Exercices pour le module "Algèbre 1 - HAX708X"

Année 2025/2026

Exercices sur le thème « anneaux »

1. Soient $n, m \geq 1$. A quelle condition existe-t-il un morphisme d'anneau $\varphi : \mathbb{Z}\backslash n\mathbb{Z} \to \mathbb{Z}\backslash m\mathbb{Z}$?

2. Montrer que tous les idéaux de $\mathbb{Z}\backslash n\mathbb{Z}$ sont principaux. Déterminer les idéaux premiers.

3. Soit N le nilradical de $\mathbb{Z}\backslash n\mathbb{Z}$. A quelle condition le quotient $\mathbb{Z}\backslash n\mathbb{Z}/N$ est-il un corps ?

4. Soient A et B deux anneaux commutatifs et soit $I \subset A \times B$. Démontrer que I est un idéal de $A \times B$ si et seulement si $I = I_A \times I_B$, où I_A est un idéal de A et I_B est un idéal de B.

5. Soient A un anneau commutatif et $\mathrm{Nil}(A) := \{x \in A | \exists n \in \mathbb{N}, x^n = 0\}$ son nilradical.

(1) Montrer que $\mathrm{Nil}(A)$ est un idéal de A.
(2) Montrer que si P est un idéal premier de A, alors $\mathrm{Nil}(A) \subset P$.
(3) Soit $x \notin \mathrm{Nil}(A)$. Montrer qu'il existe un idéal premier P tel que $x \notin P$. *On utilisera le Lemme de Zorn.*
(4) En déduire que $\mathrm{Nil}(A) = \bigcap_{P \text{ premier}} P$.

6. On considère l'anneau des séries formelles $A[[X]]$.

(1) Montrer qu'un élément $P = \sum_{n\in\mathbb{N}} a_n X^n$ est inversible si et seulement si a_0 est inversible dans A.
(2) On suppose que $A = \mathbb{K}$ est un corps.
   — Montrer que $\mathbb{K}[[X]]$ possède un seul idéal maximal.
   — Déterminer tous les idéaux de $\mathbb{K}[[X]]$.
   — Soit $n \geq 1$. Expliciter l'inverse de $(1 - X)^n$ dans $\mathbb{K}[[X]]$.
(3) Dans le cas général, caractériser les idéaux maximaux de $A[[X]]$.

7. L'anneau des décimaux est principal

Soient $\mathbb{D}$ l'anneau des décimaux et $I \subset \mathbb{D}$ un idéal.

(1) En considérant l'idéal $I \cap \mathbb{Z}$ de $\mathbb{Z}$, montrer que I est principal.
(2) Expliciter le groupe des inversibles $\mathbb{D}^\times$.
(3) Déterminer les idéaux $(0, 42) + (38500)$ et $(0, 42) \cap (38500)$.

8. Sous-anneaux quadratiques de $\mathbb{C}$

On posera successivement $\alpha = i,\ i\sqrt{2},\ i\sqrt{3},\ \frac{1+i\sqrt{3}}{2},\ \frac{1+i\sqrt{7}}{2},\ \frac{1+i\sqrt{19}}{2}$. On considère l'application $N : \mathbb{C} \to \mathbb{R}^{\geq 0}$ définie par $N(z) = |z|^2$.

(1) Montrer que tout élément de $\mathbb{Z}[\alpha]$ s'écrit de façon unique sous la forme $x + y\alpha$, avec $x, y \in \mathbb{Z}$.
(2) Montrer que l'anneau $\mathbb{Z}[\alpha]$ est stable par conjugaison.
(3) Montrer que N définit une application multiplicative de $\mathbb{Z}[\alpha]$ dans $\mathbb{N}$.
(4) Montrer que les éléments inversibles de $\mathbb{Z}[\alpha]$ sont les éléments de norme 1. Décrire le groupe multiplicatif $\mathbb{Z}[\alpha]^\times$.
(5) Soit $z \in \mathbb{C}$. Pour quels α dans la liste existe-t-il toujours $z_0 \in \mathbb{Z}[\alpha]$ tel que $N(z - z_0) < 1$? Montrer que dans ce cas, l'anneau $\mathbb{Z}[\alpha]$ est principal.

9. Eléments irréductibles de $\mathbb{Z}[i]$

On considère l'anneau $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$. Pour tout entier $n \geq 2$, on considère l'anneau quotient $A_n := \mathbb{Z}[i]/(n)$ et l'anneau de polynômes $\mathbb{Z}/n\mathbb{Z}[X]$.

(1) Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
(2) Montrer que A_n est isomorphe au quotient $\mathbb{Z}/n\mathbb{Z}[X]/(X^2 + 1)$.
(3) En déduire qu'un entier $n \geq 2$ est irréductible dans $\mathbb{Z}[i]$ si et seulement si n est un nombre premier, et si -1 n'est pas un carré de $\mathbb{Z}/n\mathbb{Z}$.
(4) Lorsque p est un nombre premier tel que $p = 3 \bmod 4$, montrer qu'il existe $\alpha_p, \beta_p \in \mathbb{Z}[i]$ irréductibles tel que $p = \alpha_p \beta_p$.
(5) Déterminer les éléments irréductibles de $\mathbb{Z}[i]$.

10. Est ce que $\cos(\frac{2\pi}{5})$ est rationnel ?

On considère le polynôme $P = X^4 + X^3 + X^2 + X + 1$.

(1) Déterminer la décomposition en facteur premier de P dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.
(2) Montrer que P est irréductible dans $\mathbb{Z}[X]$.
(3) En déduire que $\cos(\frac{2\pi}{5}) \notin \mathbb{Q}$.

