TD5 : corps finis

Exercice 1. Soient $\mathbb{F}_q$ un corps à q éléments et $\mathbb{F}_{q^n}$ une extension de degré n de $\mathbb{F}_q$. Montrer qu'il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

Exercice 2.

1. Déterminer tous les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$.
2. Montrer que $\mathbb{F}_3[X]/(X^2 - X - 1)$ et $\mathbb{F}_3[Y]/(Y^2 + 1)$ sont deux corps isomorphes.
3. On note α, resp. β, la classe de X, resp. Y, dans le quotient. Déterminer l'ordre de α et β dans le groupe multiplicatif $\mathbb{F}_9^*$.
4. Expliciter un isomorphisme et sa réciproque entre $\mathbb{F}_3(\alpha) \simeq \mathbb{F}_3[X]/(X^2 - X - 1)$ et $\mathbb{F}_3(\beta) \simeq \mathbb{F}_3[Y]/(Y^2 + 1)$.
5. Déterminer tous les générateurs de $\mathbb{F}_3(\alpha)^*$ et de $\mathbb{F}_3(\beta)^*$.

Exercice 3. Soit p un nombre premier et soit $m, n \in \mathbb{N}^*$. On note $q = p^m$.

1. Montrer que $p^m - 1$ divise $p^{mn} - 1$. En déduire que $X^{p^m-1} - 1$ divise $X^{p^{mn}-1} - 1$.
2. En déduire que le corps fini $\mathbb{F}_{p^{mn}}$ admet un unique sous-corps à p^m éléments et que $[\mathbb{F}_{p^{mn}} : \mathbb{F}_{p^m}] = n$.
3. En déduire que tout corps intermédiaire $\mathbb{F}_q \subset K \subset \mathbb{F}_{q^n}$ est un corps à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d.
4. Donner tous les sous-corps de $\mathbb{F}_8$ et $\mathbb{F}_{64}$.

Exercice 4. Soient p un nombre premier et $n, m \in \mathbb{N}^*$. On note $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ l'automorphisme de Frobenius $x \mapsto x^p$.

1. Montrer que tout polynôme irréductible de $\mathbb{F}_{p^n}[X]$ est à racines simples dans son corps de décomposition.
2. Montrer qu'il y a soit zéro, soit n morphismes de corps de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^m}$.
3. Montrer que le groupe des automorphismes de $\mathbb{F}_{p^n}$ est cyclique d'ordre n, engendré par le morphisme de Frobenius $\sigma : x \mapsto x^p$.
4. Montrer que l'ensemble des éléments de $\mathbb{F}_{p^n}$ laissés fixes par l'automorphisme $\sigma^k : x \mapsto x^{p^k}$ est le sous-corps de $\mathbb{F}_{p^n}$ à p^d éléments avec $d = n \wedge k$.

Exercice 5.

1. Quel est le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$? de degré 4 sur $\mathbb{F}_3$?
2. Donner une construction du corps $\mathbb{F}_{25}$.
3. Donner un élément d'ordre 8 dans $\mathbb{F}_{25}^*$.
4. Quel est le corps de décomposition de $X^4 + 1$ sur $\mathbb{F}_5$?
5. Quel est le corps de décomposition de $X^3 - 2$ sur $\mathbb{F}_5$? $\mathbb{F}_7$?

6. Le polynôme $X^4 - 2$ est-il irréductible sur $\mathbb{F}_5$? sur $\mathbb{F}_{25}$?

Exercice 6. Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On considère un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré $n > 1$.

1. Soit $d > 1$ un diviseur de n. Montrer que $\mathbb{F}_{q^n}$ est un corps de décomposition de P sur $\mathbb{F}_{q^d}$.
   En déduire que P n'est pas irréductible sur $\mathbb{F}_{q^d}$.
2. Soit Q un facteur irréductible de P dans $\mathbb{F}_{q^d}[X]$. Montrer qu'un corps de rupture de Q sur $\mathbb{F}_{q^d}$ est un corps de décomposition de P sur $\mathbb{F}_q$.
   En déduire que P est un produit de d facteurs irréductibles de degré n/d dans $\mathbb{F}_{q^d}[X]$.
3. Soit $k \in \mathbb{N}^*$. Montrer que P est irréductible sur $\mathbb{F}_{q^k}$ si et seulement si k et n sont premiers entre eux.

Exercice 7. Soit p premier. Pour tout $i \in \mathbb{N}^*$, on choisit un morphisme de corps $f_i : \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{(i+1)!}}$. On pose alors $K = \bigcup_{i\in\mathbb{N}^*} \mathbb{F}_{p^{i!}}$ où chaque $\mathbb{F}_{p^{i!}}$ s'identifie à son image par $f_{j-1} \circ \cdots \circ f_i$ dans $\mathbb{F}_{p^{j!}}$ pour tout $j > i$.
Montrer que K est une clôture algébrique de $\mathbb{F}_p$.

Exercice 8. On note $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ la fonction de Möbius, définie de la façon suivante :
— $\mu(n) = 0$ si n est divisible par un carré autre que 1
— sinon, $\mu(n) = 1$ si n a un nombre pair de facteurs premiers, et $\mu(n) = -1$ sinon.
On admet la formule d'inversion de Möbius :

$$\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d|n} f(d) \quad \Longleftrightarrow \quad \forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d).$$

1. Montrer que le nombre de polynômes irréductibles unitaires de degré n dans $\mathbb{F}_q[X]$ est égal à $\frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) q^d$.
2. Retrouver ainsi le nombre de polynômes irréductibles unitaires de degré 3 sur $\mathbb{F}_7$ et de degré 4 sur $\mathbb{F}_3$.

Exercice 9.

1. Calculer les polynômes cyclotomiques Φ_{14} et Φ_{15}.
2. Soient p un nombre premier et α un entier naturel non nul. Calculer Φ_p et montrer que $\Phi_{p^\alpha} = \Phi_p(X^{p^{\alpha-1}})$.

Exercice 10. Soit K une extension finie de $\mathbb{Q}$. Montrer qu'il n'y a qu'un nombre fini de racines de l'unité dans K.

Exercice 11. Soit p la caractéristique du corps fini $\mathbb{F}_q$.

1. Soit $n \in \mathbb{N}^*$ tel que $q \wedge n = 1$. Montrer que le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ si et seulement si q est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
2. Pour les entiers $n \in \{3, 4, 5, 6, 7, 8, 12\}$, discuter selon les valeurs de q de l'irréducibilité sur $\mathbb{F}_q$ de la réduction modulo p du polynôme cyclotomique Φ_n.
3. Factoriser Φ_{14} sur $\mathbb{F}_2$.

Exercice 12. Soient p un nombre premier et $n \in \mathbb{N}^*$ tel que $n = p^\alpha m$ avec $\alpha \in \mathbb{N}^*$ et $p \nmid m$. Soit Φ_n le n-ème polynôme cyclotomique.

1. Montrer que dans $\mathbb{F}_p[X]$, on a $\Phi_n = (\Phi_m)^{\varphi(p^\alpha)}$.
2. Montrer que Φ_n est réductible sur $\mathbb{F}_p$ sauf éventuellement si $(p, \alpha) = (2, 1)$.