Plaquette 4 – Quotients de K[X], corps finis et algèbres

Structures algébriques — Prépa MP / MPI (2e année)

Exercices

Méthode

L'anneau $\mathrm{K}[X]/(P)$ se calcule comme les entiers modulo n : on représente chaque classe par le **reste** de la division par P (de degré $< \deg P$), on multiplie puis on réduit avec la relation $P(\alpha) = 0$. C'est un **corps** si et seulement si P est **irréductible** ; on y inverse un élément par une relation de Bézout. Cette construction fabrique $\mathbb{C}$ à partir de $\mathbb{R}$, $\mathbb{Q}(\sqrt{2})$ à partir de $\mathbb{Q}$, et les corps finis F_4, F_8, F_9. Côté algèbres, $\mathrm{K}[A]$ (polynômes en une matrice A) est isomorphe à $\mathrm{K}[X]/(\mu_A)$, où μ_A engendre l'idéal annulateur.

Exercice 1 – Construire C à partir de R

Soit $A = \mathbb{R}[X]/(X^2+1)$ et α la classe de X.

a) Montrer que tout élément de A s'écrit de façon unique $a + b\alpha$ avec a, b réels, et calculer $(a+b\alpha)(c+d\alpha)$.

b) Montrer que $\Phi : A \to \mathbb{C}$, $a + b\alpha \mapsto a + ib$ est un isomorphisme d'anneaux.

c) Pourquoi $\mathbb{R}[X]/(X^2-1)$ n'est-il pas un corps ?

Exercice 2 – Le corps à quatre éléments

Soit $F = \mathrm{F}_2[X]/(X^2+X+1)$ et α la classe de X.

a) Montrer que X^2+X+1 est irréductible sur F_2.

b) Lister les 4 éléments de F et dresser la table de multiplication (utiliser $\alpha^2 = \alpha + 1$).

c) Montrer que $F^\times$ est cyclique d'ordre 3, engendré par α.

d) Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à F.

Exercice 3 – Inverser dans Q(racine de 2)

Soit $A = \mathbb{Q}[X]/(X^2-2)$ et α la classe de X.

a) Montrer que A est un corps et que $a + b\alpha \mapsto a + b\sqrt{2}$ est un isomorphisme de A sur $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

b) Inverser $1 + \alpha$ par une relation de Bézout entre $X^2 - 2$ et $X + 1$.

c) Inverser $3 + 2\alpha$ et vérifier par la quantité conjuguée.

Exercice 4 – Le corps à huit éléments

Soit $P = X^3 + X + 1 \in \mathrm{F}_2[X]$ et $F = \mathrm{F}_2[X]/(P)$, α la classe de X.

a) Montrer que P est irréductible, puis que F est un corps à 8 éléments.

b) Calculer α^k pour $3 \le k \le 7$ sous la forme $a + b\alpha + c\alpha^2$.

c) En déduire que $F^\times$ est cyclique, engendré par α.

d) Montrer que α^2 et α^4 sont aussi racines de P, et factoriser P dans $F[X]$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 5 – Un quotient qui n'est pas un corps

Soit $A = \mathbb{Q}[X]/(X^2 - 1)$.

a) Montrer que A possède des diviseurs de zéro.

b) Expliciter l'isomorphisme chinois $A \simeq \mathbb{Q} \times \mathbb{Q}$, $P(\alpha) \mapsto (P(1), P(-1))$.

c) Déterminer les idempotents de A et leurs images.

d) Inverser $2 + \alpha$ dans A.

Exercice 6 – Restes chinois pour les polynômes

Soient $a \neq b$ réels.

a) Montrer que le reste R de la division d'un polynôme P par $(X-a)(X-b)$ est l'unique polynôme de degré ≤ 1 prenant les valeurs $P(a)$ en a et $P(b)$ en b.

b) Calculer le reste de la division de X^{10} par $X^2 - 3X + 2$.

c) Calculer le reste de la division de X^{10} par $(X-1)^2$ (utiliser $P(1)$ et $P'(1)$).

Exercice 7 – Factoriser X⁴ + 1 selon le corps

a) Factoriser $X^4 + 1$ dans $\mathbb{C}[X]$ (racines huitièmes de l'unité d'ordre 8).

b) En déduire sa factorisation dans $\mathbb{R}[X]$.

c) Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ (pas de racine rationnelle, et étudier les factorisations en deux facteurs de degré 2 à l'aide de b)).

d) Vérifier que dans $\mathrm{F}_3[X]$: $X^4 + 1 = (X^2 + X + 2)(X^2 + 2X + 2)$.

