Structures algébriques et arithmétique

Feuille d'exercices #19

Partie A – Groupes et sous-groupes

⋆ **Exercice 1 —** *Transport de structure*

1. Soient E un ensemble, $(G,\bullet)$ un groupe et φ une bijection de G sur E. On définit une loi interne sur E par :
$$\forall x,y\in E,\quad x\star y=\varphi\left(\varphi^{-1}(x)\bullet\varphi^{-1}(y)\right)$$
Montrer que $(E,\star)$ est un groupe.
2. a) Montrer que pour tout $x,y\in\mathbb{R}$, $\operatorname{th}(x+y)=\dfrac{\operatorname{th}(x)+\operatorname{th}(y)}{1+\operatorname{th}(x)\operatorname{th}(y)}$.
b) On pose, pour tous $x,y\in]-1,1[$, $x\oplus y=\dfrac{x+y}{1+xy}$.
Montrer que $(]-1,1[,\oplus)$ est un groupe abélien.

⋆⋆ **Exercice 2 —** *Sous-groupes additifs de* $\mathbb{R}$

1. Donner des exemples de sous-groupes additifs de $\mathbb{R}$.
2. Soit G un sous-groupe de $(\mathbb{R},+)$ tel que $G\neq\{0\}$.
a) Établir l'existence de $\alpha=\inf(G\cap\mathbb{R}_+^*)$.
b) On suppose que $\alpha>0$. Montrer que $\alpha\in G$ puis en déduire que $G=\alpha\mathbb{Z}$.
c) On suppose que $\alpha=0$. Prouver que G est dense dans $\mathbb{R}$. Conclure.
3. a) Soient $a,b\in\mathbb{R}^*$. Montrer que $a\mathbb{Z}+b\mathbb{Z}$ est dense dans $\mathbb{R}$ ssi $\dfrac{a}{b}\notin\mathbb{Q}$.
b) Montrer que $\{\cos(n)\}_{n\in\mathbb{N}}$ est dense dans $[-1,1]$.

⋆ **Exercice 3 —** Pour $n\in\mathbb{N}^*$, on note $\mathrm{GL}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathrm{GL}_n(\mathbb{R})$ à coefficients dans $\mathbb{Z}$ et dont l'inverse est encore à coefficients dans $\mathbb{Z}$.

1. Montrer que $\mathrm{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.
2. Soit $M\in\mathcal{M}_n(\mathbb{Z})$. Montrer que $M\in\mathrm{GL}_n(\mathbb{Z})$ si et seulement si $\det(M)=\pm1$.

⋆ **Exercice 4 —** Montrer que $\dfrac{2}{3}\mathbb{Z}+\dfrac{1}{5}\mathbb{Z}$ est un sous-groupe monogène de $\mathbb{Q}$.

⋆ **Exercice 5 —** Montrer que tout groupe fini d'ordre $p\in\mathbb{P}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

⋆⋆ **Exercice 6 —** Soit G un groupe fini dont tous les éléments sont d'ordre 2 (à l'exception de l'élément neutre), de cardinal supérieur ou égal à 2.

1. Montrer que G est abélien.
2. Montrer que tout groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Préciser ce qu'il en est pour le groupe multiplicatif $((\mathbb{Z}/5\mathbb{Z})^*,\times)$.
3. Montrer qu'il existe $n\in\mathbb{N}^*$ tel que G soit isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

⋆⋆ **Exercice 7 —**

1. Montrer que les groupes $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ et le groupe diédral D_4 (isométries préservant le carré) sont deux à deux non isomorphes.
2. Soient p premier et $\alpha,\alpha_1,\dots,\alpha_r\in\mathbb{N}^*$. Combien existe-t-il d'éléments d'ordre p dans les groupes $\mathbb{Z}/p^\alpha\mathbb{Z}$ et $\left(\mathbb{Z}/p^{\alpha_1}\mathbb{Z}\right)\times\cdots\times\left(\mathbb{Z}/p^{\alpha_r}\mathbb{Z}\right)$?

⋆ **Exercice 8 —** *Produit de deux sous-groupes*
Soient $(G,\cdot)$ et A,B deux sous-groupes de G. On pose $AB=\{ab\mid a\in A,b\in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB=BA$.