11. Anneau de polynômes $A[X]$: éléments inversibles, nilpotents ; division euclidienne

(1) On suppose A intègre. Déterminer $(A[X])^\times$.
(2) Dans le cas général, montrer que $P = \sum_{k=0}^{n} a_k X^k$ est inversible si et seulement si $a_0 \in A^\times$ et $a_k \in Nil(A)$ pour tout $k \geq 1$.
(3) Déterminer le nilradical de $A[X]$.
(4) Montrer que l'on peut effectuer la division euclidienne par $P = \sum_{k=0}^{n} a_k X^k$ si $a_0 \in A^\times$.

12. Polynômes irréductibles

(a) Soit A un anneau factoriel. Montrer qu'un polynôme de degré ≤ 3, $P(X) = a + bX + cX^2 + dX^3$, est irréductible dans $A[X]$ si et seulement si $pgcd(a, b, c, d) = 1$ et si, de plus, $P(X)$ n'admet pas de racines dans la corps de fractions de A.

(b) Soit $p \geq 2$ un nombre premier. On note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ le corps à p élément et $\pi_p : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme associé à la projection canonique $\mathbb{Z} \to \mathbb{F}_p$. Soit $\Phi_p := \sum_{k=0}^{p-1} X^k \in \mathbb{Z}[X]$.

(1) Montrer que pour tout $1 < k < p$, le coefficient binomial C_k^p est divisible par p.
(2) Montrer que pour tout $P, Q \in \mathbb{F}_p[X]$, on a $(P - Q)^p = P^p - Q^p$.
(3) Montrer que $\pi_p(\Phi_p) = (X - 1)^{p-1}$. *On calculera* $(X - 1)\Phi_p$.
(4) Montrer que Φ_p est irréductible dans $\mathbb{Z}[X]$.

13. Critère d'Eisenstein

On considère un nombre premier $p \geq 2$ et le corps $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Soit $\phi_p : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$, le morphisme d'anneaux canonique.

(1) Pour $n \geq 1$, décrire l'ensemble $I_{p,n} \subset \mathbb{Z}[X]$ formé des polynômes Q de degré n vérifiant $\phi_p(Q) = \lambda X^n$ avec $\lambda \in \mathbb{F}_p - \{0\}$.
(2) Soit $Q = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme primitif de degré n : $pgcd(a_0, \ldots, a_n) = 1$. Montrer que Q est irréductible dans $\mathbb{Z}[X]$ si $Q \in I_{p,n}$ et si de plus p^2 ne divise pas a_0.
(3) Montrer que $8X^4 + 15X^2 + 45$ est irréductible dans $\mathbb{Z}[X]$.

14. Anneaux quotients

On considère les anneaux $A = \mathbb{Z}[X]/(2X+3)$ et $B = \mathbb{Z}[X]/(2X, 3)$

(1) Montrer que A est isomorphe à $\mathbb{Z}[\frac{1}{2}] \subset \mathbb{Q}$.
(2) Montrer que B est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.
(3) Existe-t-il un morphisme d'anneau de A vers B ? De B vers A ?

15. Corps à neuf éléments

On considère l'anneau $A = \mathbb{Z}/3\mathbb{Z}[X]$ et l'idéal $I = (X^2+1)$.

(1) Montrer que $\mathbb{K} := A/I$ est un corps. Quel est son cardinal ?
(2) Soit k un corps ayant 9 éléments.
   — Montrer que $k^\times$ est un groupe cyclique d'ordre 8. En déduire que $\exists \alpha \in k, \alpha^2 = -1$.
   — Montrer qu'il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \to k$.
   — Montrer que $\ker(\varphi) = 3\mathbb{Z}$ (on remarquera que $\mathbb{Z}/\ker(\varphi)$ est un corps qui s'injecte dans k).
   — En déduire que k est isomorphe à $\mathbb{K}$.

16. Soit $\mathbb{K}$ un corps. On pose $A = \mathbb{K}[X, Y]/(X^2, XY, Y^2)$.

(1) Déterminer les éléments inversibles de A.
(2) Déterminer tous les idéaux principaux de A.
(3) Déterminer tous les idéaux de A.

17. Sous-ensembles algébriques de $\mathbb{C}^n$: $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$

Si I est un idéal de $\mathbb{C}[X_1, \dots, X_n]$, on note $\mathcal{Z}(I)$ l'ensemble des $(x_1, \dots, x_n) \in \mathbb{C}^n$ tels que $P(x_1, \dots, x_n) = 0$ pour tout $P \in I$. Si Z est une partie de $\mathbb{C}^n$, on note $\mathcal{I}(Z)$ l'idéal formé des $P \in \mathbb{C}[X_1, \dots, X_n]$ tels que $P(x_1, \dots, x_n) = 0$ pour tout $(x_1, \dots, x_n) \in Z$.

(1) Comparer les idéaux I et $\mathcal{I}(\mathcal{Z}(I))$.
(2) Montrer que $\mathcal{Z}(I) = \emptyset$ si et seulement si $I = \mathbb{C}[X_1, \dots, X_n]$.
(3) Soit $P \in \mathcal{I}(\mathcal{Z}(I))$ et J l'idéal de $\mathbb{C}[X_1, \dots, X_n, X_{n+1}]$ engendré par I et $1 - X_{n+1}P$.
   — Montrer que $\mathcal{Z}(J) = \emptyset$.
   — En déduire qu'il existe des polynômes $P_\ell \in I$ et $Q, Q_\ell \in \mathbb{C}[X_1, \dots, X_n, X_{n+1}]$ tels que $(1 - X_{n+1}P)Q + \sum_{\ell=1}^{N} P_\ell Q_\ell = 1$.
   — En regardant la relation précécente dans $\mathbb{C}[X_1, \dots, X_n, X_{n+1}]/(1 - X_{n+1}P)$, montrer qu'il existe $m \in \mathbb{N}$ tel que $P^m \in I$.
(4) Conclure.

