déterminer $U(A)$.

Correction. Soit $x = \frac{p}{2^n}$ un élément inversible de A. Alors on dispose de q et m tels que $x \times \frac{q}{2^m} = 1$. Sans perte de généralité, on peut supposer $p \wedge 2^n = 1$ et $q \wedge 2^m = 1$. Alors

$$pq = 2^n 2^m.$$

Donc p et q sont des puissances de 2. Comme $p \wedge 2^n = 1$, on a

- soit $p = 1$ et $n = 0$
- soit $p = 1$ et $n \geqslant 1$, et alors $q = 2^n$ et $m = 0$.
- soit $p = 2^k$ ($k \in \mathbb{N}^*$) et $n = 0$, et alors $q = 1$ et $m = k$.

Finalement, l'ensemble des unités de A est l'ensemble des puissances de 2 (positives ou négatives).

Exercice 27. *Anneaux de Boole*. ●●○ On appelle anneau de Boole tout anneau $(A, +, \times)$ tel que $\forall a \in A, a^2 = a$.

1. Montrer que $\forall a \in A, a + a = 0_A$.

Correction. On calcule $(a+a)^2$ de deux manières différentes. Déjà $(a+a)^2 = a+a$ (propriété d'anneau de Boole). Ensuite, $(a+a)^2 = a^2+a^2+a^2+a^2 = a+a+a+a$, donc $a+a = a+a+a+a$, i.e. $a + a = 0$.

2. En déduire que A est commutatif pour la loi $\times$.

Correction. Soient a et b deux éléments de A. On sait que $(a + b)^2 = a + b$, et $(a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b = a + b + ab + ba$, donc $a + b = a + b + ab + ba$, donc $ab + ba = 0$, donc $ab = -ba = (-b)a = ba$ par la question précédente. Donc A est commutatif pour $\times$.

3. Montrer que si A est fini, son cardinal est nécessairement différent de 3.

Correction. Supposons A de cardinal 3. Alors $A = (0_A, 1_A, x)$, avec $x \neq 0_A$ et $x \neq 1_A$ Intéressons-nous à $x + 1_A$. On a

- soit $x + 1_A = 0_A$, i.e. $x = -1_A = 1_A$, impossible.
- soit $x + 1_A = 1_A$, i.e. $x = 0_A$, impossible.
- soit $x + 1_A = x$, i.e. $1_A = 0_A$, impossible.

Donc A ne peut être de cardinal 3.

4. Montrer que si $\text{Card}(A) > 2$, alors A n'est pas intègre.

Correction. si $\text{Card}(A) > 2$, on dispose de x dans A qui soit différent de 0_A et de 1_A. Alors $x^2 = x$, i.e. $x^2 - x = 0_A$, i.e. $x \times (x - 1_A) = 0_A$, avec $x \neq 0_A$ et $x \neq 1_A$, donc $x - 1_A \neq 0$. Donc A n'est pas intègre.

5. On définit une relation binaire sur A par $x \preceq y$ si, et seulement si $yx = x$. Montrer que $\preceq$ est une relation d'ordre sur A.

Correction. Vérifions les trois hypothèses des relations d'ordre.

- $\preceq$ est réflexive.
  Soit $x \in A$. Alors par définition $x \times x = x$, donc $x \preceq x$.
- $\preceq$ est antisymétrique.
  Soient x et y tels que $x \preceq y$ et $y \preceq x$. Alors $yx = x$ et $xy = y$. Or $\times$ est commutative donc $yx = xy$, donc $x = y$.
- $\preceq$ est transitive.
  Soient x, y et z trois éléments de A tels que $x \preceq y$ et $y \preceq z$. Alors $yx = x$ et $zy = y$. Donc $zx = zyx = yx = x$. Donc $x \preceq z$.

Donc $\preceq$ est une relation d'ordre sur A.

Exercice 28. **1.** ●●○ Déterminer tous les morphismes de corps de $\mathbb{Q}$ dans $\mathbb{Q}$ (indication : il n'y en a pas beaucoup... !)

2. ●●○ Soit f un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$. Démontrer que f est égale à l'identité sur les rationnels, puis que $f(\mathbb{R}_+) \subset \mathbb{R}_+$, puis que f est croissante, et enfin que $f = \mathrm{Id}_{\mathbb{R}}$.

Exercice 29. ●●○ Soit ϕ une racine de l'équation

$$x^2 - x - 1 = 0.$$

Montrer que $\mathbb{Q}[\phi] = \{q + \phi r, (q, r) \in \mathbb{Q}^2\}$ est un corps.

Correction. Montrons qu'il s'agit d'un sous-anneau de $\mathbb{R}$, et que chaque élément non nul admet un inverse.

