Structures algébriques et arithmétique

Travaux dirigés #21

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 $x,y\in\mathbb{R}$, $\text{th}(x+y)=\dfrac{\text{th}(x)+\text{th}(y)}{1+\text{th}(x)\text{th}(y)}$.

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 $(\mathbb{R},+)$.
   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 $\mathcal{GL}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{GL}_n(\mathbb{R})$ à coefficients dans $\mathbb{Z}$ et dont l'inverse est encore à coefficients dans $\mathbb{Z}$.

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

Exercice 4 — Montrer qu'un groupe dont tous les éléments sont d'ordre 2 (à l'exception de l'élément neutre) est abélien.

Exercice 5 — Montrer que tout groupe fini 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 $((\mathbb{Z}/5\mathbb{Z})^*,\times)$.

Exercice 6 — Soit $n\in\mathbb{N}^*$. Montrer que $M\mapsto M^TM$ est un endomorphisme de $\mathcal{GL}_n(\mathbb{R})$. En déduire que $\mathcal{O}_n(\mathbb{R})$ et $\mathcal{SO}_n(\mathbb{R})$ sont des groupes.

Exercice 7 — On considère un groupe G et deux sous-groupes H et K de G.

1. Soit $x\in G$. Montrer que $x\in HK$ si et seulement si $x^{-1}\in KH$.
2. Montrer l'équivalence des assertions suivantes :

(a) HK est un sous-groupe de G (b) KH est un sous-groupe de G

(c) $HK=KH$

Exercice 8 — Montrer que $\dfrac{2}{3}\mathbb{Z}+\dfrac{1}{5}\mathbb{Z}$ est un sous-groupe monogène de $\mathbb{Q}$.

🚲 **Exercice 9 —** 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 10 — Montrer que les éléments inversibles de $\mathbb{Z}/11\mathbb{Z}$ forment un groupe cyclique, dont on précisera les générateurs.

Exercice 11 —

1. Montrer que tout sous-groupe de $(\mathbb{U}_n,\times)$ est cyclique.
2. En déduire que tout sous-groupe d'un sous-groupe cyclique est cyclique.

Exercice 12 — 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 13 — 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 $p\vee q$.

Exercice 14 — Soient G et H deux groupes cycliques.

1. Montrer que si h est un élément d'ordre p de H et k un élément d'ordre q de K alors (h,k) est un élément d'ordre $p \vee q$ de $H \times K$.
2. Préciser alors à quelle condition le groupe $G \times H$ est cyclique.

🚲 **Exercice 15 —** *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 : $g \mathcal{R} g' \iff g^{-1}g' \in H$.

1. Montrer que $\mathcal{R}$ 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 16 — *Caractérisation des carrés dans $\mathbb{Z}/p\mathbb{Z}$*
Soient p un nombre premier différent de 2 et $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

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

⚙ Partie B – Anneaux, corps et algèbres

Exercice 17 — 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 18 — 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 19 — Soit I un idéal d'un anneau supposé commutatif A. On appelle radical de I l'ensemble $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in I\}$.

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 20 — Soit $A = \left\{ \dfrac{m}{2^n} \;\middle|\; m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$.

1. Montrer que A est un sous-anneau de $(\mathbb{Q},+\times)$.
2. Quels sont ses éléments inversibles?

🚲 **Exercice 21 —** *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 $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$.
   b) Montrer alors que x est de la forme $(1+\sqrt{2})^n$ avec $n \in \mathbb{N}$ et conclure.

Exercice 22 — On considère l'ensemble $\mathbb{Z}[j] = \mathbb{Z} + j\mathbb{Z}$ où $j = e^{2i\pi/3}$.

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 23 — *Algèbre des quaternions*

Soient les quatre matrices suivantes :

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

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 24 — Trouver le dernier chiffre de 2021^{2021} et de 1789^{2021}.

Exercice 25 —

1. Résoudre dans $\mathbb{Z}$ les équations $12x \equiv 3\ [14]$ et $12x \equiv 8\ [14]$.
2. a) Déterminer une condition nécessaire et suffisante pour que $ax \equiv b\ [n]$ admette une solution.
   b) Préciser une démarche de résolution de l'équation $ax = b$ dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 26 — Résoudre dans $\mathbb{Z}$ le système de congruences :

$$\begin{cases} x \equiv 4\ [5] \\ x \equiv 3\ [6] \end{cases}$$

🚲 **Exercice 27 —** *Retour sur le petit théorème de Fermat*

1. Soient p un entier premier et $k \in [\![1, p-1]\!]$. Montrer que p divise $\binom{p}{k}$.
2. Démontrer que pour tous $x, y \in \mathbb{Z}$, $(x+y)^p \equiv x^p + y^p\ [p]$.
3. En déduire par récurrence que pour tout entier a, $a^p \equiv a\ [p]$. Simplifier dans le cas où $p \nmid a$.

Exercice 28 — *Théorème de Wilson*

Soit $p \in \mathbb{N}^*$. Montrer que p est premier si et seulement si :

$$(p-1)! + 1 \equiv 0\ [p]$$

On déterminera les solutions dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $\overline{x}^2 = \overline{1}$.

Partie D – Anneaux de polynômes

Exercice 29 — 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 30 —** Soit $\alpha \in]0, \pi[$. Factoriser $X^{2n} - 2\cos(n\alpha)X^n + 1$ dans $\mathbb{R}[X]$.

Exercice 31 — Résoudre dans $\mathbb{C}[X]^2$ l'équation $(X^2+X+1)P - (X+2)Q = X^3$.

Exercice 32 — Trouver une condition nécessaire et suffisante sur $n \in \mathbb{N}^*$ de telle sorte que $X^2 + X + 1 \mid X^{2n} + X^n + 1$.

Exercice 33 — 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 34 — *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 $k \in \mathbb{N}^*$, $\phi_k \in \mathbb{Z}[X]$.

CCINP Exercices : 66, 86 et 94.