⋆ **Exercice 9 —** Montrer que les éléments inversibles de l'anneau $\mathbb{Z}/11\mathbb{Z}$ forment un groupe cyclique, dont on précisera les générateurs.

⋆ **Exercice 10 —** Soit G un groupe. Montrer que xy et yx sont conjugués pour tous $x,y\in G$ et que ces deux éléments ont même ordre.

⋆ **Exercice 11 —** Soient $n\in\mathbb{N}^*$ et $k\in\mathbb{Z}$. On pose $d=k\wedge n$.

1. Déterminer l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe.
3. Décrire l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

⋆ **Exercice 12 —** Montrer que tout sous-groupe de $(\mathbb{U}_n,\times)$ est cyclique.
En déduire que tout sous-groupe d'un groupe cyclique est cyclique.

⋆ **Exercice 13 —** Soient G un groupe cyclique d'ordre n et d un diviseur de n. Montrer que G possède un et un seul sous-groupe d'ordre d.

⋆⋆ **Exercice 14 —** *Ordre du produit de deux éléments*
Soient G un groupe abélien et $a, b \in G$ d'ordres respectifs p et q.

1. Montrer que si $p \wedge q = 1$, alors ab est d'ordre pq.
2. Montrer que si d est un diviseur de p, il existe un élément de G d'ordre d.
3. En déduire qu'il existe un élément d'ordre $p \vee q$.
4. On considère ici $G = \mathrm{GL}_2(\mathbb{R})$, $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $b = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$.
   Que dire de l'ordre de a? de b? de ab? Conclure.

⋆ **Exercice 15 —** Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

⋆ **Exercice 16 —** Soient $a, b \in \mathbb{N} \setminus \{0, 1\}$.
Montrer que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique si et seulement si $a \wedge b = 1$.

⋆⋆ **Exercice 17 —** Pour $m, n \in \mathbb{N}^*$, on considère $f : z \in \mathbb{U}_{mn} \mapsto (z^n, z^m) \in \mathbb{U}_n \times \mathbb{U}_m$.

1. Montrer que f est un morphisme de groupes et trouver un entier $k \in \mathbb{N}^*$ tel que $\mathrm{Ker}(f) = \mathbb{U}_k$.
2. À quelle condition nécessaire et suffisante sur m et n l'application f est-elle un isomorphisme de groupes de $\mathbb{U}_{nm}$ sur $\mathbb{U}_m \times \mathbb{U}_n$?

⋆⋆ **Exercice 18 —**

1. Soit G un groupe monogène. Montrer que les endomorphismes de groupe de G sont exactement les applications $x \mapsto x^k$, k décrivant $\mathbb{Z}$.
2. Décrire les groupes d'automorphismes suivants et préciser un groupe usuel auquel ils sont isomorphes : $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $\mathrm{Aut}(\mathbb{Q})$.

⋆ **Exercice 19 —** *Théorème de Lagrange*
Soient G un groupe fini d'ordre n et H un sous-groupe de G.
On définit alors sur G la relation : $g \mathscr{R} g' \iff g^{-1}g' \in H$.

1. Montrer que $\mathscr{R}$ est une relation d'équivalence.
2. Démontrer que chaque classe d'équivalence a autant d'éléments que H.
   En déduire que l'ordre de H divise celui de G.
3. Que dire de l'intersection de sous-groupes d'ordres premiers entre eux?

⋆⋆ **Exercice 20 —** Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ tel que $G \cap \mathrm{SL}_n(\mathbb{C}) = \{I_n\}$.
Montrer que G est cyclique.

⋆ **Exercice 21 —** Soit f un morphisme d'un groupe $(G, \cdot)$ dans $(\mathbb{C}^*, \times)$ que l'on suppose non constant. Déterminer $\sum_{x \in G} f(x)$.
On introduira g tel que $f(g) \neq 1$ et on calculera $f(gx)$ pour $x \in G$.

⋆⋆ **Exercice 22 —** *Caractérisation des carrés dans $\mathbb{Z}/p\mathbb{Z}$*
Soient p un nombre premier différent de 2 et $x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^*$.

