TD - Théorie des corps

J. Le Borgne

Exercice 1

Soit A un anneau intègre fini. Démontrer que A est un corps.

Exercice 2

On suppose que K est un corps fini de cardinal q.

1. Démontrer que la caractéristique de K est un nombre premier p, et en déduire que $q = p^n$ pour un certain $n \geq 1$.
2. Démontrer que pour tout $x \in K$, $x^q = x$.
3. Soit E un corps de décomposition de $X^q - X \in \mathbf{F}_p[X]$.
   a) Démontrer que l'ensemble des racines de $X^q - X$ est un sous-corps de E, et en déduire que E est de cardinal q.
   b) Démontrer qu'il existe un isomorphisme $\mathbf{F}_p$-linéaire $E \simeq K$.

Exercice 3

Soit K un corps et soit $\Gamma \subset K^\times$ un sous-groupe fini d'ordre n.

1. Pour $d|n$, on note $\tau(d)$ le nombre d'éléments d'ordre d de Γ. Justifier que $\sum_{d|n} \tau(d) = n$.
2. On suppose que $\tau(d) \neq 0$, et on se donne $\gamma \in \Gamma$ d'ordre d.
   a) Justifier que l'ensemble des racines de $X^d - 1 \in K[X]$ est le sous-groupe engendré par γ.
   b) En déduire que $\tau(d) = \varphi(d)$.
3. Démontrer que Γ est un groupe cyclique.

Exercice 4

Soient K et L deux corps finis.

1. On suppose que L est une extension de K. Démontrer que K et L sont de même caractéristique p et que $[K : \mathbf{F}_p]$ divise $[L : \mathbf{F}_p]$.
2. On suppose que K et L sont de même caractéristique p et que $[K : \mathbf{F}_p]$ divise $[L : \mathbf{F}_p]$. Démontrer que L est une extension de K.

Exercice 5

Soit $K = \mathbf{F}_q$.

1. Si K est de caractéristique 2, démontrer que tout élément de K est un carré.
2. On suppose maintenant que q est impair.
   a) En considérant l'application $K^\times \to K^\times$ définie par $x \mapsto x^2$, démontrer qu'il y a $\frac{q+1}{2}$ carrés dans K.
   b) Démontrer que $x \in K^\times$ est un carré si et seulement si $x^{\frac{q-1}{2}} = 1$.

Exercice 6

Soit K un corps fini de caractéristique p, et L une extension finie de K.

1. Soit $\omega \in L^\times$ un générateur du groupe $L^\times$. Démontrer que $L = K(\omega)$.
2. En déduire que pour tout $n \in \mathbf{N}$, il existe un polynôme irréductible de degré n dans $K[X]$.

Exercice 7

Soit K un corps fini de caractéristique p.

1. Justifier que l'endomorphisme de Frobenius $x \mapsto x^p$ est un automorphisme de K.
2. Démontrer que l'image de l'application $Q \mapsto Q^p$ définie sur $K[X]$ est $K[X^p]$.
3. Soit $P \in K[X]$ tel que $P' = 0$. Montrer qu'il existe $Q \in K[X]$ tel que $P = Q^p$.
4. Soit $P \in K[X]$ irréductible. Démontrer que P et P' sont premiers entre eux.

Exercice 8

1. Déterminer le cardinal de $GL_n(\mathbf{F}_q)$.
2. Proposer une méthode pour exhiber un élément d'ordre $q^n - 1$ de $GL_n(\mathbf{F}_q)$.
3. Dénombrer les sous-espaces vectoriels de dimension k de $\mathbf{F}_q^n$.

Exercice 9

Démontrer que $A \in \mathcal{M}_n(\mathbf{F}_q)$ est diagonalisable si et seulement si $A^q = A$.

Exercice 10

Soit q une puissance d'un nombre premier p, soit $n \geq 1$ et soit $K = \mathbf{F}_{q^n}$.

1. Soit ω un générateur du groupe $K^\times$. Démontrer que $\{\omega, \omega^q, \cdots, \omega^{q^{n-1}}\}$ est de cardinal n et stable par $\mathrm{Frob}_q : x \mapsto x^q$.
2. Démontrer que le polynôme minimal de ω sur $\mathbf{F}_q$ est $\prod_{0 \leq i \leq n-1}(X - \omega^{q^i})$.
3. En déduire que si $\sigma \in \mathbf{F}_{q^n}$ est un automorphisme $\mathbf{F}_q$-linéaire, alors il existe $0 \leq i \leq n-1$ tel que $\sigma = \mathrm{Frob}_q^i$.
4. Démontrer que le morphisme de groupes naturel $\mathbf{Z} \to \mathrm{Aut}_{\mathbf{F}_q}(K)$ qui envoie 1 sur Frob_q induit un isomorphisme $\mathbf{Z}/n\mathbf{Z} \to \mathrm{Aut}_{\mathbf{F}_q}(K)$.

Exercice 11

Soit $n \geq 1$ et soit $K = \mathbf{F}_q$ un corps fini de caractéristique p. On suppose que p ne divise pas n. On considère le polynôme cyclotomique $\Phi_n \in K[X]$, et on fixe E/K un corps de décomposition de Φ_n.

