

IX. — CORPS FINIS

Exercice 1 Morphisme de Frobenius Soit K un corps de caractéristique p . Montrer que $f : K \rightarrow K \ x \mapsto x^p$ est un morphisme de corps.

Exercice 2 Symbole de Legendre Soit p un nombre premier impair. On note $\mathbb{F}_p$ le corps fini $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.

- Quel est le noyau du morphisme de groupes $\mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times, x \mapsto x^2$? En déduire que le sous-groupe $\mathcal{C} = \{x^2 : x \in \mathbb{F}_p^\times\}$ est d'ordre $\frac{p-1}{2}$.
- Soit $x \in \mathbb{F}_p^\times$, montrer que $x \in \mathcal{C} \Leftrightarrow x^{\frac{p-1}{2}} = 1$.
- Si $x \in \mathbb{F}_p^\times$ n'est pas un carré, alors que vaut $x^{\frac{p-1}{2}}$? *Indication. Élever au carré.*
- Soit x un entier premier à p . On pose $\left(\frac{x}{p}\right) = 1$ si x est un carré mod p , -1 sinon. Vérifier que

$$\forall x \in \mathbb{F}_p^\times, x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) \bmod p.$$

En déduire que $\mathbb{F}_p^\times \rightarrow \{\pm 1\}, x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes.

- Déduire de ce qui précède que -1 est un carré mod $p \Leftrightarrow p \equiv 1 \bmod 4$.
- Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$. En déduire que p est irréductible sur $\mathbb{Z}[i] \Leftrightarrow p \equiv -1 \bmod 4$.
- Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$ ou $\mathbb{F}_p \times \mathbb{F}_p$.
- Montrer que $\mathbb{Z}[i]/(2)$ n'est ni un corps ni isomorphe à $\mathbb{F}_2 \times \mathbb{F}_2$.
- En utilisant $N(z) = |z|^2$, montrer que p est réductible dans $\mathbb{Z}[i] \Leftrightarrow p = a^2 + b^2$ pour certains entiers a, b . On dit que p est somme de 2 carrés.

Exercice 3 Existence et unicité des corps finis Soit $\mathbb{F}_q$ un corps fini de cardinal q .

- Montrer que $\mathbb{F}_q$ est de caractéristique un nombre premier p et que comme groupe $(\mathbb{F}_q, +) \simeq ((\mathbb{Z}/p\mathbb{Z})^n, +)$ pour un certain $n \geq 1$.
- Soient $d, e \geq 1$ des entiers montrer que :

$$X^{p^d-1} - 1 \wedge X^{p^e-1} - 1 = X^{p^d-1 \wedge p^e-1} - 1 = X^{p^{d \wedge e}-1} - 1.$$

- Montrer que si P est un polynôme irréductible de degré d sur $\mathbb{F}_q$, alors tout corps K de cardinal q^d qui contient $\mathbb{F}_q$ est isomorphe à $\mathbb{F}_q[X]/(P)$. *Indications. Montrer d'abord que $P|X^{q^n} - X$ sur $\mathbb{F}_q$ (en raisonnant dans l'anneau $\mathbb{F}_q[X]/(P)$). En déduire que P a une racine dans le corps K et construire un morphisme $\mathbb{F}_q[X] \rightarrow K$.*
- On pose $\Phi_n(X) = \prod_z (X - z) \in \mathbb{C}[X]$ où z décrit les éléments d'ordre n dans $\mathbb{C}^\times$. En utilisant la relation :

$$X^n - 1 = \prod_{d|n} \Phi_d(X),$$

montrer que $\Phi_n(X) \in \mathbb{Z}[X]$.

- e) Soit $n \geq 1$. Soit $N = p^n - 1$. Montrer que le polynôme $X^N - 1$ n'a que des facteurs irréductibles simples.
 On considère le polynôme $\Phi_N(X)$ dans $\mathbb{F}_p[X]$. Soit F un facteur irréductible de $\Phi_N(X)$ de degré d dans $\mathbb{F}_p[X]$. En raisonnant dans l'anneau $\mathbb{F}_p[X]/(F)^\dagger$, montrer que $F|X^{p^d-1} - 1$. En utilisant une des questions précédentes, montrer que $F|X^{p^{d'}-1} - 1$ avec $d' = d \wedge n$.
- f) Montrer que si $e|n$, avec $e < n$, alors F ne divise pas $X^{p^e-1} - 1$. En déduire que $d = n$.
- g) En déduire pour tout n l'existence d'un corps fini de cardinal p^n .
- h) Montrer que si P est irréductible de degré n sur $\mathbb{F}_q$, alors $P|X^{q^n} - X$. Montrer que $d|n \Rightarrow X^{q^d} - X|X^{q^n} - X$. En déduire que si $I_d(q)$ est l'ensemble des polynômes irréductibles de degré d unitaires sur $\mathbb{F}_q$, alors

$$\prod_{d|n} \prod_{f \in I_d(q)} f | X^{q^n} - X .$$

- i) Montrer qu'un facteur irréductible de $X^{q^n} - X$ sur $\mathbb{F}_q$ est de degré $d|n$.
- j) Calculer le polynôme dérivé de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. En déduire que les facteurs irréductibles de $X^{q^n} - X$ n'apparaissent qu'une seule fois dans la factorisation en irréductibles.
- k) Montrer que
- $$\prod_{d|n} \prod_{f \in I_d(q)} f = X^{q^n} - X .$$
- l) En déduire une formule pour $|I_n(q)|$ en fonction de q et de n (à l'aide de la fonction de Möbius).

Exercice 4 Irréductibilité des polynômes cyclotomiques

Soit $z \in \mathbb{C}^*$ d'ordre $n \geq 1$. Soit P le polynôme minimal unitaire de z sur $\mathbb{Q}$. Soit p un nombre premier.

- a) Montrer que $P \in \mathbb{Z}[X]$.
- b) Montrer que $p|P(z^p)$ dans $\mathbb{Z}[z]$.
- c) Montrer que $P(z^p) \neq 0 \Rightarrow P(z^p)|n^n$ dans $\mathbb{Z}[z]$. *Indication. Vérifier que dans ce cas, $P(z^p)|\Delta$, le discriminant de $X^n - 1$, et utiliser que $\Delta = \pm n^n$.*
- d) En déduire $P(z^p) \neq 0 \Rightarrow p|n$ et que $p \nmid n \Rightarrow P(z^p) = 0$.
- e) Montrer que $P = \Phi_n$ et en déduire que Φ_n est irréductible sur $\mathbb{Q}$.

†. Quel est son cardinal ?