

TD6 : Corps finis

M1 MIC – Algèbre

Année 2025–2026

Exercice 1. Existe-t-il un corps à 8 éléments ? 9 éléments ? 12 éléments ?

Exercice 2. Soit q, q' deux puissances de nombres premiers. À quelle condition le corps $\mathbb{F}_{q'}$ est-il une extension de $\mathbb{F}_q$?

Exercice 3. (a) Déterminer tous les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.

(b) Pourquoi les anneaux $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ et $\mathbb{F}_2[X]/(X^4 + X + 1)$ sont-ils isomorphes ?

(c) Calculer l'ordre multiplicatif de la classe de X dans chacun de ces quotients.

(d) Construire un isomorphisme explicite.

Exercice 4. (a) Quels sont les sous-corps de $\mathbb{F}_{64}$?

(b) Combien existe-t-il de générateurs de l'extension $\mathbb{F}_2 \subset \mathbb{F}_{64}$, c'est-à-dire d'éléments $x \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(x)$?

(c) Combien le groupe $\mathbb{F}_{64}^\times$ a-t-il de générateurs ?

(d) Est-ce qu'il y a un lien entre ces deux notions ?

Exercice 5. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie de corps.

(a) Si $[\mathbb{L} : \mathbb{K}]$ est un nombre premier, démontrer que l'extension est monogène.

(b) Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Démontrer que si $\deg(P)$ et $[\mathbb{L} : \mathbb{K}]$ sont premiers entre eux, alors P est irréductible sur $\mathbb{L}$.

(c) Soit $\alpha \in \mathbb{K}$ un élément algébrique de degré impair. Démontrer que $\mathbb{K}(\alpha) = \mathbb{K}(\alpha^2)$.

Exercice 6. Corps à huit, neuf et seize éléments.

(a) Dresser une liste de tous les polynômes irréductibles de degré inférieur ou égal à 4 sur les corps $\mathbb{F}_2$ et $\mathbb{F}_3$.

(b) Parmi les polynômes précédents, lesquels ont pour corps de rupture $\mathbb{F}_9$ et $\mathbb{F}_8$? écrire la table de multiplication du corps correspondant dans ces cas.

(c) Donner des isomorphismes explicites entre les corps ainsi obtenus.

(d) Dans chacun des cas, est-ce que l'élément primitif canonique (la classe de X dans le quotient $\mathbb{K}[X]/(P)$) est un générateur du groupe multiplicatif du corps ?

(e) Démontrer que $\mathbb{F}_8^\times$ est cyclique.

(f) Démontrer que tous les éléments de $\mathbb{F}_8$ sont algébriques sur $\mathbb{F}_2$ et donner leurs polynômes minimaux.

(g) Reprendre les trois dernières questions en remplaçant $\mathbb{F}_8$ par $\mathbb{F}_{16}$.

Exercice 7. Soit p un nombre premier et a un nombre premier avec p . On veut démontrer que le polynôme $P = X^p - X - a$ est irréductible sur $\mathbb{F}_p$ et sur $\mathbb{Q}$.

(a) Soit $\mathbb{K}$ une extension de $\mathbb{F}_p$ dans laquelle P possède une racine notée α . Démontrer que les racines de P dans $\mathbb{K}$ sont $\alpha, \alpha + 1, \dots, \alpha + p - 1$.

(b) Soit $U \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire de degré $d \geq 1$ qui divise P . Démontrer que P est divisible par $U(X + j)$ pour tout $j \in \{0, \dots, p - 1\}$.

(c) En déduire que $d = p$ et donc que $U = P$. On pourra distinguer le cas où les $U(X + j)$ sont deux à deux distincts et le cas où $U(X + j) = U(X + k)$ avec $j \neq k$.

(d) En déduire que P est irréductible sur $\mathbb{F}_p$, puis sur $\mathbb{Q}$.

Exercice 8. (a) Le nombre 2 est-il un carré dans $\mathbb{F}_5$?

- (b) Démontrer que $P = X^2 + X + 1$ est irréductible dans $\mathbb{F}_5[X]$.
- (c) Quelle est la caractéristique de $\mathbb{F}_{25}$?
- (d) Démontrer que le quotient $\mathbb{F}_5[X]/(P)$ est isomorphe à $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.
- (e) On note α une racine de P dans $\mathbb{F}_{25}$. Démontrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire de manière unique sous la forme $\beta = x + \alpha y$ avec $x, y \in \mathbb{F}_5$.
- (f) Soit $Q = X^5 - X + 1$. Déterminer $c, d \in \mathbb{F}_5$ tels que $Q(\alpha) = c + d\alpha$.
- (g) En utilisant le résultat de la question d, démontrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $Q(\beta) \neq 0$.
- (h) En déduire que Q est irréductible dans $\mathbb{F}_5[X]$. Le polynôme Q est-il irréductible dans $\mathbb{Q}[X]$?
- (i) Le polynôme Q est-il irréductible dans $\mathbb{F}_{25}[X]$?

Exercice 9. Soit $n \geq 1$ un entier et p un nombre premier. Soit P un polynôme irréductible de degré d dans $\mathbb{F}_p[X]$.

- (a) Démontrer que le quotient $\mathbb{K} := \mathbb{F}_p[X]/(P(X))$ est un corps. Quel est l'ordre du groupe multiplicatif $\mathbb{K}^\times$? En déduire que tout élément $x \in \mathbb{K}$ vérifie $x^{p^d} = x$.
- (b) Démontrer ensuite que P divise $X^{p^n} - X$ si et seulement si d divise n . On redémontrera un résultat du cours si nécessaire.
- (c) Soit $Q_n := X^{p^n} - X$. Calculer Q'_n , le polynôme dérivé de Q_n . En déduire que Q_n n'est divisible par aucun carré de polynôme de degré ≥ 1 .
- (d) Démontrer que, dans $\mathbb{F}_p[X]$, le polynôme Q_n est le produit de tous les polynômes unitaires irréductibles dont le degré divise n .
- (e) On prend $n = 4$ et $p = 2$. Retrouver l'ensemble des polynômes irréductibles de degré 2 puis 4 dans $\mathbb{F}_2[X]$.
- (f) Soit R un polynôme de degré n dans $\mathbb{F}_p[X]$. Démontrer que R est irréductible si, et seulement si, les deux assertions suivantes sont vérifiées :
 - i. Le polynôme R divise Q_n .
 - ii. Pour tout diviseur premier q de n , le polynôme R est premier avec le polynôme $Q_{n/q}$.