- $\mathbb{Q}[\phi] \neq \emptyset$ car $0 \in \mathbb{Q}[\phi]$.
- Si x et y sont dans $\mathbb{Q}[\phi]$, on dispose de q, r, q', r' quatre rationnels tels que $x = q + \phi r$ et $y = q' + \phi r'$.
  - Montrons que $x - y \in \mathbb{Q}[\phi]$.
  $$x - y = q + \phi r - (q' + \phi r') = (q - q') + \phi(r - r') \in \mathbb{Q}[\phi].$$
  - Montrons que $xy \in \mathbb{Q}[\phi]$.
  $$\begin{aligned} xy &= (q + \phi r)(q' + \phi r') \\ &= qq' + \phi r q' + \phi r' q + \phi^2 r r' \end{aligned}$$
  Or, $\phi^2 = \phi + 1$, donc
  $$xy = (qq' + rr') + \alpha(rq' + r'q + 1).$$
  Or, $qq' + rr' \in \mathbb{Q}$ et $rq' + r'q + 1 \in \mathbb{Q}$, donc $xy \in \mathbb{Q}[\alpha]$.
- Soit enfin x non nul dans $\mathbb{Q}[\phi]$. Son inverse dans $\mathbb{R}$ est $\frac{1}{x}$ Montrons que $\frac{1}{x} \in \mathbb{Q}[\phi]$. On dispose de q et r rationnels tels que $x = q + r\alpha$. Alors
$$\frac{1}{x} = \frac{1}{q + r\phi}$$
Écrivons $\phi = \frac{1 + \sqrt{5}}{2}$ (le cas $\frac{1 - \sqrt{5}}{2}$ est similaire). Alors
$$\begin{aligned} \frac{1}{x} &= \frac{2}{2q + r + r\sqrt{5}} \\ &= \frac{2}{(2q + r) + \sqrt{5}r} \\ &= \frac{2((2q + r) - \sqrt{5}r)}{(2q + r)^2 - 5r^2} \\ &= \frac{2((2q + r) + r - r - \sqrt{5}r)}{(2q + r)^2 - 5r^2} \\ &= 4\frac{q + r}{(2q + r)^2 - 5r^2} + \phi\frac{-4r}{(2q + r)^2 - 5r^2} \in \mathbb{Q}[\phi]. \end{aligned}$$

Donc $\mathbb{Q}[\phi]$ est un corps.

Exercice 30. *Anneau $\mathbb{Z}(\sqrt{2})$.* ●◐○ - ●●●
On définit $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau commutatif et intègre.

Correction. On l'a montré avec $\mathbb{Q}[\alpha]$ (il s'agit du même type de raisonnement) ! La commutativité et l'intégrité viennent de la commutativité et de l'intégrité de $\mathbb{R}$.

---

2. Soit $x = a + \sqrt{2}b$ un élément de $\mathbb{Z}[\sqrt{2}]$.

(a) Montrer que le couple (a, b) est unique.

Correction. Supposons que $a+\sqrt{2}b = a'+\sqrt{2}b'$. Alors $a-a' = \sqrt{2}(b-b')$ et $a-a' \in \mathbb{Z}$, donc nécessairement $b - b' = 0$. Donc $b = b'$ et il vient $a = a'$. D'où l'unicité.

(b) On pose alors $N(x) = a^2 - 2b^2$. Montrer que pour tous x, y de $\mathbb{Z}[\sqrt{2}]$,

$$N(xy) = N(x)N(y).$$

Correction. Soient x et y dans $\mathbb{Z}[\sqrt{2}]$. On dispose de a, b, α, β entiers tels que $x = a + \sqrt{2}b$ et $y = \alpha + \sqrt{2}\beta$. Donc

$$xy = (a\alpha + 2b\beta) + \sqrt{2}(a\beta + b\alpha).$$

Donc

$$\begin{aligned} N(xy) &= (a\alpha + 2b\beta)^2 - 2(a\beta + b\alpha)^2 \\ &= a^2\alpha^2 + 4ab\alpha\beta + 4b^2\beta^2 - 2a^2\beta^2 - 4ab\alpha\beta - 2b\alpha^2 \\ &= a^2\alpha^2 - 2a^2\beta^2 - 2b^2\alpha^2 + 4b^2\beta^2 \\ &= (a^2 - 2b^2)(\alpha^2 - 2\beta^2) \\ &= N(x)N(y). \end{aligned}$$

---

3. On veut déterminer $U(\mathbb{Z}[\sqrt{2}])$.

(a) Montrer que $x \in U(\mathbb{Z}[\sqrt{2}])$ si, et seulement si $N(x) = 1$ ou $N(x) = -1$.

