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

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

Corrections détaillées

Boîte à outils

Quotients de $\mathrm{K}[X]$**.**

— $\mathrm{K}[X]/(P)$ ($\deg P = n$) est un K-espace de dimension n, de base $1, \alpha, \ldots, \alpha^{n-1}$ où α est la classe de X et $P(\alpha) = 0$.

— $\mathrm{K}[X]/(P)$ est un corps $\Leftrightarrow$ P irréductible ; inverse de $Q(\alpha)$ si $P \wedge Q = 1$: $UP + VQ = 1$ donne $Q(\alpha)^{-1} = V(\alpha)$.

— **Théorème chinois** : si $P \wedge Q = 1$, $\mathrm{K}[X]/(PQ) \simeq \mathrm{K}[X]/(P) \times \mathrm{K}[X]/(Q)$.

— En degré 2 ou 3, P est irréductible sur K si et seulement s'il n'a pas de racine dans K.

— Dans $\mathrm{F}_p[X]$: $X^p - X = \prod_{a \in \mathrm{F}_p} (X - a)$.

— **Algèbre** $\mathrm{K}[A]$: $P \mapsto P(A)$ est un morphisme d'algèbres de noyau (μ_A), et

$$\mathrm{K}[A] \simeq \mathrm{K}[X]/(\mu_A), \qquad \dim \mathrm{K}[A] = \deg \mu_A$$

Correction de l'exercice 1 – Construire C à partir de R

a) La classe d'un polynôme est celle de son reste dans la division par $X^2 + 1$, de degré ≤ 1, unique. Avec $\alpha^2 = -1$:

$$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd\alpha^2 = (ac - bd) + (ad + bc)\alpha$$

b) Φ est une bijection $\mathbb{R}$-linéaire ; elle respecte le produit car la formule de a) est celle de la multiplication des complexes ($i^2 = -1$), et $\Phi(1) = 1$. C'est la construction algébrique de $\mathbb{C}$: $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$, corps car $X^2 + 1$ est irréductible sur $\mathbb{R}$.

c) $X^2 - 1 = (X - 1)(X + 1)$: $(\alpha - 1)(\alpha + 1) = 0$ avec deux facteurs non nuls, diviseurs de zéro. (Par le théorème chinois, cet anneau est isomorphe à $\mathbb{R} \times \mathbb{R}$.)

Réponse. $(a + b\alpha)(c + d\alpha) = (ac - bd) + (ad + bc)\alpha$; $A \simeq \mathbb{C}$; $\mathbb{R}[X]/(X^2 - 1) \simeq \mathbb{R}^2$, non intègre.

Correction de l'exercice 2 – Le corps à quatre éléments

a) Degré 2 sans racine dans F_2 ($0 + 0 + 1 = 1$, $1 + 1 + 1 = 1$) : irréductible. Donc F est un corps.

b) Éléments : $0, 1, \alpha, \alpha + 1$. Avec $\alpha^2 = -\alpha - 1 = \alpha + 1$ (caractéristique 2) :

$$\alpha \cdot \alpha = \alpha + 1, \quad \alpha(\alpha + 1) = \alpha^2 + \alpha = 1, \quad (\alpha + 1)^2 = \alpha^2 + 1 = \alpha$$

— et 1 est neutre, 0 absorbant.

c) $\alpha^1 = \alpha$, $\alpha^2 = \alpha + 1$, $\alpha^3 = \alpha(\alpha + 1) = 1$: $F^\times = \{1, \alpha, \alpha^2\}$ est cyclique d'ordre 3.

d) $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre ($\overline{2} \times \overline{2} = \overline{0}$) ; de plus F est de caractéristique 2 ($x + x = 0$) alors que $\overline{1} + \overline{1} = \overline{2} \neq \overline{0}$. Il existe un corps à 4 éléments, mais ce n'est pas $\mathbb{Z}/4\mathbb{Z}$.

Réponse. $F = \{0, 1, \alpha, \alpha + 1\}$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$; $F \simeq \mathbb{Z}/4\mathbb{Z}$.

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).