1. a) Montrer que si x est un carré, alors $x^{(p-1)/2} = 1$.
   b) Montrer que -1 est un carré dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ alors $p \equiv 1$ [4].
2. a) Montrer que 1 et -1 sont les seules racines carrées de 1 dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$.
   b) En déduire que l'image du morphisme ϕ défini sur $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ par $\phi(x) = x^2$ est un sous-groupe d'ordre $(p-1)/2$. Conclure.

⋆⋆⋆ **Exercice 23 —** *Groupes de permutations et p-cycles*
On note n un entier naturel supérieur ou égal à 2 et $p \in [\![2, n]\!]$.

1. a) Simplifier $(x_1\ x_2)(x_2\ x_3)\cdots(x_{p-1}\ x_p)$ et vérifier que pour tous $x_1, \ldots, x_p \in [\![1, n]\!]$ et pour toute permutation $\sigma \in \mathfrak{S}_n$,
   $$\sigma \circ (x_1\ x_2\ \cdots\ x_p) \circ \sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_p))$$
   b) En déduire que tout p-cycle de $[\![1, n]\!]$ est un conjugué de $(1\ 2\ \cdots\ p)$.
2. Montrer que si $n \geqslant 3$, seule id commute avec tous les éléments de $\mathfrak{S}_n$.
3. a) Montrer que $\mathfrak{S}_n$ est engendré par les transpositions.
   b) En déduire que $\mathfrak{S}_n$ est engendré par les transpositions $(1\ i)$, pour i décrivant $[\![2, n]\!]$.
4. On pose $G = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = 1\}$. On souhaite montrer que G est un sous-groupe maximal de $\mathfrak{S}_n$, autrement dit que G et $\mathfrak{S}_n$ sont les seuls sous-groupes de $\mathfrak{S}_n$ contenant G. On note H un sous-groupe de $\mathfrak{S}_n$ contenant strictement G. On fixe $\sigma \in H \setminus G$.
   a) Montrer que G est un sous-groupe de $\mathfrak{S}_n$.
   b) Montrer que la transposition $(1\ \sigma(1))$ apparaît dans la décomposition en produits de cycles disjoints du produit $\sigma \circ (\sigma(1)\ \sigma^{-1}(1))$.
   c) En déduire grâce à **3.b)**, que H contient $(1\ \sigma(1))$ puis que $H = \mathfrak{S}_n$.

Partie B – Anneaux, corps et algèbres

⋆ **Exercice 24 —** Soit $A = \left\{ \dfrac{k}{2n+1} \;\middle|\; k \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$.
Montrer que $(A, +, \times)$ est un anneau et préciser ses éléments inversibles.

⋆ **Exercice 25 —** Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$.
Montrer que $\left(\mathbb{Q}[\sqrt{d}], +, \times\right)$ est un corps.

⋆ **Exercice 26 —** On considère l'anneau $(A, +, \times)$ et deux éléments a et b de A.

1. Si ab est un élément nilpotent, montrer que $1 - ab$ est inversible et déterminer $(1-ab)^{-1}$.
2. Si ab et ba sont nilpotents, exprimer $(1-ba)^{-1}$ en fonction de $(1-ab)^{-1}$.
3. On ne suppose plus ab ni ba nilpotents. Montrer que si $1-ab$ est inversible, alors $1-ba$ est également inversible.

⋆⋆ **Exercice 27 —** Soit A un anneau commutatif.
On note $\mathfrak{Nil}(A)$ l'ensemble des éléments nilpotents de A.
Montrer que $\mathfrak{Nil}(A)$ est un idéal de A. Déterminer $\mathfrak{Nil}(\mathbb{Z}/n\mathbb{Z})$ pour $n \in \mathbb{N}^*$.

⋆⋆ **Exercice 28 —** Soit I un idéal d'un anneau supposé commutatif A. On appelle radical de I l'ensemble $\sqrt{I} = \left\{ x \in A \mid \exists n \in \mathbb{N}, x^n \in I \right\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A contenant I.
2. Soient I et J deux idéaux de A.
   a) Montrer que $I \subset J \Longrightarrow \sqrt{I} \subset \sqrt{J}$.
   b) Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et comparer $\sqrt{I+J}$ et $\sqrt{I} + \sqrt{J}$.
3. Trouver le radical des idéaux de $\mathbb{Z}$.

⋆ **Exercice 29 —** Soit p un nombre premier supérieur ou égal à 3.