18. Nombres algébriques

Un nombre complexe $\alpha \in \mathbb{C}$ est dit *algébrique*, s'il existe $P \in \mathbb{Q}[X]$ non-nul tel que $P(\alpha) = 0$. Pour tout $\alpha \in \mathbb{C}$, on considère $\mathbb{Q}[\alpha] = \{Q(\alpha), Q \in \mathbb{Q}[X]\} \subset \mathbb{C}$: c'est une sous $\mathbb{Q}$-algèbre de $\mathbb{C}$.

(1) Montrer que les assertions suivantes sont équivalentes.
   — $\alpha \in \mathbb{C}$ est algébrique.
   — $\mathbb{Q}[\alpha]$ est de dimension finie sur $\mathbb{Q}$.
   — $\mathbb{Q}[\alpha]$ est un corps.
(2) Soient $\alpha, \beta \in \mathbb{C}$ deux nombres algébriques.
   — Montrer que $\alpha + \beta$ et $\alpha\beta$ sont algébriques.
   — Lorsque $\alpha \neq 0$, montrer que α^{-1} est algébrique.
(3) En déduire que l'ensemble $\mathcal{A}$ des nombres algébriques est un sous-corps de $\mathbb{C}$.
(4) Est-ce que $\mathcal{A} = \mathbb{C}$?

Exercices sur le thème « modules »

19. Morphismes de $\mathbb{Z}$-modules

(1) Soient $a, b \geq 1$. Montrer que le groupe $\hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ est isomorphe à $\mathbb{Z}/a \wedge b\mathbb{Z}$.

(2) Existe-t-il un morphisme bijectif $\varphi : \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z} \longrightarrow \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ de $\mathbb{Z}$-modules ?

20. Endomorphismes de A^n

Soit A un anneau commutatif unitaire. Soient $m, n \geq 1$.

(1) Montrer que l'anneau $\hom_A(A^n, A^n)$ est isomorphe à l'anneau $M_n(A)$ formé des matrices $n \times n$ à coefficient dans A.

(2) Montrer que les assertions suivantes sont équivalentes :
— $X \in \hom_A(A^n, A^n)$ est inversible.
— $X \in \hom_A(A^n, A^n)$ est inversible à gauche.
— $X \in \hom_A(A^n, A^n)$ est inversible à droite.
— $\det(X) \in A^\times$.

(3) Montrer qu'il existe $\varphi \in \hom_A(A^n, A^m)$ bijectif si et seulement si $n = m$.

21. Facteurs invariants de $\mathbb{Z}$-modules

a. Soit $L \subset \mathbb{Z}^2$ le sous-groupe engendré par $(6, -4)$ et $(5, 5)$.

(1) On considère le morphisme $f : \mathbb{Z}^2 \to \mathbb{Z}$ défini par $f(x, y) = x$. Montrer qu'il existe $u_1 \in L$ tel que $f(u_1) = 1$. En déduire que $\mathbb{Z}^2 = \mathbb{Z}u_1 \oplus \ker(f)$ et $L = \mathbb{Z}u_1 \oplus (L \cap \ker(f))$.

(2) Déterminer $u_2 \in \mathbb{Z}^2$ et $n \in \mathbb{Z}$ tel que $\ker(f) = \mathbb{Z}u_2$ et $L \cap \mathbb{Z}u_2 = \mathbb{Z}n\, u_2$.

(3) En déduire les facteurs invariants de $\mathbb{Z}^2/L$.

b. Soit $M \subset \mathbb{Z}^3$ le sous-groupe engendré par $(6, -3, 6)$ et $(15, 5, -10)$.

(1) On considère le morphisme $g : \mathbb{Z}^3 \to \mathbb{Z}$ défini par $g(x, y, z) = y + z$. Montrer qu'il existe $u_1 \in M$ tel que $f(u_1) = 1$. En déduire que $\mathbb{Z}^3 = \mathbb{Z}u_1 \oplus \ker(g)$ et $M = \mathbb{Z}u_1 \oplus (M \cap \ker(g))$.

(2) Déterminer le groupe $M \cap \ker(g)$.

(3) En déduire les facteurs invariants de $\mathbb{Z}^3/M$.

22. Exemples

Donner des exemples :

(1) de modules non-libres,

(2) d'une famille libre à n éléments dans A^n qui ne soit pas une base,

(3) d'une partie génératrice minimale qui ne soit pas une base,

(4) de sous-module n'ayant pas de supplémentaire,

(5) de module libre ayant un sous-module qui ne l'est pas.

(6) de module sans torsion qui ne soit pas libre.

23. Modules libres

(1) Soit I un idéal de A.
— Quand est-ce que A/I est un A-module libre ?
— Montrer que si I est un A-module libre alors $\exists x \in A$ tel que $I = (x)$.
— Est-ce que $\mathbb{Z}[X]$ possède un idéal qui n'est pas un $\mathbb{Z}[X]$-module libre ?

(2) Considérons l'anneau $A = \mathbb{Z}/6\mathbb{Z}[X]$. Pour quels polynômes $P \in A$, l'idéal (P) est-il libre ?

