ANNEAU $\mathbb{Z}/n\mathbb{Z}$: THÉORÈME CHINOIS, AUTOMORPHISMES, INDICATRICE D'EULER, INVERSIBLES

Exercice 1 (Groupes d'automorphismes)

1. Montrer que les automorphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont obtenus par multiplication par un inversible de $(\mathbb{Z}/n\mathbb{Z}, \times)$.
2. Décrire un isomorphisme de $\mathbb{Z}/10\mathbb{Z}$ sur $(\mathbb{Z}/11\mathbb{Z})^\star$.
3. Montrer que si G et H sont deux groupes d'ordre premiers entre eux, alors
$$Aut(G \times H) = Aut(G) \times Aut(H).$$
4. En déduire le groupe des automorphismes de $\mathbb{Z}/133\mathbb{Z}$.
5. Soit p un nombre premier et n un entier naturel non nul. Montrer que
$$Aut((\mathbb{Z}/p\mathbb{Z})^n) = GL(n, \mathbb{F}_p).$$
6. Montrer que $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to Bij((1,0),(1,1),(0,1))$ est un isomorphisme.

Exercice 2 (Exemple de produits semi-directs)

1. Montrer que, après avoir fixé un générateur de $(\mathbb{Z}/11\mathbb{Z})^\star$, la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $Aut(\mathbb{Z}/11\mathbb{Z})$ revient à la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/10\mathbb{Z}$.
2. En déduire une structure de produit semi-direct sur $\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$.
3. Montrer que toutes les structures de produit semi-direct donnent des groupes isomorphes. *On pourra montrer que si* $\varphi, \psi \in Hom(\mathbb{Z}/5\mathbb{Z}, Aut(\mathbb{Z}/11\mathbb{Z})$ *alors il existe* $\gamma \in Aut(\mathbb{Z}/11\mathbb{Z})$ *tel que* $\psi(h) = \gamma \circ \varphi(h) \circ \gamma^{-1}$.
4. Montrer que tous les morphismes de $\mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$ sont de la forme $t \mapsto \{x \mapsto k^t x\}$ où k est un élément de $(\mathbb{Z}/q\mathbb{Z})^\star$ d'ordre p.

Exercice 3 (Théorème des deux carrés)

Le but de cet exercice est de montrer le théorème des deux carrés : Un nombre premier p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1[4]$.

1. Montrer le sens direct en énumérant les carrés modulo 4.
2. Montrer le sens direct en vérifiant que si le nombre premier $p \neq 2$ s'écrit $p = a^2 + b^2$ avec $(a, b) \in \mathbb{N}^2$, alors ab^{-1} est un élément d'ordre 4 dans $\mathbb{F}_p^\star$.
3. On suppose désormais que p est un nombre premier congru à 1 modulo 4. Montrer que (-1) admet une racine carrée dans $\mathbb{F}_p^\star$. On la notera c dans la suite.
4. On rappelle que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est un anneau euclidien. Vérifier que l'application
$$\begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{F}_p \\ (a+ib) & \mapsto & a+cb \end{array}$$
est un morphisme d'anneaux dont le noyau est l'idéal engendré par
$$D = \mathrm{pgcd}(p, 1+ic).$$
5. Vérifier que le module de D au carré vaut p et conclure.

Exercice 4 (Changements de base dans $\mathbb{C}^N$)

Soit N un entier naturel non nul. On considère l'espace $(\mathbb{C}^N, <\ ,\ >)$ muni du produit scalaire hermitien standard et de la base canonique (b_i). On choisit ω une racine primitive N-ième de l'unité. Pour tout $x = \sum_i x[i]b_i \in \mathbb{C}^N$, on pose

$$\hat{x}[n] := \sum_i x[i]\omega^{ni} \text{ et } \mathcal{F}(x) := \begin{pmatrix} \hat{x}[0] \\ \hat{x}[1] \\ \vdots \\ \hat{x}[N-1] \end{pmatrix}.$$

1. Écrire la matrice de $\mathcal{F}$ dans la base canonique de $\mathbb{C}^N$.
2. Pour tout $n = 0 \cdots N-1$, on définit $W_n := \begin{pmatrix} 1 \\ \omega^{-n} \\ \omega^{-2n} \\ \vdots \\ \omega^{-(N-1)n} \end{pmatrix}$. Montrer que $(W_n)_{n=0\cdots N-1}$ est une base orthogonale de $\mathbb{C}^N$.
3. Montrer que l'écriture de x dans la base $(W_n)_{n=0\cdots N-1}$ est
$$x = \frac{1}{N}\sum_n \hat{x}[n]W_n.$$

Exercice 5 (Transformation de Fourier sur $\mathbb{Z}/N\mathbb{Z}$)

Soit N un entier naturel non nul. On considère les groupes $(U, \times)$ des nombres complexes de module 1, son sous-groupe μ_N des racines N-ième de l'unité, $G := (\mathbb{Z}/N\mathbb{Z}, +)$ et $\hat{G} := (Hom(G, U), \times)$.