Exercice 8 – Polynôme minimal et algèbre K[A]

a) Pour $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, montrer que $(A - I_2)^2 = 0$ et que $A - I_2 \neq 0$. En déduire le polynôme minimal μ_A.

b) Montrer que $\mathbb{R}[A] = \mathrm{Vect}(I_2, A)$ et que $\mathbb{R}[A] \simeq \mathbb{R}[X]/((X-1)^2)$. Est-ce un corps ?

c) Calculer A^n en divisant X^n par $(X-1)^2$.

d) Pour un projecteur $p \neq 0, \mathrm{id}$, déterminer μ_p et $\dim \mathrm{K}[p]$.

Exercice 9 – L'algèbre engendrée par la matrice J

Soit $J \in M_3(\mathbb{R})$ la matrice dont tous les coefficients valent 1.

a) Montrer que $J^2 = 3J$ et déterminer μ_J.

b) Décrire $\mathbb{R}[J]$ et sa dimension. Est-elle isomorphe à $\mathbb{R}^2$?

c) Montrer que $J - I_3$ est inversible et calculer son inverse dans $\mathbb{R}[J]$.

d) Calculer $(J - I_3)^n$.

Exercice 10 – Polynômes irréductibles de degré 2 sur Fp

Soit p premier.

a) Combien y a-t-il de polynômes unitaires de degré 2 dans $\mathrm{F}_p[X]$?

b) Combien sont réductibles (de la forme $(X-a)(X-b)$, $a, b \in \mathrm{F}_p$) ?

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) En déduire qu'il y a $\frac{p(p-1)}{2}$ polynômes unitaires irréductibles de degré 2, et les lister pour $p = 2$ et $p = 3$.
d) En déduire l'existence d'un corps à p^2 éléments pour tout p.

Exercice 11 – Le polynôme X^p − X sur Fp

Soit p premier.

a) Montrer que tout $a \in \mathrm{F}_p$ est racine de $X^p - X$ (Fermat), et en déduire $X^p - X = \prod_{a \in \mathrm{F}_p} (X - a)$.

b) En comparant les coefficients de X dans $X^{p-1} - 1 = \prod_{a \neq 0} (X - a)$, retrouver le théorème de Wilson.
c) Vérifier la factorisation pour $p = 3$.
d) En déduire que le produit des éléments non nuls de F_p vaut -1, et que $\sum_{a \in \mathrm{F}_p} a = 0$ pour p impair.

Exercice 12 – Le corps à neuf éléments

Soit $F = \mathrm{F}_3[X]/(X^2 + 1)$ et α la classe de X.

a) Montrer que F est un corps à 9 éléments.
b) Calculer l'ordre de α dans $F^\times$. Engendre-t-il $F^\times$?
c) Calculer $(1 + \alpha)^2$, $(1 + \alpha)^4$ et en déduire que $1 + \alpha$ engendre $F^\times$.
d) Combien $F^\times$ a-t-il de générateurs ?

Exercice 13 – Inverser dans un corps de nombres de degré 3

Soit $A = \mathbb{Q}[X]/(X^3 - 2)$ et α la classe de X (on identifie α à $\sqrt[3]{2}$).

a) Montrer que $X^3 - 2$ est irréductible sur $\mathbb{Q}$, donc que A est un corps de dimension 3.
b) Diviser $X^3 - 2$ par $X + 1$ et en déduire l'inverse de $1 + \alpha$.
c) Vérifier numériquement : $\frac{1}{1 + \sqrt[3]{2}}$ et $\frac{\sqrt[3]{4} - \sqrt[3]{2} + 1}{3}$.

Exercice 14 – Morphisme d'évaluation et idéal annulateur

Soit $u \in L(E)$ (E de dimension finie n) et $\varphi : \mathrm{K}[X] \to L(E)$, $P \mapsto P(u)$.

a) Montrer que φ est un morphisme d'algèbres et que son noyau est un idéal non nul (considérer $\mathrm{id}, u, \ldots, u^{n^2}$).
b) En déduire l'existence et l'unicité du polynôme minimal μ_u, unitaire, générateur du noyau.
c) Montrer que u est inversible si et seulement si $\mu_u(0) \neq 0$, et exprimer alors u^{-1} comme polynôme en u.
d) Application : $\mu_u = X^2 - 3X + 2$. Exprimer u^{-1}.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 15 – Synthèse : racines de X² + X + 1 dans les corps finis

Soit p un nombre premier différent de 3 et $\Phi = X^2 + X + 1$.

a) Montrer que les racines de Φ dans un corps sont exactement les éléments d'ordre 3 du groupe multiplicatif.

b) En déduire que Φ a une racine dans F_p si et seulement si $3 \mid p-1$ (utiliser que $\mathrm{F}_p^\times$ est cyclique d'ordre $p-1$).

c) Vérifier pour $p = 7$ (racines ?) et $p = 5$.

d) Pour $p = 2$, retrouver le corps F_4.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).