Correction. Si $x \in U(\mathbb{Z}[\sqrt{2}])$, alors on dispose de $y \in U(\mathbb{Z}[\sqrt{2}])$ tel que $xy = 1$. Donc $N(xy) = 1$, i.e. $N(x)N(y) = 1$, i.e., comme N est toujours entier, $N(x) = 1$ ou $N(x) = -1$. Réciprquement, si $N(x) = 1$, posons $y = a - \sqrt{2}b$. Alors $xy = N(x) = 1$. Si $N(x) = -1$, on pose $y = \sqrt{2}b - a$ et on a le résultat.

(b) Montrer que pour tout entier n de $\mathbb{Z}$, $(1+\sqrt{2})^n$ appartient à $U(\mathbb{Z}[\sqrt{2}])$.

Correction. On montre par récurrence évidente que $N(x^n) = N(x)^n$. Donc $N((1+\sqrt{2})^n) = N(1+\sqrt{2})^n = (1-2)^n = (-1)^n$. D'où le résultat.

4. ●●● Montrer que réciproquement, les inversibles de $\mathbb{Z}[\sqrt{2}]$ sont de la forme $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$.

Correction. Supposons que l'on ait un élément inversible de la forme $a+\sqrt{2}b$ avec a, b positifs (c'est possible, quitte à multiplier par -1 et/ou par le conjugué, et tel que $\min(a,b)$ soit minimal, mais tel que $(a,b) \neq (1,1)$.
Alors $\dfrac{a+\sqrt{2}b}{1+\sqrt{2}} = -(a-2b) - \sqrt{2}(b-a)$. Alors

- si $a \leqslant b$, $\min|a-2b|, |b-a| = b-a$, et, quitte à diviser à nouveau par $1+\sqrt{2}$, on obtient une valeur minimale égale au reste dans la division euclidienne de b par a, absurde !
- on continue ainsi la disjonction de cas en obtenant à chaque fois une contradiction !

Exercice 31. ●●◐ Soit E un ensemble. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

Correction. Déjà, Δ et $\cap$ sont sans difficultés des lois de composition internes. Rappelons que si A et B sont deux ensembles,

$$\mathbb{1}_{A\Delta B} = \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B \text{ et } \mathbb{1}_{A\cap B} = \mathbb{1}_A\mathbb{1}_B.$$

1. $(\mathcal{P}(E), \Delta)$ est un groupe abélien.

- Δ est associative. Soient A, B et C. Montrons que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$ en utilisant les fonctions indicatrices :

$$\begin{aligned}\mathbb{1}_{(A\Delta B)\Delta C} &= \mathbb{1}_{A\Delta B} + \mathbb{1}_C - 2\mathbb{1}_{A\Delta B}\mathbb{1}_C \\ &= \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_C - 2(\mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B)\mathbb{1}_C \\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_A\mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C,\end{aligned}$$

et

$$\begin{aligned}\mathbb{1}_{A\Delta(B\Delta C)} &= \mathbb{1}_A + \mathbb{1}_{B\Delta C} - 2\mathbb{1}_A\mathbb{1}_{B\Delta C} \\ &= \mathbb{1}_A + (\mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C) - 2\mathbb{1}_A(\mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C) \\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_A\mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C,\end{aligned}$$

d'où l'égalité désirée.

- Δ admet un élément neutre, c'est l'ensemble vide. En effet, si $A \in \mathcal{P}(E)$,

$$\mathbb{1}_{A\Delta\emptyset} = \mathbb{1}_A + \mathbb{1}_\emptyset - 2\mathbb{1}_A\mathbb{1}_\emptyset = \mathbb{1}_A + 0 - 2.0 = \mathbb{1}_A.$$

De même, $\mathbb{1}_{\emptyset\Delta A} = \mathbb{1}_A$.

- Tout élément de $\mathcal{P}(E)$ admet lui-même comme inverse pour Δ. En effet, si $A \in \mathcal{P}(E)$,

$$\mathbb{1}_{A\Delta A} = \mathbb{1}_A + \mathbb{1}_A - 2\mathbb{1}_A\mathbb{1}_A = 2\mathbb{1}_A - 2\mathbb{1}_A = 0 = \mathbb{1}_\emptyset.$$

- Enfin, Δ est commutative par commutativité de l'addition et de la multiplication.

2. $\cap$ est associative
3. $\cap$ possède un élément neutre : il s'agit de E !
4. $\cap$ est distributive sur Δ.

Je vous laisse vérifier de la même manière les autres propriétés, il s'agit d'un bon exercice de révision sur les fonctions indicatrices.
Remarque : cet anneau est un anneau de Boole !