Correction de l’exercice 3 – Inverser dans Q(racine de 2)

a) X^2-2 n’a pas de racine rationnelle ($\sqrt{2}\notin\mathbb{Q}$), donc est irréductible sur $\mathbb{Q}$ (degré 2) : A est un corps. L’évaluation $P\mapsto P(\sqrt{2})$ est un morphisme $\mathbb{Q}[X]\to\mathbb{R}$, de noyau (X^2-2) (polynôme minimal de $\sqrt{2}$), d’image $\mathbb{Q}(\sqrt{2})$; le théorème d’isomorphisme conclut.

b) Division : $X^2-2=(X+1)(X-1)-1$, donc

$$(X+1)(X-1)-(X^2-2)=1$$

— et dans A : $(1+\alpha)(\alpha-1)=1$, soit $(1+\alpha)^{-1}=\alpha-1$ (c’est $\sqrt{2}-1$).

c) $(3+2\alpha)(3-2\alpha)=9-4\alpha^2=9-8=1$: $(3+2\alpha)^{-1}=3-2\alpha$.

Réponse. $A\simeq\mathbb{Q}(\sqrt{2})$; $(1+\alpha)^{-1}=\alpha-1$; $(3+2\alpha)^{-1}=3-2\alpha$.

Correction de l’exercice 4 – Le corps à huit éléments

a) $P(0)=1$, $P(1)=1$: pas de racine, et en degré 3 cela suffit. F est un corps, de base $1,\alpha,\alpha^2$ sur F_2 : $2^3=8$ éléments.

b) Avec $\alpha^3=\alpha+1$:

$$\alpha^4=\alpha^2+\alpha,\quad \alpha^5=\alpha^3+\alpha^2=\alpha^2+\alpha+1,\quad \alpha^6=\alpha^3+\alpha^2+\alpha=\alpha^2+1,\quad \alpha^7=\alpha^3+\alpha=1$$

c) α est d’ordre 7 (premier, et $\alpha\neq1$) : il engendre $F^\times$, de cardinal 7. Les 7 puissances listées sont les 7 éléments non nuls.

d) Par le Frobenius, $P(\alpha^2)=P(\alpha)^2=0$ (coefficients dans F_2), de même $P(\alpha^4)=0$. Vérification : $\alpha^6+\alpha^2+1=(\alpha^2+1)+\alpha^2+1=0$. Les trois racines sont distinctes, d’où

— $P=(X-\alpha)(X-\alpha^2)(X-\alpha^4)$ dans $F[X]$.

Réponse. $\alpha^3=\alpha+1$ et $\alpha^7=1$; $F^\times=\langle\alpha\rangle$; $P=(X-\alpha)(X-\alpha^2)(X-\alpha^4)$.

Correction de l’exercice 5 – Un quotient qui n’est pas un corps

a) $(\alpha-1)(\alpha+1)=\alpha^2-1=0$ avec $\alpha\pm1\neq0$ (restes de degré 1).

b) Le morphisme $P\mapsto(P(1),P(-1))$ de $\mathbb{Q}[X]$ dans $\mathbb{Q}^2$ est surjectif (interpolation) de noyau les multiples de $(X-1)(X+1)$; d’où l’isomorphisme

$$\mathbb{Q}[X]/(X^2-1)\simeq\mathbb{Q}\times\mathbb{Q}$$

c) Idempotents de $\mathbb{Q}^2$: $(0,0)$, $(1,1)$, $(1,0)$, $(0,1)$. Antécédents de degré ≤1 : 0, 1, $\frac{1+\alpha}{2}$ et $\frac{1-\alpha}{2}$. Contrôle : $\left(\frac{1+\alpha}{2}\right)^2=\frac{1+2\alpha+1}{4}=\frac{1+\alpha}{2}$.

d) Image de $2+\alpha$: $(3,1)$, d’inverse $\left(\frac{1}{3},1\right)$, dont l’antécédent $a+b\alpha$ vérifie $a+b=\frac{1}{3}$, $a-b=1$: $a=\frac{2}{3}$, $b=-\frac{1}{3}$. $(2+\alpha)^{-1}=\frac{2-\alpha}{3}$; contrôle : $(2+\alpha)(2-\alpha)=4-1=3$.

Réponse. Diviseurs de zéro $\alpha\pm1$; $A\simeq\mathbb{Q}^2$; idempotents $0,1,\frac{1\pm\alpha}{2}$; $(2+\alpha)^{-1}=\frac{2-\alpha}{3}$.

