ENS de Lyon Option C
2017-2018

TD Révisions sur les corps finis

Exercice 1 [Groupe multiplicatif d'un corps fini]

1. Montrer que $k^\times$ est cyclique lorsque k est un corps fini. Combien $k^\times$ a-t-il de générateurs ?
2. Soit K/k une extension de corps finis. Montrer qu'il existe $\alpha \in K$ tel que $K = k(\alpha)$ (théorème de l'élément primitif dans le cas des corps finis). En déduire que K est isomorphe à $k[X]/P$ pour un polynôme $P \in k[X]$ irréductible de degré $[K : k]$.
3. Soit $k = \mathbf{F}_q$, et $n \leq 1$ un entier. Montrer que $X^n - 1$ a exactement $\operatorname{pgcd}(n, q-1)$ racines dans k. Montrer que k contient exactement $(q-1)/\operatorname{pgcd}(n, q-1)$ éléments non nuls qui sont des puissances n-ièmes d'éléments de k.
4. Montrer que dans $\mathbf{F}_{2^n}$ tout élément est un carré. Comment trouver sa racine carrée ?
5. Soit $q = p^n$ impair. Montrer que $x \in \mathbf{F}_q^\times$ est un carré si et seulement si $x^{(q-1)/2} = 1$.
6. Montrer que $\mathbf{F}_q$ a des racines primitives n-ièmes de 1 si et seulement si n divise $q-1$. Montrer que dans ce cas il y en a $\varphi(n)$, où φ est l'indicatrice d'Euler.
7. Soit Φ_n le n-ième polynôme cyclotomique. On rappelle que Φ_n est à coefficients entiers, et donc définit un élément de $\mathbf{F}_p[X]$ par réduction. Montrer sur un exemple que Φ_n n'est pas nécessairement irréductible dans $\mathbf{F}_p[X]$.
8. On suppose que n est premier à p. Soit $q = p^m$. On note s l'ordre de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Montrer que la factorisation de Φ_n dans $\mathbf{F}_q$ fait apparaître r facteurs de même degré s, deux à deux distincts, où $rs = \varphi(n)$.
9. Soit $\alpha \in \mathbf{F}_q^\times$. Montrer que α est un générateur du groupe multiplicatif $\mathbf{F}_q^\times$ si et seulement si son polynôme minimal sur $\mathbf{F}_p$ divise Φ_{q-1}.

Exercice 2 [Séparabilité des polynômes]

1. Dans cette question seulement, on suppose que k est un corps de caractéristique 0. Soit $P \in k[X]$. Donner une méthode pour factoriser P sous la forme QR où Q est sans facteur carré et R divise une puissance de Q (c'est-à-dire que tous les facteurs irréductibles de R apparaissent déjà dans Q). Vérifier que Q et R sont à coefficients dans k.
2. Que se passe-t-il dans le cas où k est de caractéristique $p > 0$?
3. Soit $P \in \mathbf{F}_q[X]$ un polynôme tel que $P' = 0$. Montrer qu'il existe $Q \in \mathbf{F}_q[X]$ tel que $P = Q^p$. Donner une méthode explicite pour calculer Q.
4. En déduire une méthode de factorisation $P = QR$ comme dans la première question.
5. Soit $P \in \mathbf{F}_q[X]$ un polynôme irréductible. Montrer que P est à racines simples dans une clôture algébrique de $\mathbf{F}_q$.

Exercice 3 [Morphisme de Frobenius]

Soit q une puissance d'un nombre premier, et $k = \mathbf{F}_{q^n}$, $n \geq 1$. On appelle *morphisme de Frobenius* l'application $F_q : k \to k$ définie par $F_q(x) = x^q$.

1. Vérifier que F_q est un automorphisme du corps k.
2. Montrer que le corps fixé par F_q (c'est-à-dire $\{x : F(x) = x\}$) est $\mathbf{F}_q$.
3. Montrer que le corps fixé par F_q^m est $\mathbf{F}_{q^d}$ où d est le pgcd de n et m. Montrer que F_q est un automorphisme de k d'ordre n.
4. Fixons un isomorphisme entre k et $\mathbf{F}_q[X]/(P)$, où P est un polynôme irréductible de degré n à coefficients dans $\mathbf{F}_q$. Montrer que tout automorphisme de corps de k fixant $\mathbf{F}_q$ envoie une racine de P sur une racine de P. Montrer qu'un tel automorphisme est entièrement déterminé par l'image d'une racine de P.
5. En déduire que l'ensemble des automorphismes du corps k fixant $\mathbf{F}_q$ est exactement l'ensemble des itérés de F_q.

Exercice 4 [Corps de décomposition des polynômes]
On reprend les notations de l'exercice précédent.

1. Soit P un polynôme à coefficients dans $\mathbf{F}_q$. Vérifier que si α est une racine de P dans k, alors $F_q(\alpha)$ aussi.
2. Soit P un polynôme irréductible de degré $n \geq 1$ à coefficients dans $\mathbf{F}_q$. Montrer que P possède une racine α dans $\mathbf{F}_{q^n}$, puis que les racines de P sont exactement les α^{q^k} avec $0 \leq k \leq n-1$. En déduire que P est scindé à racines simples dans $\mathbf{F}_{q^n}$.
3. Avec les notations de la question précédente, comment obtenir le polynôme minimal de α sur $\mathbf{F}_{q^m}$ lorsque m divise n ?