24. Torsion

Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si $\exists a \in A - \{0\}, ax = 0$. On note $T(M)$ l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

(1) Montrer que $T(M)$ est un sous-module de M.
(2) Montrer que $M/T(M)$ est sans torsion.
(3) Déterminer la torsion du $\mathbb{Z}$-modules $M = \mathbb{R}/\mathbb{Z}$.

25. Module $\mathbb{Q}$

a. Montrer que $\mathbb{Q}$, en tant que $\mathbb{Z}$-module, est sans torsion, n'est pas libre et n'est pas de type fini.

b. Montrer que $\mathbb{Q}/\mathbb{Z}$ est un $\mathbb{Z}$-module de torsion (donc pas libre), et qui n'est pas de type fini.

26. Extensions de modules libres

Soient M et N deux A-modules et $f \in \hom_A(M, N)$.

(1) On suppose que $\ker(f)$ et $\mathrm{Im}(f)$ sont de type fini. Montrer que M est de type fini.
(2) On suppose que $\ker(f)$ et $\mathrm{Im}(f)$ sont libres. Montrer que M est libre.

27. Modules de type fini

Soit A un anneau principal.

a. Montrer que si L et M sont des A-modules de type fini, alors $\hom_A(L, M)$ est un module de type fini.

b. Montrer que tout sous-module d'un A-module de type fini est encore de type fini.

28. Groupes abéliens finis

L'exposant d'un groupe fini G est le plus petit entier $n \geq 1$ tel que $g^n = 1$ pour tout $g \in G$.

(1) Soit G un groupe abélien fini d'exposant e.
   — Montrer que G possède un élément d'ordre e.
   — Quel est le lien entre e et les facteurs invariants de G ?
(2) Montrer qu'un sous-groupe fini du groupe multiplicatif $\mathbb{K}^\times$ d'un corps commutatif $\mathbb{K}$ est cyclique.

29. Bases de $\mathbb{Z}$-modules

Déterminer une base des $\mathbb{Z}$-modules suivants :

(1) $M := \{(x, y, z) \in \mathbb{Z}^3, 2x - y + 5z \in 6\mathbb{Z}\}$.
(2) $N := \{(x, y, z) \in \mathbb{Z}^3, x - y + z \in 4\mathbb{Z} \text{ et } 3x + y + 8z \in 10\mathbb{Z}\}$.

30. Indice

Soit M un sous $\mathbb{Z}$-module de $\mathbb{Z}^n$ de rang égal à n. À chaque base $\mathcal{B} := \{v_1, \ldots, v_n\}$ de M on associe $d(\mathcal{B}) = |\det(v_1, \ldots, v_n)|$.

(1) Montrer que $d(\mathcal{B})$ ne dépend pas de la base de M. On note $d(M)$ cette quantité.
(2) On note $d_1, \ldots, d_n$ les facteurs invariants de $\mathbb{Z}^n/M$. Montrer que $\sharp(\mathbb{Z}^n/M) = d_1 \cdots d_n = d(M)$.
(3) Montrer qu'il y autant de sous-modules L contenant M que de sous-groupes de $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$.

31. Supplémentaires

a. Soit A un anneau principal et L un A-module libre de rang fini. Soit M un sous A-module de L. Montrer que les assertions suivantes sont équivalentes :

— L/M est un A-module sans-torsion.

— M possède un supplémentaire dans L.
— Il existe $\varphi \in \hom(L, A^r)$ surjectif tel que $\ker(\varphi) = M$.

b. À $\vec{u} := (a, b, c), \vec{v} = (a', b', c') \in \mathbb{Z}^3$, on associe le sous $\mathbb{Z}$-module $M = \mathbb{Z}\vec{u} + \mathbb{Z}\vec{v} \subset \mathbb{Z}^3$. A quelles conditions possède-t-il un supplémentaire ?

32. Facteurs invariants de $\mathbb{Z}$-modules

Déterminer les facteurs invariants des $\mathbb{Z}$-modules suivants :

(1) $\mathbb{Z}^3/M$ où M est défini à l'exercice 29.
(2) $(\mathbb{Z}/100\mathbb{Z}) \times (\mathbb{Z}/80\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$.

33. Matrices de $M_n(\mathbb{Z})$

À $X \in M_n(\mathbb{Z})$, on associe les sous-modules $\mathrm{Im}(X) = X(\mathbb{Z}^n)$ et $\ker(X)$ de $\mathbb{Z}^n$. Soient $A, B \in M_n(\mathbb{Z})$.

(1) Montrer l'équivalence : $\mathrm{Im}(A) = \mathrm{Im}(B) \iff \exists P \in GL_n(\mathbb{Z})$ tel que $A = BP$.
(2) Vérifier que l'hypothèse « $\ker(A) = \ker(B)$ » n'est pas équivalente à « $\exists Q \in GL_n(\mathbb{Z})$ tel que $A = QB$ ».
(3) Montrer que les modules $\mathbb{Z}^n/\mathrm{Im}(A)$ et $\mathbb{Z}^n/\mathrm{Im}(B)$ ont les mêmes facteurs invariants ssi $\exists P, Q \in GL_n(\mathbb{Z})$ tel que $A = QBP$.

34. Commutant

Soit A un anneau principal et M un A-module de type fini. D'après le théorème de classification, il existe $m_1, \ldots, m_s \in M$ tels que $M = \oplus_{k=1}^{s} Am_k$ et $\mathrm{Ann}(m_1) \supset \cdots \supset \mathrm{Ann}(m_s)$.