Correction de l’exercice 6 – Restes chinois pour les polynômes

a) $P=(X-a)(X-b)Q+R$ avec $\deg R\le1$; en évaluant en a et b : $R(a)=P(a)$, $R(b)=P(b)$. Un polynôme de degré ≤1 est déterminé par deux valeurs (interpolation) :

$$R=P(a)\frac{X-b}{a-b}+P(b)\frac{X-a}{b-a}$$

b) $X^2-3X+2=(X-1)(X-2)$, $P(1)=1$, $P(2)=1\,024$:
$R=1\times\frac{X-2}{-1}+1\,024(X-1)=1\,023X-1\,022$. Contrôle : $R(1)=1$, $R(2)=1\,024$.

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) $(X-1)^2$: $R = P(1) + P'(1)(X-1) = 1 + 10(X-1) = 10X - 9$ (Taylor à l'ordre 1 en 1, car $(X-1)^2$ divise le reste de Taylor).

Réponse. R interpole P en a, b ; $X^{10} \bmod (X-1)(X-2) = 1023X - 1022$; $\bmod (X-1)^2$: $10X - 9$.

Correction de l'exercice 7 – Factoriser X⁴ + 1 selon le corps

a) Les racines sont les z avec $z^4 = -1$: $\mathrm{e}^{i\pi/4}$, $\mathrm{e}^{3i\pi/4}$, $\mathrm{e}^{5i\pi/4}$, $\mathrm{e}^{7i\pi/4}$, et $X^4 + 1 = \prod (X - z_k)$.

b) On regroupe les racines conjuguées : $(X - \mathrm{e}^{i\pi/4})(X - \mathrm{e}^{-i\pi/4}) = X^2 - \sqrt{2}X + 1$; de même avec $\mathrm{e}^{\pm 3i\pi/4}$:

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

c) Pas de racine réelle, donc pas de facteur de degré 1. Un facteur unitaire de degré 2 dans $\mathbb{Q}[X]$ serait aussi un facteur dans $\mathbb{R}[X]$, donc (unicité de la factorisation en irréductibles de $\mathbb{R}[X]$) l'un des deux facteurs de b), à coefficients irrationnels. Donc $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

d) $(X^2 + X + 2)(X^2 + 2X + 2) = X^4 + 3X^3 + 6X^2 + 6X + 4 \equiv X^4 + 1 \pmod 3$. Irréductible sur $\mathbb{Q}$, il peut se factoriser modulo un nombre premier.

Réponse. $\mathbb{R}$: $(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$; irréductible sur $\mathbb{Q}$; réductible sur F_3.

Correction de l'exercice 8 – Polynôme minimal et algèbre K[A]

a) $A - I_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, de carré nul. μ_A divise $(X-1)^2$, est unitaire, et n'est pas $X - 1$: $\mu_A = (X-1)^2$.

b) L'évaluation $P \mapsto P(A)$ a pour noyau (μ_A) ; par le théorème d'isomorphisme,

$$\mathbb{R}[A] \simeq \mathbb{R}[X]/((X-1)^2), \qquad \dim \mathbb{R}[A] = 2$$

— de base I_2, A. Pas un corps : $A - I_2$ est nilpotent non nul.

c) Reste de X^n modulo $(X-1)^2$: $1 + n(X-1)$ (exercice précédent). Donc $A^n = I_2 + n(A - I_2) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

d) $p^2 = p$: $\mu_p \mid X^2 - X = X(X-1)$; ni X ($p \neq 0$) ni $X - 1$ ($p \neq \mathrm{id}$) : $\mu_p = X^2 - X$, et $\dim \mathrm{K}[p] = 2$ ($\mathrm{K}[p] = \mathrm{Vect}(\mathrm{id}, p) \simeq \mathrm{K}^2$).

Réponse. $\mu_A = (X-1)^2$; $\mathbb{R}[A] \simeq \mathbb{R}[X]/((X-1)^2)$, pas un corps ; $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$; $\mu_p = X^2 - X$.

