

Corps finis.

Exercice 1. Décrire un corps à 8 éléments. Décrire un anneau à 8 éléments qui n'est pas un corps. Existe-t-il un corps à 6 éléments ? Déterminer $\mathbb{F}_9 \cap \mathbb{F}_{27}$ dans $\overline{\mathbb{F}_3}$.

Exercice 2. Soit $P(X) \in \mathbb{F}_p[X]$ irréductible et $\alpha \in \overline{\mathbb{F}_p}$ une racine de $P(X)$. Montrer que toute racine $\beta \in \overline{\mathbb{F}_p}$ de $P(X)$ est dans $\mathbb{F}_p[\alpha]$.

Exercice 3. Montrer que $\bigcup_{n \geq 1} \mathbb{F}_{p^n}$ est une clôture algébrique de \mathbb{F}_p .

Exercice 4. 1. Montrer que $\mathbb{K}_1 = \mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{K}_2 = \mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont des corps.

2. Les corps \mathbb{K}_1 et \mathbb{K}_2 sont-ils \mathbb{F}_3 -isomorphes ?

3. Donner un générateur du groupe \mathbb{K}_1^\times .

Exercice 5. Soit p un nombre premier et \mathbb{K} un corps de caractéristique p . Soit $b \in \mathbb{K}$, on pose $Q(X) := X^p - X - b$ et \mathbb{L} une extension de décomposition de $Q(X)$ sur \mathbb{K} .

1 Montrer que le morphisme de Frobenius en caractéristique p est un morphisme de l'extension \mathbb{L}/\mathbb{F}_p .

2 Soit α une racine de $Q(X)$ dans \mathbb{L} . Montrer que $Q(X) = \prod_{i \in \mathbb{F}_p} (X - \alpha - i)$. En déduire que $\mathbb{L} = \mathbb{K}(\alpha)$.

3 Soit $P(X) = X^d - a_1 X^{d-1} + \dots + (-1)^d a_d \in \mathbb{L}[X]$ un facteur unitaire de $Q(X)$. Montrer que $a_1 - d\alpha \in \mathbb{F}_p$ puis que $a_1^p - a_1 = db$.

4 Montrer que $Q(X)$ est irréductible sur \mathbb{K} si et seulement si il est sans racine dans \mathbb{K} .

5 Montrer que $X^{1789} - X - 7$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 6. Montrer que $\mathbb{Z}[X]/(3, X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont des corps. Sont-ils isomorphes ?

Exercice 7. Soit $P(X) = X^5 + X^4 + 3X^2 + 1$, on note $\overline{P}(X)$ la réduction de $P(X)$ modulo 2.

1. Montrer que $P(X)$ n'a pas de racine dans \mathbb{Z} .
2. Quels sont les irréductibles de degré 1, 2 et 3 dans $\mathbb{F}_2[X]$?
3. Factoriser $\overline{P}(X)$ en produits d'irréductibles dans $\mathbb{F}_2[X]$.
4. Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$ puis dans $\mathbb{Z}[X]$.

Exercice 8. Soit p un nombre premier, $q = p^r$ avec $r \geq 1$. On note $G = \text{Aut}(\mathbb{F}_q)$.

1 Montrez que $\mathbb{F}_q = \mathbb{F}_p(\zeta)$ où $\langle \zeta \rangle = \mathbb{F}_q^\times$.

2 On note $\text{Frob}_p : \mathbb{F}_q \rightarrow \mathbb{F}_q$ le morphisme de Frobenius en caractéristique p .

- a) Montrez que Frob_p est un isomorphisme et que G est un groupe pour la loi de composition.
- b) Montrez que $\text{Frob}_p^r = \text{Id}$ et que pour tout $d \leq r$ on a $\zeta^{p^d} \neq \zeta$. En déduire que l'ordre de Frob_p dans G est r .
- c) Quel est le degré de $P(X) := \text{Irr}(\zeta, \mathbb{F}_p, X)$? Montrez que $\text{Frob}_p|_{\mathbb{F}_p} = \text{Id}_{\mathbb{F}_p}$, en déduire que pour $1 \leq i \leq r-1$, $P(\text{Frob}_p^i(\zeta)) = 0$. Montrez enfin que $\text{card}\{\zeta, \dots, \text{Frob}_p^{r-1}(\zeta)\} = r$.
- d) En déduire que $P(X) = (X - \zeta)(X - \text{Frob}_p(\zeta)) \dots (X - \text{Frob}_p^{r-1}(\zeta))$

3 Soit $\sigma \in G$.

- a) Montrez que $\sigma|_{\mathbb{F}_p} = \text{Id}_{\mathbb{F}_p}$.
- b) Montrez qu'il existe i avec $0 \leq i \leq r-1$ tel que $\sigma(\zeta) = \text{Frob}_p^i(\zeta)$. En déduire que $\sigma = \text{Frob}_p^i$.
- c) Conclure que $G \simeq \mathbb{Z}/r\mathbb{Z}$.