UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°1 : Corps finis

1 Extensions de corps

Exercice 1

Un corps fini est-il algébriquement clos ?

Exercice 2

Montrer que tout morphisme de corps est injectif ?

Exercice 3

Soit K un corps, et soit $P \in K[X]$ un polynôme irréductible sur K.

1. Soit K' un corps de rupture de P sur K, et soit L une extension de K. Montrer qu'il y a une bijection naturelle entre les morphismes K-linéaires de corps de K' dans L et les racines de P dans L.
2. On suppose que K est de caractéristique 0. Combien y a-t-il de morphismes K-linéaires de corps de K' dans une clôture algébrique $\overline{K}$ de K ?

Exercice 4

On considère la suite d'entiers définie par

(i) $u_0 = 3$, $u_1 = 0$, $u_2 = 2$;

(ii) $u_{n+3} = u_n + u_{n+1}$ pour $n \geqslant 0$.

Montrer que si p est un nombre premier, alors u_p est multiple de p. (On pourra déterminer l'image de u_n dans un corps bien choisi. Notez que, comme pour le petit théorème de Fermat, la réciproque est fausse).

Exercice 5

Soit L/K une extension finie de corps. Pour simplifier les raisonnements, on suppose de plus que K est de caractéristique 0. Soit $x \in L$. On considère l'application K-linéaire de L dans L, m_x, donnée par la multiplication par x. On définit la *norme* de x, notée $N_{L/K}(x)$, comme le déterminant de m_x, et la *trace* de x, notée $\mathrm{Tr}_{L/K}(x)$, comme la trace de m_x.

1. Montrer qu'il y a exactement $d = [L\colon K]$ morphismes de corps K linéaires de L dans une clôture algébrique de K. On note σ_1, ..., σ_d ces morphismes.
2. Montrer que les valeurs propres de m_x sont $\sigma_1(x)$, ..., $\sigma_d(x)$. (On pourra commencer par le cas où $L = K(x)$).
3. En déduire que $N_{L/K}(x) = \prod_{i=1}^d \sigma_i(x)$ et $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^d \sigma_i(x)$.

2 Corps finis

Exercice 6

Écrire la table de multiplication de $\mathbb{F}_4$.

Exercice 7

Soit K un corps de caractéristique p. Montrer que l'application $K \to K$, $x \mapsto x^p$ est un automorphisme de corps et déterminer ses points fixes.

Exercice 8

Soit $P = X^3 + 2X + 1 \in \mathbb{F}_3[X]$. Posons $\mathbb{L} = \mathbb{F}_3[X]/(P)$ et α la classe de X dans $\mathbb{L}$.

1. Montrer que P est irréductible sur $\mathbb{F}_3$. En déduire que $\mathbb{L}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? Donner une base du $\mathbb{F}_3$-espace vectoriel $\mathbb{L}$.
2. Quels sont les ordres possibles pour les éléments de $\mathbb{L}^* \setminus \mathbb{F}_3^*$ (dans le groupe $\mathbb{L}^*$).
3. L'objet de la question est de montrer que α est un générateur de $\mathbb{L}^*$.
   (a) Montrer que $\alpha^{13} = -1$ si et seulement si P divise $(X-1)^4X + 1$ dans $\mathbb{F}_3[X]$.
   (b) Conclure.
4. Le polynôme $Q = X^4 + X^3 + X^2 + X + 1$ a-t-il une racine dans $\mathbb{L}$?

Exercice 9

Soit $P = X^3 + X + 1$ dans $\mathbb{F}_5[X]$ et l'anneau $K = \mathbb{F}_5[X]/(P)$. On note α la classe de X.

1. Montrer que K est un corps. Donner sa caractéristique, son cardinal ainsi qu'une base $\mathcal{B}$ de K en tant que $\mathbb{F}_5$-espace vectoriel.
2. Donner les développements de α^3, α^{15} et α^{30} dans $\mathcal{B}$. Donner l'ordre de α et de 2α dans $K^\star$.
3. Déterminer les coordonnées de l'inverse de $1 + \alpha$ dans $\mathcal{B}$.
4. Que vaut $P(\alpha^5)$? Donner les racines de P dans K.

Exercice 10

Soit $P = X^2 + X + 2 \in \mathbb{F}_5[X]$. On note $\mathbb{K} = \mathbb{F}_5[X]/(P)$ et α la classe de X dans $\mathbb{K}$.