Correction de l'exercice 9 – L'algèbre engendrée par la matrice J

a) Chaque coefficient de J^2 vaut $1 + 1 + 1 = 3$. $\mu_J \mid X^2 - 3X = X(X-3)$, et $J \neq 0$, $J \neq 3I_3$: $\mu_J = X(X-3)$.

b) $\mathbb{R}[J] = \mathrm{Vect}(I_3, J)$, de dimension 2, isomorphe à $\mathbb{R}[X]/(X(X-3)) \simeq \mathbb{R} \times \mathbb{R}$ (théorème chinois, $X \wedge (X-3) = 1$).

c) $J^2 - 3J = 0$ s'écrit $(J - I_3)(J - 2I_3) = J^2 - 3J + 2I_3 = 2I_3$, donc

$$(J - I_3)^{-1} = \frac{1}{2}(J - 2I_3)$$

d) Par l'isomorphisme, $J - I_3$ correspond au couple $(0-1, 3-1) = (-1, 2)$; en

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).

interpolant : $(J-I_3)^n = (-1)^n I_3 + \frac{2^n-(-1)^n}{3}J$. Contrôle $n=1$: $-I_3+J$.

Réponse. $\mu_J = X(X-3)$; $\mathbb{R}[J] \simeq \mathbb{R}^2$; $(J-I_3)^{-1} = \frac{1}{2}(J-2I_3)$; $(J-I_3)^n = (-1)^n I_3 + \frac{2^n-(-1)^n}{3}J$.

Correction de l'exercice 10 – Polynômes irréductibles de degré 2 sur Fp

a) X^2+aX+b : p^2 polynômes.

b) Un polynôme réductible unitaire de degré 2 est déterminé par la paire non ordonnée $\{a,b\}$ de ses racines (éventuellement égales) : $\binom{p}{2}+p = \frac{p(p+1)}{2}$.

c) Irréductibles :

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$$

— $p=2$: 1 polynôme, X^2+X+1. $p=3$: 3 polynômes sans racine dans F_3 : X^2+1, X^2+X+2, X^2+2X+2 (on vérifie qu'aucun ne s'annule en 0, 1, 2).

d) Pour P irréductible de degré 2, $\mathrm{F}_p[X]/(P)$ est un corps de dimension 2 sur F_p : p^2 éléments.

Réponse. p^2 unitaires, $\frac{p(p+1)}{2}$ réductibles, $\frac{p(p-1)}{2}$ irréductibles ; corps à p^2 éléments.

Correction de l'exercice 11 – Le polynôme X^p − X sur Fp

a) $a^p = a$ dans F_p (petit Fermat, vrai aussi pour $a=0$). Le polynôme unitaire X^p-X, de degré p, a p racines distinctes : il est égal au produit des $X-a$.

b) Pour p impair, en divisant par X : $X^{p-1}-1 = \prod_{a\neq 0}(X-a)$. Le coefficient constant donne

$$-1 = \prod_{a\neq 0}(-a) = (-1)^{p-1}(p-1)! = (p-1)!$$

— car $p-1$ est pair : $(p-1)! \equiv -1 \pmod p$.

c) $X(X-1)(X-2) = X(X^2-3X+2) \equiv X(X^2+2) = X^3+2X \equiv X^3-X \pmod 3$.

d) Le produit est le coefficient constant de b) au signe près : -1. La somme des racines de X^p-X est l'opposé du coefficient de X^{p-1}, nul pour $p \geq 3$.

Réponse. $X^p-X = \prod_a (X-a)$; Wilson par le coefficient constant ; somme des éléments nulle.

Correction de l'exercice 12 – Le corps à neuf éléments

a) X^2+1 n'a pas de racine dans F_3 ($0+1$, $1+1$, $4+1 \equiv 2$, tous non nuls) : irréductible. F est un corps de dimension 2 sur F_3 : 9 éléments.

b) $\alpha^2=-1$, $\alpha^4=1$: α est d'ordre 4, alors que $\mathrm{card} F^\times = 8$. Il n'engendre pas.

c) $(1+\alpha)^2 = 1+2\alpha+\alpha^2 = 2\alpha$, puis $(1+\alpha)^4 = 4\alpha^2 = -4 = 2 \neq 1$. L'ordre de $1+\alpha$ divise 8, n'est ni 1, ni 2, ni 4 : il vaut 8.

$$F^\times = \langle 1+\alpha \rangle \simeq \mathbb{Z}/8\mathbb{Z}$$

d) $\varphi(8)=4$ générateurs : $(1+\alpha)^k$ pour $k \in \{1,3,5,7\}$.

Réponse. F corps à 9 éléments ; $\mathrm{ord}\alpha = 4$; $1+\alpha$ d'ordre 8 ; 4 générateurs.

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).