(1) Montrer qu'il existe $u_i \in \mathrm{End}_A(M)$ tel que $u_i(m_k) = \delta_{ks} m_i, \forall k$.
(2) Soit $u \in \mathrm{End}_A(M)$ qui commute avec tous les éléments de $\mathrm{End}_A(M)$. Montrer que u est la multiplication par un scalaire $a \in A$.
(3) Même question en supposant seulement que $u : M \to M$ est un morphisme de groupe additif qui commute avec tous les éléments de $\mathrm{End}_A(M)$.
(4) Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. A chaque sous-ensemble $\mathcal{X} \subset \mathrm{End}_{\mathbb{K}}(E)$, on associe son commutant

$$C(\mathcal{X}) = \{u \in \mathrm{End}_{\mathbb{K}}(E); u \circ f = f \circ u, \forall f \in \mathcal{X}\}.$$

Montrer que pour tout $u \in \mathrm{End}_{\mathbb{K}}(E)$ on a la relation $C(C(\{v\})) = \mathbb{K}[v]$. *On utilisera la structure de $\mathbb{K}[X]$-module sur E associée à $v \in \mathrm{End}_{\mathbb{K}}(E)$.*

Exercices sur le thème « produit tensoriel »

35. Produit tensoriel des groupes $\mathbb{Z}/n\mathbb{Z}$

Soient $m, n \geq 1$.

(1) Montrer que $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$ si m, n sont premiers entre eux
(2) Montrer qu'en général $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/pgcd(m,n)\mathbb{Z}$.

36. Produit tensoriel et torsion

Soit M un $\mathbb{Z}$-module.

(1) Montrer que $M \otimes_{\mathbb{Z}} \mathbb{Q}$ est sans torsion.
(2) Montrer que M_{tor} est le noyau du morphisme naturel $M \to M \otimes_{\mathbb{Z}} \mathbb{Q}$.
(3) Montrer que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^n$ si M est un module de type fini.

37. Produit tensoriel et polynômes

(1) Montrer que le produit tensoriel $\mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y]$ est isomorphe à $\mathbb{K}[X, Y]$.
(2) Montrer que le produit tensoriel $\mathbb{K}(X) \otimes_{\mathbb{K}} \mathbb{K}(Y)$ s'identifie à une sous-algèbre stricte de $\mathbb{K}(X, Y)$.

38. Produit tensoriel de $\mathbb{K}$-algèbres

Soient A, B deux $\mathbb{K}$-algèbres.

(1) Montrer que le produit $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$ définit une structure de $\mathbb{K}$-algèbre sur $A \otimes_{\mathbb{K}} B$.
(2) Montrer que $M_n(\mathbb{K}) \otimes_{\mathbb{K}} B$ est une $\mathbb{K}$-algèbre isomorphe à $M_n(B)$.
(3) Montrer que $M_n(\mathbb{K}) \otimes_{\mathbb{K}} M_m(\mathbb{K})$ est une $\mathbb{K}$-algèbre isomorphe à $M_{nm}(\mathbb{K})$.

39. Produit tensoriel de $\mathbb{K}$-espaces vectoriels

Soient E, F deux $\mathbb{K}$-espaces vectoriels. On pose $E^* := \hom_{\mathbb{K}}(E, \mathbb{K})$ et on considère le morphisme canonique $\varphi : E^* \otimes_{\mathbb{K}} F \to \hom_{\mathbb{K}}(E, F)$.

(1) Décrire l'image de φ.
(2) Quand est-ce que φ est un isomoprhisme ?

40. Produit tensoriel d'endomorphismes

On considère deux $\mathbb{C}$-espaces vectoriels E et F de dimension fini. Soient $\phi \in \mathrm{End}(E)$ et $\psi \in \mathrm{End}(F)$.

(1) Montrer qu'il existe $\theta \in \mathrm{End}(E \otimes_{\mathbb{C}} F)$ définie par la relation $\theta(e \otimes f) = \phi(e) \otimes \psi(f)$.
(2) À quelles conditions θ est un isomorphisme ?
(3) Montrer la relation : $\mathrm{rang}(\theta) = \mathrm{rang}(\phi)\,\mathrm{rang}(\psi)$. *On pourra considérer des supplémentaires de* $\ker(\phi)$ *et* $\ker(\psi)$.

41. Produit tensoriel et suites exactes

Soient $0 \to M \to N \to P \to 0$ une suite exacte de A-modules, et R un A-module.

(1) Montrer que la suite induite $M \otimes_A R \to N \otimes_A R \to P \otimes_A R \to 0$ est exacte.
(2) Est-ce que la suite $0 \to M \otimes_A R \to N \otimes_A R$ est exacte en général ?

42. L'espace $\wedge^k E$ et les familles libres de E

Soit E un espace vectoriel de dimension $n \geq 1$. Notons $\wedge^k E$ l'algèbre extérieure de E de degré $k \geq 1$.

(1) Quelle est la dimension de $\wedge^k E$?
(2) Montrer qu'une famille $\{v_1, \ldots, v_k\}$ est libre ssi $v_1 \wedge \cdots \wedge v_k \neq 0$.
(3) Soient $\mathcal{V} := \{v_1, \ldots, v_k\}$ et $\mathcal{W} := \{w_1, \ldots, w_k\}$ deux familles libres. Montrer que $\mathrm{Vect}(\mathcal{V}) = \mathrm{Vect}(\mathcal{W})$ si et seulement si $v_1 \wedge \cdots \wedge v_k$ et $w_1 \wedge \cdots \wedge w_k$ sont colinéaires.