1. Soit ζ une racine de Φ_n dans E.
   a) Démontrer que si $k \neq n$, alors $\Phi_k(\zeta) \neq 0$.
   b) En déduire que ζ est d'ordre n dans $E^\times$.
2. Soit $P \in K[X]$ un facteur irréductible de Φ_n, et soit d l'order de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$.
   a) Démontrer que si $\zeta \in E$ est racine de P, alors les racines de P dans E sont $\zeta, \zeta^q, \ldots, \zeta^{q^{d-1}}$.
   b) En déduire que P est de degré d.
3. Démontrer que $\Phi_n \in K[X]$ est scindé si et seulement si n divise $q - 1$.
4. a) Démontrer que $\Phi_n \in K[X]$ est irréductible si et seulement si $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique et que q en est un générateur.
   b) En déduire un exemple de $P \in \mathbf{Z}[X]$ tel que P soit irréductible dans $\mathbf{Z}[X]$ et réductible dans $\mathbf{F}_p[X]$ pour tout p premier.

Exercice 12

Soit $n \geq 1$. Le but de cet exercice est de démontrer qu'il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod{n}$.

1. En utilisant l'exercice précédent, démontrer que $p \equiv 1 \pmod{n}$ si et seulement si Φ_n a une racine dans $\mathbf{F}_p$.
2. On raisonne par l'absurde en supposant que l'ensemble des nombres premiers congrus à 1 modulo n est $\{p_1, \ldots, p_r\}$. On note $a = p_1 \cdots p_r$.
   a) Soit $k \in \mathbf{N}^*$ divisible par a. Démontrer que $\Phi_n(k)$ n'est divisible par aucun des p_i.
   b) Démontrer qu'il existe $k \in \mathbf{N}^*$ divisible par a tel que $\Phi_n(k) \notin \{\pm 1\}$.
   c) On fixe un tel entier k. En considérant un facteur premier p de $\Phi_n(k)$, aboutir à une contradiction.

Exercice 13

Soit $K = \mathbf{F}_q$ et soit $n \geq 1$.

1. Soit $P \in K[X]$ irréductible de degré n. Démontrer que P divise $X^{q^n} - X$.
2. Soit $P \in K[X]$ un facteur irréductible de $X^{q^n} - X$. Démontrer que le degré de P est un diviseur de n.
3. Pour $d \in \mathbf{N}$, on note $I_q(d)$ l'ensemble des polynômes irréductibles unitaires de degré d dans $K[X]$. Démontrer que
$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I_q(d)} P.$$
4. En déduire que $q^n = \sum_{d|n} d|I_q(d)|$.

Exercice 14

Soit $K = \mathbf{F}_q$ et soit $P \in K[X]$. On suppose que $P = P_1 \dots P_r$ avec les P_i deux à deux distincts et irréductibles.

1. Pour $1 \leq i \leq r$, on note $d_i = \deg P_i$. Justifier qu'il existe un isomorphisme de $\mathbf{F}_q$-algèbres :
$$K[X]/(P) \simeq \mathbf{F}_{q^{d_1}} \times \cdots \times \mathbf{F}_{q^{d_r}}.$$
2. Soit $A = K[X]/(P)$ et Frob_q l'endomorphisme de A défini par $a \mapsto a^q$. Démontrer que $r = \dim \ker(\mathrm{Frob}_q - id)$.
3. Soit $R \in K[X]$ tel que $\bar{R} \in \ker(\mathrm{Frob}_q - id)$.
   a) Démontrer que P divise $R^q - R$.
   b) En déduire que $P = \prod_{\alpha \in K} \mathrm{pgcd}(P, R - \alpha)$.
   c) On suppse que $r \geq 2$. Démontrer qu'il existe $R \in \ker(\mathrm{Frob}_q - id)$ et $\alpha \in K$ tels que $\mathrm{pgcd}(P, Q - \alpha)$ soit un diviseur non trivial de P.
4. Proposer un algorithme de factorisation des polynômes sans facteurs carrés dans $\mathbf{F}_q[X]$ basé sur ce qui précède.

Exercice 15

Soit p premier impair, q une puissance de p et $K = \mathbf{F}_q$. Soit $P \in K[X]$. On suppose que $P = P_1 \dots P_r$ avec les P_i deux à deux distincts, irréductibles et de même degré d.

1. Expliciter un isomorphisme de K-algèbres $f : K[X]/(P) \simeq \mathbf{F}_{q^d}^r$.
2. Soit $A \in K[X]$ non nul tel que $\deg A < \deg P$ et a son image dans $K[X]/(P)$.
   a) Justifier que les composantes de $f(a^{\frac{q^d-1}{2}})$ sont dans $\{-1, 0, 1\}$.
   b) Démontrer que si l'une des composantes de $f(a^{\frac{q^d-1}{2}})$ est nulle, alors $\mathrm{pgcd}(A, P)$ est un diviseur non trivial de P.
   c) On suppose que $\mathrm{pgcd}(A, P) = 1$. Démontrer que $\mathrm{pgcd}(A^{\frac{q^d-1}{2}} - 1, P)$ est un diviseur non trivial de P si et seulement si les composantes de $f(a^{\frac{q^d-1}{2}})$ ne sont pas toutes égales.
   d) Déterminer les cardinaux des ensembles suivants :
   — $(K[X]/(P))^\times$
   — $\{a \in K[X]/(P) \mid a^{\frac{q^d-1}{2}} = \pm 1\}$
3. Démontrer que, si l'on tire uniformément A parmi les éléments de $K[X]$ de degré $< \deg P$ premiers avec P, la probabilité que $A^{\frac{q^d-1}{2}} - 1$ ait un facteur commun non trivial avec P est $1/2^{r-1}$.
4. Proposer un algorithme de factorisation pour les polynômes de la forme considérée.