Correction de l’exercice 13 – Inverser dans un corps de nombres de degré 3

a) Degré 3 : irréductible si et seulement si sans racine rationnelle. Une racine $\frac{p}{q}$ (fraction irréductible) vérifierait $p^3 = 2q^3$, d’où p pair, puis q pair : contradiction. Donc A est un corps de base $1, \alpha, \alpha^2$.

b) $X^3 - 2 = (X+1)(X^2 - X + 1) - 3$, donc dans A :

$$(1+\alpha)(\alpha^2 - \alpha + 1) = 3, \qquad (1+\alpha)^{-1} = \frac{\alpha^2 - \alpha + 1}{3}$$

c) $\sqrt[3]{2} \approx 1{,}2599$: $\frac{1}{2{,}2599} \approx 0{,}4425$ et $\frac{1{,}5874 - 1{,}2599 + 1}{3} = \frac{1{,}3275}{3} \approx 0{,}4425$.

Réponse. $(1+\alpha)^{-1} = \frac{\alpha^2 - \alpha + 1}{3}$, soit $\frac{1}{1+\sqrt[3]{2}} = \frac{\sqrt[3]{4} - \sqrt[3]{2} + 1}{3}$.

Correction de l’exercice 14 – Morphisme d’évaluation et idéal annulateur

a) $(PQ)(u) = P(u) \circ Q(u)$ et $(\lambda P + Q)(u) = \lambda P(u) + Q(u)$, $1(u) = \mathrm{id}$. Les $n^2 + 1$ endomorphismes u^k ($0 \le k \le n^2$) sont liés dans $L(E)$, de dimension n^2 : une combinaison non triviale s’annule, d’où un polynôme non nul dans le noyau.

b) Le noyau est un idéal non nul de $\mathrm{K}[X]$, principal : il a un unique générateur unitaire, μ_u.

c) Écrivons $\mu_u = XQ + c$ avec $c = \mu_u(0)$. Si $c \neq 0$: $u \circ Q(u) = -c\,\mathrm{id}$, donc

$$u^{-1} = -\frac{1}{\mu_u(0)} Q(u)$$

— Si $c = 0$: $u \circ Q(u) = 0$ avec $Q(u) \neq 0$ (car $\deg Q < \deg \mu_u$), donc u n’est pas injectif.

d) $u^2 - 3u + 2\,\mathrm{id} = 0$, donc $u(3\,\mathrm{id} - u) = 2\,\mathrm{id}$ et $u^{-1} = \frac{1}{2}(3\,\mathrm{id} - u)$.

Réponse. $\ker \varphi = (\mu_u)$; u inversible ssi $\mu_u(0) \neq 0$; d) $u^{-1} = \frac{1}{2}(3\,\mathrm{id} - u)$.

Correction de l’exercice 15 – Synthèse : racines de X² + X + 1 dans les corps finis

a) $X^3 - 1 = (X-1)\Phi$. Une racine x de Φ vérifie $x^3 = 1$; et $x \neq 1$ car $\Phi(1) = 3 \neq 0$ ($p \neq 3$) : x est d’ordre 3. Réciproquement, si x est d’ordre 3, $(x-1)\Phi(x) = 0$ avec $x \neq 1$, donc $\Phi(x) = 0$.

b) Dans le groupe cyclique $\mathrm{F}_p^\times$ d’ordre $p - 1$, il existe un élément d’ordre 3 si et seulement si $3 \mid p - 1$ (un unique sous-groupe d’ordre d pour chaque diviseur d).

c) $p = 7$: $3 \mid 6$; racines 2 et 4 ($4 + 2 + 1 = 7 \equiv 0$, $16 + 4 + 1 = 21 \equiv 0$). $p = 5$: $3 \nmid 4$, pas de racine (Φ prend les valeurs $1, 3, 2, 3, 1$ en $0, \dots, 4$) ; Φ est irréductible sur F_5, et $\mathrm{F}_5[X]/(\Phi)$ est un corps à 25 éléments.

d) $p = 2$: $3 \nmid 1$, Φ irréductible et $\mathrm{F}_2[X]/(\Phi) = \mathrm{F}_4$, dont les éléments α et α^2 sont d’ordre 3, racines de Φ.

Réponse. Racines = éléments d’ordre 3 ; racine dans F_p ssi $3 \mid p - 1$; $p = 7$: $2, 4$; $p = 5$: aucune.

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).