43. Vecteurs décomposable de $\wedge^k E$

Soit E un espace vectoriel de dimension $n \geq 1$. Un vecteur $\alpha \in \wedge^k E$ est décomposable s'il existe $v_1, \cdots, v_k$ tels que $\alpha = v_1 \wedge \cdots \wedge v_k$. On note $M_\alpha : V \to \wedge^{k+1} E$ l'application linéaire $v \mapsto \alpha \wedge v$.

(1) Vérifier que tous les éléments de $\wedge^1 E$ et $\wedge^n E$ sont décomposables.
(2) Montrer que tous les éléments de $\wedge^{n-1} E$ sont décomposables. *On pourra utiliser le fait que dans ce cas* $\ker(M_\alpha)$ *est un hyperplan de* E *et décomposer les vecteurs de* $\wedge^{n-1} E$ *relativement à la somme directe* $E = \ker(M_\alpha) \oplus \mathbb{R}w$.
(3) Si $f_1, \ldots, f_{2k}$ est une famille libre de E, montrer que $\alpha = \sum_{j=1}^{k} f_{2j-1} \wedge f_{2j}$ n'est pas décomposable. *Considérer* $\alpha \wedge \alpha$.
(4) Montrer que si $\alpha \in \wedge^k E$ est non-nul, alors $\dim \ker(M_\alpha) \leq k$.
(5) Montrer que pour tout $\alpha \in \wedge^k E$ non-nul, α est décomposable ssi $\dim \ker(M_\alpha) = k$.

44. Pfaffien

A une matrice $X \in M_{2n}(\mathbb{R})$ *anti-symétrique* on associe le vecteur $\rho(X) := \sum_{1 \leq i < j \leq 2n} a_{i,j}\, e_i \wedge e_j \in \wedge^2 \mathbb{R}^{2n}$. Comme $\rho(X)^n \in \wedge^{2n} \mathbb{R}^{2n}$, on définit le pfaffien de X par la formule

$$\frac{1}{n!}\rho(X)^n = \mathrm{Pf}(X)\, e_1 \wedge \ldots \wedge e_{2n}.$$

a. Si on considère avec la matrice

$$A_\lambda = \begin{pmatrix} 0 & \lambda_1 & & & \\ -\lambda_1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & \lambda_n \\ & & & -\lambda_n & 0 \end{pmatrix},$$

montrer que $\mathrm{Pf}(A_\lambda) = \lambda_1 \cdots \lambda_n$.

b. Montrer que pour toute matrice $X \in M_{2n}(\mathbb{R})$ *anti-symétrique*, il existe $\lambda = (\lambda_1, \cdots, \lambda_n)$ et $g \in GL_{2n}(\mathbb{R})$ tel que $X = g\, A_\lambda\, g^t$.

c. Montrer que $\mathrm{Pf}(X)^2 = \det(X)$ pour toute matrice $X \in M_{2n}(\mathbb{R})$ *anti-symétrique*.

Exercices sur le thème « représentations de groupes finis »

45. Représentations fidèles

Soit G un groupe fini de cardinal n.

(1) Montrer que G admet une représentation fidèle sur tout corps $\mathbb{K}$.
(2) Montrer que G est isomorphe à un sous-groupe de $\mathrm{SO}(2n)$.

46. Diagonalisation

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie et soit H un sous-groupe *fini* de $GL(E)$.

(1) Démontrer que tout élément de H est diagonalisable et que, si H est commutatif, tous les éléments de H sont diagonalisables dans une même base.
(2) En déduire que toutes les représentations complexes irréductibles d'un groupe abélien fini sont de degré 1.

47. Représentations irréductibles : quelques exemples

Montrer que les repésentations suivantes sont irréductibles

(1) L'action canonique de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathbb{K}^n$.
(2) L'action canonique de $\mathrm{GL}_n(\mathbb{R})$ sur $E = \{\text{formes quadratiques sur } \mathbb{R}^n\}$.
(3) L'action de $\mathfrak{S}_n$ sur $V = \{x \in \mathbb{K}^n, \sum_k x_k = 0\}$.

48. Représentations irréductibles

(1) Soient G et H des groupes. Soit ρ une représentation irréductible de H et soit $\pi : G \to H$ un morphisme de groupes surjectif. Montrer que $\rho \circ \pi$ est une représentation irréductible de G.
(2) Soient V une représentation irréductible de G. Montrer que pour toute représentation W de degré 1 de G, la représentation $V \otimes W$ est irréductible. Quand est-ce que $V \otimes W \simeq V$?

49. Représentations et sous-groupes distingués

Soit H un sous-groupe distingué d'un groupe fini G. On considère le groupe quotient G/H.

(1) Quel est le lien entre les représentations de G et celles de G/H ?
(2) Montrer que l'ensemble des représentations irréductibles de G/H s'identifie avec un sous-ensemble des représentations irréductibles de G.

50. Représentations de degré 1

(1) Montrer qu'un morphisme de groupe $G \to \mathbb{C}^*$ est à valeurs dans un sous-groupe des racines N-ième, lorsque G est fini.
(2) Déterminer tous les morphismes de groupes $\mathfrak{S}_n \to \mathbb{C}^*$.
(3) Déterminer tous les morphismes de groupes $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$.
(4) Déterminer tous les morphismes de groupes continus $(\mathbb{R}, +) \to \mathbb{C}^*$.
(5) Déterminer tous les morphismes de groupes continus $U(1) \to \mathbb{C}^*$

51. Dual d'un groupe abélien

Soit G un groupe fini. On note $\widehat{G} = \hom(G, \mathbb{C}^*)$.

(1) Supposons G abélien.
   — Montrer que $\widehat{G}$ est un groupe abélien fini isomorphe à G.