1. Montrer que pour tout $k \in [\![2, p-1]\!]$, p divise $\binom{p}{k}$.
2. En déduire que $f : \overline{x} \mapsto \overline{x}^p$ est un morphisme d'anneaux sur $\mathbb{Z}/p\mathbb{Z}$.
3. Redémontrer à partir de cela le petit théorème de Fermat.

⋆⋆⋆ **Exercice 30 —** Soient $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$.

1. Quels sont les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$? les éléments inversibles ?
2. Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$? les éléments idempotents ?
3. Quels sont les morphismes d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$? de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$? de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$? de $\mathbb{Q}$ dans $\mathbb{Z}/n\mathbb{Z}$?

⋆⋆ **Exercice 31 —** *Équation de Pell-Fermat $x^2 - 2y^2 = 1$*
On considère l'ensemble $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau intègre de $\mathbb{R}$.
2. On pose, pour tout $x = a + b\sqrt{2}$ de $\mathbb{Z}[\sqrt{2}]$, $N(x) = a^2 - 2b^2$.
   a) Montrer que pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, $N(xy) = N(x)N(y)$.
   b) En déduire que x est inversible dans $\mathbb{Z}[\sqrt{2}]$ ssi $N(x) = \pm 1$.
3. Montrer que les éléments $\pm(1+\sqrt{2})^n$ de $\mathbb{Z}[\sqrt{2}]$ sont inversibles.
4. On veut établir que tout inversible x de $\mathbb{Z}[\sqrt{2}]$ est de la forme précédente.
   a) Montrer qu'on peut se restreindre à $x = a + b\sqrt{2}$, avec $a, b \in \mathbb{N}^*$.
   b) Montrer alors que x est de la forme $(1+\sqrt{2})^n$ avec $n \in \mathbb{N}$ et conclure.

⋆⋆ **Exercice 32 —** On considère l'ensemble $\mathbb{Z}[j] = \mathbb{Z} + j\mathbb{Z}$ où $j = \mathrm{e}^{2i\pi/3}$.

1. Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $(\mathbb{C}, +, \times)$. Est-ce un corps ?
2. On note $\mathbb{Z}[j]^*$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[j]$.
   a) Prouver que $x \in \mathbb{Z}[j]^*$ si et seulement si $|x| = 1$.
   b) Déterminer alors les inversibles de $\mathbb{Z}[j]$.
   Que dire de $(\mathbb{Z}[j]^*, \times)$?
3. Soient $x, y \in \mathbb{Z}[j]$ avec $y \neq 0$.
   Justifier l'existence de $(q, r) \in \mathbb{Z}[j]^2$ vérifiant $x = qy + r$ avec $|r| < |y|$.
4. En conclure que tous les idéaux de $\mathbb{Z}[j]$ sont principaux.

⋆⋆ **Exercice 33 —** *Algèbre des quaternions*
Soient les quatre matrices suivantes :

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} ; \quad J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} ; \quad K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} ; \quad L = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$$

Montrer que $\mathbb{H} = \{aI + bJ + cK + dL, (a, b, c, d) \in \mathbb{R}^4\} \subset \mathcal{M}_2(\mathbb{C})$ est une $\mathbb{R}$-algèbre.

Partie C – Arithmétique de $\mathbb{Z}$

⋆ **Exercice 34 —** Trouver le dernier chiffre de 2026^{2026} et de 1789^{2026}.

⋆⋆ **Exercice 35 —** *Théorème de Wilson*

Soit $p \in \mathbb{N}^*$. Montrer que p est premier ssi $(p-1)! + 1 \equiv 0\ [p]$.
On déterminera les solutions dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $\overline{x}^2 = \overline{1}$.

⋆⋆⋆ **Exercice 36 —** *Formule de Legendre et minoration de Tchebychev*

On note $v_p(n)$ la valuation p-adique d'un entier naturel n non nul et $\pi(x)$ le nombre d'entiers premiers inférieurs ou égaux à x.

1. Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$; en déduire que $\binom{2n}{n}$ divise $\prod_{\substack{p \text{ premier} \\ p \leqslant 2n}} p^{\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor}$.
2. Montrer que $\frac{4^n}{2n+1} \leqslant \binom{2n}{n} \leqslant (2n)^{\pi(2n)}$ et enfin que $\frac{x}{\ln(x)} \underset{x\to+\infty}{=} O(\pi(x))$.