On note $(F(\mu_N), +, \cdot, \times))$ l'algèbre des fonctions sur μ_N à valeurs dans $\mathbb{C}$ munie des opérations déduites des opérations sur le but $\mathbb{C}$.

On note $(F(G), +, \cdot, \star)$ l'algèbre des fonctions sur G à valeurs complexes munie du produit de convolution défini à l'aide de la mesure de comptage μ sur G

$$x \star y[i] := \int_G x[g]y[i-g]d\mu(g).$$

À toute fonction x de $F(G)$, on associe la fonction $\mathcal{F}(x)$ de $F(\hat{G})$ par

$$\mathcal{F}(x)[\chi] := \int_G \chi(g)x[g]d\mu(g).$$

1. Vérifier que $\hat{G}$ est naturellement isomorphe au groupe μ_N.
2. Pour $a \in G$, on notera $\delta_a \in F(G)$ la fonction caractéristique de $\{a\}$. Montrer que $\delta_a \mapsto X^a$ définit un isomorphisme α de $(F(G), +, \cdot, \star)$ sur $(\mathbb{C}[X]/(X^N - 1), +, \cdot, \times)$.
3. Montrer que $f \mapsto (f(1), f(\omega), \cdots, f(\omega^{N-1}))$ réalise un isomorphisme β de $(F(\mu_N), +, \cdot, \times))$ sur l'algèbre produit $(\mathbb{C}^N, +, \cdot, \times)$.
4. Montrer que $\beta \circ \mathcal{F} \circ \alpha^{-1}$ est l'application d'évaluation sur les puissances de la racine primitive ω. Cette application sera donc appelée "transformation de Fourier discrète" et notée TFD_ω. Montrer que TFD_ω est inversible d'inverse $\frac{1}{N}TFD_{\omega^{-1}}$.
5. On choisit un entier $p < N/2$ et $P := \sum_{i=0}^{p} X^i$, et $Q := \sum_{i=0}^{p}(-1)^i X^i$. Le but est de calculer le produit PQ. Calculer $TFD_\omega(P)$ et $TFD_\omega(Q)$ et conclure.

LES GROUPES $\mathrm{SL}_n(K), \mathrm{GL}_n(K), \mathrm{PSL}_n(K)$

Exercice 6 (Cardinaux des groupes linéaires)

1. En comptant le nombre de base de $\mathbb{F}_p^n$ déterminer le cardinal de $GL_n(\mathbb{F}_p)$.
2. Montrer que les cardinaux des groupes sur $\mathbb{F}_q$ sont
   — $|\ \mathrm{SL}_n(\mathbb{F}_q)\ | = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}$
   — $|\ \mathrm{PGL}_n(\mathbb{F}_q)\ | = |\ \mathrm{SL}_n(\mathbb{F}_q)\ |$
   — $|\ \mathrm{PSL}_n(\mathbb{F}_q)\ | = |\ \mathrm{SL}_n(\mathbb{F}_q)\ | \,/\, \mathrm{pgcd}(n, q-1)$.
3. Montrer que l'ensemble des matrices triangulaires supérieures strictes est un p-sous-groupe de Sylow de $GL(n, \mathbb{F}_p)$.

Exercice 7 (Isomorphismes exceptionnels)

Soit K un corps. On rappelle que $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times$ est le groupe projectif linéaire et $\mathbb{P}^n(K)$ l'ensemble des droites vectorielles de K^{n+1}.

1. Rappeler l'action de $\mathrm{PGL}_{n+1}(K)$ sur $\mathbb{P}^n(K)$ et montrer qu'elle est fidèle et transitive.
2. Soit $K = \mathbb{F}^q$ le corps à q éléments. En déduire, pour $N = q^n + q^{n-1} + \cdots + 1$, une injection $\mathrm{PGL}_{n+1}(K) \to \Sigma_N$.
3. En déduire les isomorphismes exceptionnels suivants :
$$\mathrm{PGL}_2(\mathbb{F}_2) \simeq \Sigma_3, PGL_2(\mathbb{F}_3) \simeq \Sigma_4, \mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$$

Exercice 8 (Isomorphismes exceptionnels (suite))

Soit K un corps. On rappelle que $\mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K))$ est le groupe projectif spécial linéaire.