— Pour $\chi \in \widehat{G}$, calculer $\sum_{g\in G}\chi(g)$. *On calculera le produit* $\chi(h)\left(\sum_{g\in G}\chi(g)\right)$.

— Montrer que $\widehat{\widehat{G}}$ est canoniquement isomorphe à G.

(2) Dans le cas général, montrer que $\widehat{G}$ est isomorphe à l'abélianisé de G.

52. Produit hermitien invariant

Soit V une représentation *irréductible* d'un groupe fini G. On considère l'ensemble $\mathcal{H}$ formé des produit hermitiens $\Phi : V \times V \to \mathbb{C}$ qui sont G-invariants, c'est-à-dire tels que $\Phi(g \cdot v, g \cdot w) = \Phi(v, w)$ pour tous $g \in G$ et $v, w \in V$.

Montrer que tous les éléments de $\mathcal{H}$ sont proportionnels.

53. Produit tensoriel

Soient G_1 et G_2 deux groupes finis. Déterminer l'ensemble des représentations irréductibles de $G_1 \times G_2$ en fonction des représentations irréductibles de G_1 et G_2.

54. Caractères à valeurs réelles

(1) Montrer que si $\chi : \mathfrak{S}_n \to \mathbb{C}$ est le caractère d'une représentation de $\mathfrak{S}_n$, alors $\chi(\mathfrak{S}_n) \subset \mathbb{R}$.

(2) Soit V une représentation d'un groupe fini G de caractère χ. On note $V^* = \hom_{\mathbb{C}}(E, \mathbb{C})$ la représentation duale. Montrer que les représentations V et V^* sont isomorphes si et seulement si $\chi(G) \subset \mathbb{R}$.

55. Caractère de la représentation régulière

Soit G un groupe fini.

(1) Calculer le caractère de la représentation régulière de G.

(2) Soit χ_V le caractère d'une représentation de G vérifiant $\forall g \in G - \{e\}, \chi_V(g) = 0$. Montrer que $V \simeq m\mathbb{C}[G]$ pour un entier $m \in \mathbb{N}$.

56. Caractères de sous-représentations

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation complexe d'un groupe fini. On considère les sous-espaces vectoriels $\mathcal{S}_V$ et $\mathcal{A}_V$ de $V \otimes_{\mathbb{C}} V$ suivants :

$$\mathcal{S}_V = \mathrm{Vect}(v \otimes w + w \otimes v;\ v, w \in V\}, \qquad \mathcal{A}_V = \mathrm{Vect}(v \otimes w - w \otimes v;\ v, w \in V\}.$$

(1) Si $\{e_1, \ldots, e_n\}$ est une base de V, expliciter des bases respectives de $V \otimes_{\mathbb{C}} V$, $\mathcal{S}_V$ et $\mathcal{A}_V$.

(2) Montrer que $\mathcal{S}_V$ et $\mathcal{A}_V$ sont deux sous-représentations de $V \otimes_{\mathbb{C}} V$.

(3) Notons χ_V et $\chi_{\mathcal{S}}$ les caractères respectifs des représentations V et $\mathcal{S}_V$. Montrer que

$$\chi_{\mathcal{S}}(g) = \frac{1}{2}\left(\chi_V(g)^2 + \chi_V(g^2)\right), \qquad \forall g \in G.$$

On pourra utiliser une base de V qui diagonalise l'endomorphisme $\rho(g)$.

57. Représentations du groupe affine

Soit $p \geq 2$ un nombre premier. Le groupe affine Γ_p de $\mathbb{Z}/p\mathbb{Z}$ est formé des bijections de la forme

$$\begin{aligned} \phi_{a,b} : \mathbb{Z}/p\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ x &\longmapsto ax + b, \end{aligned}$$

où $a \in (\mathbb{Z}/p\mathbb{Z})^\times := \mathbb{Z}/p\mathbb{Z} - \{0\}$ et $b \in \mathbb{Z}/p\mathbb{Z}$.

(1) Calculer les expressions : $\phi_{a,b}^{-1}$, $\phi_{c,1} \circ \phi_{a,b} \circ \phi_{c,1}^{-1}$, et $\phi_{1,d} \circ \phi_{a,b} \circ \phi_{1,d}^{-1}$.

(2) Montrer que Γ_p possède p classes de conjugaison.

(3) Montrer que Γ_p possède $p-1$ représentations irréductibles complexes de dimension 1. *On utilisera le morphisme de groupe $\phi_{a,b} \mapsto a$ et le fait que le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Soit E l'espace vectoriel formé des fonctions $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$. On considère l'action linéaire de Γ_p sur E définie par la relation $(\phi_{a,b} \cdot f)(x) = f(a^{-1}x - a^{-1}b)$. On note $F \subset E$ le sous-espace vectoriel des fonctions f vérifiant $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} f(x) = 0$.

(4) Vérifier que F est une sous-représentation de E.
(5) Calculer les caractères χ_E et χ_F des représentations E et F.
(6) Montrer que F est une représentation irréductible de Γ_p.

58. Tables de caractères de petits groupes

(1) Soit $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions, avec les relations
$$i^2 = j^2 = k^2 = -1 \quad \text{et} \quad ij = k.$$
Calculer ses classes de conjugaison et sa table de caractères.
(2) Soit D_{2n} le groupe diédral, c'est-à-dire le groupe des isométries du polygone régulier à n côtés. On note s une symétrie de D_{2n} et r la rotation d'angle $\frac{2\pi}{n}$.
— Montrer que r et s engendrent D_{2n}, et que $srs^{-1} = r^{-1}$.
— Donner les classes de conjugaison de D_{2n}, en distinguant les cas où n est pair et impair.
— Calculer la table de caractères de D_{2n}, en distinguant encore ces cas. Que peut-on dire de celle de D_8 ?
(3) Calculer la table de caractères de $\mathfrak{A}_4$.