⋆ **Exercice 37 —** Résoudre dans $\mathbb{Z}$ le système de congruences : $\begin{cases} x \equiv 4\ [5] \\ x \equiv 3\ [6] \end{cases}$

Partie D – Anneaux de polynômes

⋆ **Exercice 38 —** Soient A et B deux éléments de $\mathbb{K}[X]$.

1. On suppose ici que $A^2 | B^2$. Montrer que $A | B$.
2. Montrer que $A \wedge B = 1$ si et seulement si $(A+B) \wedge AB = 1$.
3. Montrer que si $A \wedge B = 1$, alors $A \wedge BC = A \wedge C$.

⋆ **Exercice 39 —** Soit $\alpha \in]0, \pi[$. Factoriser $X^{2n} - 2\cos(n\alpha)X^n + 1$ dans $\mathbb{R}[X]$.

⋆ **Exercice 40 —** Résoudre dans $\mathbb{C}[X]^2$ l'équation $(X^2+X+1)P - (X+2)Q = X^3$.

⋆ **Exercice 41 —** Prouver que lorsque $n \in \mathbb{N}^*$, $(X^2+X+1)^2 | (X+1)^{6n+1} - X^{6n+1} - 1$.

⋆ **Exercice 42 —** Soient $n \in \mathbb{N}^*$ et $\theta \in \mathbb{R}$.
Montrer que $X^2 - 2\cos(\theta)X + 1 | \sin(2\theta)X^n - \sin(n\theta)X^2 + \sin((n-2)\theta)$.

⋆⋆ **Exercice 43 —** Soient p et q deux entiers naturels premiers entre eux.
Montrer que $(X^p - 1)(X^q - 1) \mid (X-1)(X^{pq} - 1)$.

⋆ **Exercice 44 —** Montrer que si $P \in \mathbb{R}[X]$ est scindé sur $\mathbb{R}$, P' aussi.
On commencera par traiter le cas des polynômes scindés à racines simples.

⋆⋆ **Exercice 45 —** Soient $P \in \mathbb{R}_n[X]$ scindé à racines simples notées $x_1, \dots, x_n$ et $A \in \mathbb{R}[X]$ tels que $\deg(A) < \deg(P)$.

1. Donner la décomposition en éléments simples de A/P.
2. Montrer que $\sum_{k=1}^{n} \frac{1}{P'(x_k)} = 0$.

⋆⋆ **Exercice 46 —** On considère $P \in \mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$.

1. Montrer que le coefficient dominant de P est positif.
2. Montrer que les racines réelles de P sont de multiplicité paire.
3. Montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

⋆⋆⋆ **Exercice 47 —** Soit $P \in \mathbb{R}[X]$ un polynôme scindé sur $\mathbb{R}$. Montrer que pour tout réel α, $P' + \alpha P$ est scindé sur $\mathbb{R}$.

⋆⋆⋆ **Exercice 48 —** *Polynômes cyclotomiques*

Pour $n \in \mathbb{N}^*$, on appelle racine primitive n-ième de l'unité tout complexe ξ engendrant $\mathbb{U}_n$. On note Z_n l'ensemble des racines primitives. On pose :

$$\phi_n = \prod_{\xi \in Z_n} (X - \xi)$$

1. Déterminer ϕ_n pour $n \in \{1,2,3,4,5,6\}$.
2. Exprimer $\deg(\phi_n)$ à l'aide de l'indicatrice d'Euler.
3. Déterminer ϕ_p pour p premier.
4. Montrer que pour tout entier non nul n, $X^n - 1 = \prod_{k \mid n} \phi_k(X)$.
5. a) Montrer que si $A = BC$ avec $A, B \in \mathbb{Q}[X]$ et $C \in \mathbb{C}[X]$, alors $C \in \mathbb{Q}[X]$. Montrer que si $A, B \in \mathbb{Z}[X]$ et sont de plus unitaires, alors il en va de même pour C.
   b) En déduire que pour tout $k \in \mathbb{N}^*$, $\phi_k \in \mathbb{Z}[X]$.