1. Montrer que l'action de $\mathrm{PSL}_{n+1}(K)$ sur $\mathbb{P}^n(K)$ est fidèle et transitive.
2. Montrer que $\mathrm{PSL}_n(K)$ est un sous-groupe distingué de $\mathrm{PGL}_n(K)$ et que le quotient est isomorphe à $K^\times/(K^\times)^n$.
3. En déduire les isomorphismes exceptionnels suivants :
$$\mathrm{PSL}_2(\mathbb{F}_2) \simeq \Sigma_3, \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4, \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$$
4. On note $q = p^s$. On considère l'action de $\mathrm{PSL}_2(\mathbb{F}_q)$ sur $\mathbb{P}^1(\mathbb{F}_q)$. En faisant le choix d'un point à l'infini, les translations du complémentaires donnent des permutations de $\mathbb{F}_q$. Montrer qu'elles se décomposent en produit de p^{s-1} cycles de longueur p. Retrouver alors les résultats précédents.

SIMPLICITÉ

Exercice 9 (Exemple de produit semi-direct)

1. Montrer que l'ensemble des matrices $M_{20} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \right\} \subset \mathrm{PSL}_3(\mathbb{F}_4)$ est un groupe, contenant les sous-groupes $\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$ et $\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \right\}$
2. Est-ce un groupe simple ?

3. En déduire une structure de produit semi-directe sur $M_{20} \equiv \mathbb{F}_4^{\oplus 2} \rtimes \mathrm{SL}_2(\mathbb{F}_4)$.

Exercice 10 (Simplicité de $\mathfrak{A}_5$)

1. Faire la liste des classes de conjugaison de $\mathfrak{S}_n$ dans $\mathfrak{A}_n$ en les dénombrant.
2. Montrer que les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
3. Montrer que les éléments d'ordre 2 sont conjugués dans $\mathfrak{A}_n$.
4. Montrer que tout sous-groupe distingué H de $\mathfrak{A}_n$ qui contient un élément d'ordre 5 les contient tous. (On remarquera que le groupe engendré par un élément d'ordre 5 est un Sylow.)
5. Montrer que tout sous-groupe distingué H de $\mathfrak{A}_n$ non réduit à $\{\mathrm{id}\}$ contient au moins deux types d'éléments en plus de l'identité. Montrer alors que $H = \mathfrak{A}_n$.

ALGÈBRES ASSOCIATIVES SUR UN ANNEAU COMMUTATIF

Exercice 11 (Exemples)

1. À l'aide d'algèbre de polynômes, donner un exemple d'algèbre associative et commutative de dimension finie sur un corps k.
2. Donner l'exemple d'une algèbre associative mais non commutative sur un anneau commutatif.

Exercice 12 (Théorème de Frobenius)

Le but de l'exercice est de démontrer le théorème de Frobenius qui caractérise les algèbres associatives à division de dimension finie sur le corps commutatif $\mathbb{R}$ des réels. Il n'y en a que trois (à isomorphisme près) : le corps $\mathbb{R}$ des réels, celui $\mathbb{C}$ des complexes et le corps non commutatif $\mathbb{H}$ des quaternions. Un anneau à division est un anneau (unitaire) non nul dans lequel tout élément non nul a un inverse.

Soient donc D une $\mathbb{R}$-algèbre associative à division et de dimension finie sur $\mathbb{R}$ mais non réduite à $\mathbb{R}$, x un élément non réel de D, et $C = \mathbb{R}[x]$.

1. Montrer que C est isomorphe à $\mathbb{C}$.
2. Soit donc i l'une des deux racines carrées de -1 dans C. Montrer que l'automorphisme intérieur $d \mapsto i^{-1}di$ associé à i est un endomorphisme diagonalisable du $\mathbb{R}$ espace vectoriel D.
3. On note D^+ et D^- les espaces propres associés à 1 et -1. Montrer que $D^+ = C$.
4. Montrer que si $D^- = \{0\}$, alors D est isomorphe à $\mathbb{C}$.
5. Si D^- est non nul, soient y un élément non nul de D^- et (comme précédemment) j l'une des deux racines carrées de -1 dans l'algèbre $\mathbb{R}[y] = \mathbb{R} + \mathbb{R}y$. Montrer que y^2 est un réel négatif et donc que j appartient à D^-.
6. En considérant la bijection $d \mapsto dj$, montrer que
$$D = C \oplus Cj = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$
avec $k = ij = -ji$, et D est alors isomorphe au corps des quaternions.