59. Représentations irréductibles du groupe $\mathfrak{A}_5$

Soit $\mathfrak{A}_5 \subset \mathfrak{S}_5$ le groupe alterné. On note $V_1 = \mathbb{C}$ la représentation triviale de $\mathfrak{A}_5$.

(1) Montrer que $\mathfrak{A}_5$ admet cinq classes de conjugaisons, celles de Id, (123), (12)(34), (12345) et (12354). Déterminer leur cardinaux respectifs.
(2) Soit χ_2 le caractère de la représentation de dimension 4 donnée par la permutation des coordonnées de l'hyperplan $V_2 = \{\sum_{i=1}^5 x_i = 0\} \subset \mathbb{C}^5$. Calculer le caractère χ_2 et en déduire que V_2 est une représentation irréductible de $\mathfrak{A}_5$.
(3) Soit $W \subset \mathbb{C}[X_1, X_2, X_3, X_4, X_5]$ le sous-espace des polynômes homogènes de degré 2. Le groupe $\mathfrak{A}_5$ agit linéairement sur W par permutation des variables.
— Exhiber une base de W et calculer le caractère χ_W.
— Calculer les multiplicités des représentations irréductibles V_1 et V_2 dans W.
— Montrer que W possède une sous-représentation irréductible de dimension 5.
(4) Quelle est la dimension des autres représentations irréductibles du groupe $\mathfrak{A}_5$?

60. Groupes simples

Soit G un groupe fini. À tout caractère χ_V d'une représentation V de G on associe $G_V := \{g \in G, \chi_V(g) = \chi_V(e)\}$.

(1) Montrer que G_V est un sous-groupe distingué de G.
(2) Exprimer $G_{V\oplus W}$ en fonction de G_V et G_W.
(3) Montrer que G est un groupe simple si et seulement si $G_V = \{e\}$ pour toute représentation irréductible V distincte de la représentation triviale.

61. Centre d'un groupe

On considère un groupe fini G. On note $Z(G)$ son centre et $|G|$ son cardinal.

(1) Montrer que pour toute représentation irréductible $\rho : G \to GL(V)$, il existe un morphisme de groupe $\lambda : Z(G) \to \mathbb{C} - \{0\}$ tel que $\rho(g) = \lambda(g) Id_V$, $\forall g \in Z(G)$.
(2) Considérons un élément $g_o \in G$ tel que pour toute representation irréductible $\rho : G \to GL(V)$, l'endomorphisme $\rho(g_o)$ est une homothétie. Montrer que $g_o \in Z(G)$. *On utilisera la représentation régulière de G.*
(3) Soient $\chi_1, \cdots, \chi_r$ les caractères des représentations irréductibles complexes de G. Montrer que

$$Z(G) = \Big\{ g \in G,\ \sum_{j=1}^{r} \chi_j(g)\overline{\chi_j(g)} = |G| \Big\}.$$

62. Transformation de Fourier discrète, côté théorique

Soit G un groupe abélien fini. On munit $\mathbb{C}[G]$ du produit Hermitien $\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$.

Soient $\widehat{G}$ le groupe dual et $\mathbb{C}[\widehat{G}]$ l'algèbre associée. On définit une application $\phi \in \mathbb{C}[G] \to \widehat{\phi} \in \mathbb{C}[\widehat{G}]$ en posant $\widehat{\phi}(\chi) = \langle \phi, \chi \rangle, \forall \chi \in \widehat{G}$.

(1) Montrer que la représentation régulière de G est unitaire : $\langle g \cdot \phi, g \cdot \psi \rangle = \langle \phi, \psi \rangle$, $\forall g \in G$.
(2) Montrer que $(\chi)_{\chi \in \widehat{G}}$ est une base orthonormée de $(\mathbb{C}[G], \langle -, - \rangle)$.
(3) Montrer que $\phi \to \widehat{\phi}$ est un isomorphisme de G-représentations pour une structure de représentation sur $\mathbb{C}[\widehat{G}]$ à expliciter.
(4) (*Inversion*) Montrer que pour tout $\phi \in \mathbb{C}[\widehat{G}]$, on a $\phi = \sum_{\chi \in \widehat{G}} \widehat{\phi}(\chi)\chi$.
(5) (*Convolution*) Montrer que $\widehat{\phi \star \psi} = |G| \widehat{\phi}\,\widehat{\psi}$.

63. Transformation de Fourier discrète, côté pratique

On travaille avec le groupe $G = \mathbb{Z}/n\mathbb{Z}$. À un polynôme $P \in \mathbb{C}[X]$, on associe la fonction $\phi_P \in \mathbb{C}[G]$ définie par $\phi_P(\overline{k}) := \frac{1}{k!} \frac{d^k}{dX^k}(P)(0)$, pour $0 \leq k \leq n-1$.

(1) Montrer que $\widehat{G}$ est canoniquement isomorphe au groupe des racines n-ièmes de l'unité.
(2) Expliciter la transformation de Fourier discrète.
(3) Calculer $\widehat{\phi_P}$ en fonction du polynôme P, lorsque $d^o P \leq n-1$.
(4) Soient $P, Q \in \mathbb{C}[X]$ des polynômes de degré au plus $\frac{n}{2} - 1$. Calculer le produit PQ au moyen de la transformation de Fourier discrète.