Exercice 5 [Isomorphismes entre corps finis]
Expliciter un isomorphisme de corps entre $\mathbf{F}_2[X]/(X^3 + X + 1)$ et $\mathbf{F}_2[Y]/(Y^3 + Y^2 + 1)$.

Exercice 6 [Test d'irréductibilité de Rabin]
Soit $P \in \mathbf{F}_q[X]$ de degré d.

1. Montrer que P a une racine dans $\mathbf{F}_{q^n}$ si et seulement si $\mathrm{pgcd}(P, X^{q^n} - X) \neq 1$.
2. Montrer que P est irréductible dans $\mathbf{F}_q[X]$ si et seulement si il divise $X^{q^d} - X$ et il est premier avec $X^{q^{d/s}} - X$, pour tout facteur premier s de d.
3. On suppose que l'on connaît la liste des facteurs premiers de d. Écrire un algorithme inspiré par le critère précédent permettant de savoir si P est irréductible dans $\mathbf{F}_q$. Quel est son coût ?

Exercice 7 [Interlude : fonction d'inversion de Moebius]
Pour tout entier n, on définit $\mu(n)$ de la façon suivante :

- si n a un facteur carré, $\mu(n) = 0$
- si n est sans facteur carré et a exactement r facteurs premiers distincts, $\mu(n) = (-1)^r$

1. Montrer que μ est multiplicative, c'est-à-dire que si n et m sont premiers entre eux, alors $\mu(mn) = \mu(m)\mu(n)$.
2. Montrer que pour tout entier $n > 1$, on a $\sum_{d|n} \mu(d) = 0$.
3. Soit $f : \mathbf{N}^* \to A$, où A est un groupe abélien noté additivement. On pose $g(n) = \sum_{d|n} f(d)$. Montrer que $f(n) = \sum_{d|n} \mu(n/d)g(d)$.

Exercice 8 [Nombre de polynômes irréductibles]
On fixe dans la suite q une puissance de p, et $n \geq 1$.

1. Soit P un polynôme irréductible à coefficients dans $\mathbf{F}_q$, de degré m. Montrer que P a une racine dans $\mathbf{F}_{q^n}$ (et donc y est scindé) si et seulement si m divise n.
2. Soit P un polynôme irréductible à coefficients dans $\mathbf{F}_q$, de degré m. Montrer que P est scindé dans $\mathbf{F}_{q^n}$ si et seulement si P divise $X^{q^n} - X$.
3. Notons $I_m(q)$ l'ensemble des polynômes irréductibles unitaires de degré m à coefficients dans $\mathbf{F}_q$. Montrer que :
$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I_d(q)} P$$
4. En déduire que
$$q^n = \sum_{d|n} d\mathrm{Card}(I_d(q))$$
5. En déduire :
$$\mathrm{Card}(I_n(q)) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d$$
En particulier, montrer que $\mathrm{card}(I_n(q)) > 0$ pour tout n, et en donner un équivalent quand $n \to \infty$.
6. Calculer le cardinal de $I_n(q)$ pour des petites valeurs de n et q (que dire quand n est premier ?), énumérer les polynômes de $I_n(q)$ lorsque le cardinal n'est pas trop grand (disons $q = 2$ ou $q = 3$, $n \leq 3$, et $q = 4$, $n = 2$). Comment faire cela avec l'ordinateur ?

Exercice 9 [Nombre de polynômes irréductibles, deuxième méthode]
On fixe dans la suite q une puissance de p, et $n \geq 1$. Soit $I_n(q)$ le nombre de polynômes irréductibles unitaires à coefficients dans $\mathbf{F}_q$ de degré n.

1. Montrer que $nI_n(q)$ est le nombre d'éléments de $\overline{\mathbf{F}_q}$ qui sont de degré exactement n sur $\mathbf{F}_q$.
2. En déduire que $nI_n(q) = \mathrm{Card}(\mathbf{F}_{q^n} \setminus (\cup_{\ell|n} \mathbf{F}_{q^{n/\ell}}))$, où ℓ parcourt l'ensemble des diviseurs premiers de n.
3. En utilisant la formule d'inclusion-exclusion, retrouver la formule de l'exercice précédent.

Exercice 10 [Logarithme de Zech]

Dans cet exercice, on décrit une manière alternative de calculer dans le corps fini $\mathbf{F}_{2^m}$. Soit g un générateur de $\mathbf{F}_{2^m}^\times$. On a une bijection $\mathbf{Z}/(2^m - 1)\mathbf{Z} \cong \mathbf{F}_{2^m}^\times$ donnée par $i \mapsto g^i$. On convient également que $g^\infty = 0$, ce qui nous donne une bijection entre $\mathbf{F}_{2^m}$ et l'ensemble $L = \mathbf{Z}/(2^m - 1)\mathbf{Z} \cup \{\infty\}$.

1. Comment calculer le produit de deux éléments de $\mathbf{F}_{2^m}$ avec cette représentation ?

Pour l'addition, on utilise la remarque suivante : $g^i + g^j = g^i(1 + g^{j-i})$. Il suffit donc de savoir calculer $1 + g^i$ pour tout i dans L. On définit une application $z : L \to L$ par $1 + g^i = g^{z(i)}$.

2. Montrer que z est une involution sans point fixe qui vérifie $z(2i) = 2z(i)$ et $z(-i) = z(i) - i$ pour tout $i \in L$.
3. Choisir un générateur de $\mathbf{F}_{16}^\times$ puis construire la *table de Zech* donnant explicitement l'application z pour ce générateur.