1. Montrer que P est irréductible sur $\mathbb{F}_5$. En déduire que $\mathbb{K}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? En donner une base comme $\mathbb{F}_5$-espace vectoriel.
2. Exprimer toutes les puissances distinctes de α dans cette base. Quel est l'ordre de α dans $\mathbb{K}^*$?
3. Montrer que $\mathbb{F}_5 = \{x \in \mathbb{K}/x = x^5\}$.
4. Soit $a \in \mathbb{K} \setminus \mathbb{F}_5$. Montrer que le polynôme $P_a = (X-a)(X-a^5)$ est irréductible dans $\mathbb{F}_5[X]$.
5. Montrer que si $Q \in \mathbb{F}_5[X]$ alors a est racine de Q si et seulement si P_a divise Q.
6. Factoriser le polynôme $X^{25} - X$ dans $\mathbb{F}_5[X]$ et donner les racines dans $\mathbb{K}$ de chaque facteur.

Exercice 11

Quels sont les sous-corps de $\mathbb{F}_{64}$?

Exercice 12

Soit k un corps fini à q éléments. Notons I_n le nombre de polynômes unitaires irréductibles de degré n dans $k[X]$.

(i) Montrer que l'on a $\sum_{d|n} dI_d = q^n$, pour tout entier $n \geqslant 1$.

(ii) On définit la fonction de Möbius par : $\mu(n) = 0$ si n a un facteur carré, et $\mu(n) = (-1)^r$ si n est un produit de r facteurs premiers distincts. Montrer que $I_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

(iii) Montrer que $I_n > 0$ pour tout entier $n \geqslant 1$.

(iv) En déduire l'existence de corps finis de cardinal toute puissance d'un nombre premier.

(v) Trouver un équivalent de I_n quand n tend vers l'infini.

Exercice 13

Trouver un générateur de $\mathbb{F}_{31}^{\times}$.

Exercice 14

Questions préliminaires :

(a) Déterminer tous les idéaux de l'anneau $\mathbb{Z}$. Donner tous les idéaux I de $\mathbb{Z}$ tels que $\mathbb{Z}/I$ soit un corps.

(b) Montrer que le groupe multiplicatif d'un corps fini est cylique.

1. Déterminer tous les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$. (Rappel : $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$).
2. Soit $f = 2X^5 + X^4 + 2X^3 + X + 2$.
   (a) Donner la classe $\bar{f}$ de f dans l'anneau $\frac{\mathbb{F}_3[X]}{(2X^2+2)}$.
   (b) Donner la classe $\widetilde{f}$ de f dans l'anneau $\frac{\mathbb{F}_3[X]}{(2X^2+X+1)}$.
   (c) f a-t-il des racines dans $\mathbb{F}_3$?
   (d) f est-il irréductible dans $\mathbb{F}_3[X]$?
3. On considère l'anneau $A = \frac{\mathbb{F}_3[X]}{(f)}$. Soit $f_1 = 2X^2 + X + 1$.
   (a) Montrer que A est isomorphe à un anneau produit $\frac{\mathbb{F}_3[X]}{(f_1)} \times \frac{\mathbb{F}_3[X]}{(f_2)}$. On précisera le polynôme f_2 et l'isomorphisme mis en jeu. Indication : lemme chinois.
   (b) A est-il un corps ? A est-il un anneau intègre ?
4. Soient $A_1 = \frac{\mathbb{F}_3[X]}{(f_1)}$ et $A_2 = \frac{\mathbb{F}_3[X]}{(f_2)}$. Soit ω une racine de f_2 dans A_2.
   (a) A_1, A_2 sont-ils des corps ?
   (b) ω est-il un générateur du groupe multiplicatif $A_2^\star$?
   (c) Donner le polynôme minimal de ω^2 sur $\mathbb{F}_3$.

Exercice 15

Décomposer le polynôme $X^4 + 1$ en produit de facteurs irréductibles dans $\mathbb{F}_7[X]$.

Exercice 16

Montrer qu'il n'y a pas d'entier impair $n > 1$ tel que $a^{n-1} \equiv -1 \pmod{n}$ pour un certain $a \in \mathbb{Z}$.

3 Carrés dans les corps finis

Exercice 17

Soit $\mathbb{F}_q$ un corps fini à q éléments, de caractéristique p.

(i) Soit $x \in \mathbb{F}_q$. Montrer que $N_{\mathbb{F}_q/\mathbb{F}_p}(x) = x^{\frac{q-1}{p-1}}$.

(ii) Montrer que x est un carré dans $\mathbb{F}_q$ si et seulement si $N_{\mathbb{F}_q/\mathbb{F}_p}(x)$ est un carré dans $\mathbb{F}_p$.

Exercice 18

Est-ce que 94 est un carré modulo 131 ?

Exercice 19

Résoudre l'équation aux congruences $x^2 \equiv 39 \pmod{105}$.