Corps finis

Énoncés

Exercice 1 – Considérons le corps $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$. Vérifier explicitement que pour tout $x \in \mathbb{F}_4^\times$, on a l'identité $x^3 = 1$.

Exercice 2 – Soit k un corps fini de cardinal q. Montrer que pour tout $x \in k$, on a la relation $x^q = x$ (indication : utiliser le théorème de Lagrange).

Exercice 3– Soit K un corps fini de cardinal $q = p^d$, où p est un nombre premier impair. Un élément $a \in K^\times$ est un *carré* s'il existe $b \in K^\times$ tel que $a = b^2$. Le but de cet exercice est de démontrer le *critère d'Euler* :

Un élément $a \in K^\times$ est un carré si et seulement si $a^{\frac{q-1}{2}} = 1$.

1. Déterminer le noyau et l'image de l'homomorphisme $f : K^\times \to K^\times$ défini par $f(x) = x^2$.
2. En déduire qu'il existe $\frac{q-1}{2}$ carrés dans $K^\times$.
3. Montrer que si $a \in K^\times$ est un carré alors $a^{\frac{q-1}{2}} = 1$ (indication : utiliser le théorème de Lagrange).
4. Supposons maintenant que $a \in K^\times$ vérifie $a^{\frac{q-1}{2}} = 1$. Montrer que a est un carré (indication : considérer le polynôme $X^{\frac{q-1}{2}} - 1$ et utiliser le point précédent).
5. Montrer que si $a \in K^\times$ n'est pas un carré alors $a^{\frac{q-1}{2}} = -1$ (indication : factoriser le polynôme $X^{q-1} - 1$).

Exercice 4 – Soit p un nombre premier. Montrer que le polynôme $X^2 + 1 \in \mathbb{F}_p[X]$ est irréductible si et seulement si p est congru à 3 modulo 4 (indication : utiliser le critère d'Euler de l'exercice précédent).

Exercice 5 – Le but de cet exercice est de démontrer le *théorème des deux carrés de Fermat* :

Un nombre premier est somme de deux carrés si et seulement s'il n'est pas congru à 3 modulo 4.

Dans la suite, on fixe un nombre premier p.

1. Éxprimer explicitement p comme somme de deux carrés pour $p \in \{2, 5, 13, 17\}$.
2. Vérifier que que le carré d'un entier est congru à 0 ou 1 modulo 4. En déduire que si p est somme de deux carrés alors il n'est pas congru à 3 modulo 4.

On suppose désormais que p est congru à 1 modulo 4. Fixons un entier w tel que $w^2 \equiv -1 \pmod{p}$ (il existe d'après l'exercice 4) et considérons l'ensemble $S = \{0, 1, \ldots, n\}$, où n est le plus grand entier inférieur ou égal à $\sqrt{p}$, de telle sorte que $n < \sqrt{p} < n + 1$.

3. Considérons l'application $f : S \times S \to \mathbb{F}_p$ définie par $f(x, y) = x + wy$. Montrer que f n'est pas injective (indication : comparer les cardinaux de $S \times S$ et $\mathbb{F}_p$).
4. Soient $(x, y) \neq (u, v)$ deux éléments de $S \times S$ tels que $f(x, y) = f(u, v)$. En posant $a = x - u$ et $b = v - y$, montrer que l'on a la congruence

$$a \equiv bw \pmod{p}.$$

   En déduire que p divise $a^2 + b^2$.
5. Montrer que l'on a les inégalités

$$0 < a^2 + b^2 < 2p$$

   et conclure.

Exercice 6 – Notons K l'anneau quotient $\mathbb{F}_7[X]/(X^2 - X - 1)$ et $\alpha \in K$ la classe de X.

1. Vérifier que le polynôme $X^2 - X - 1 \in \mathbb{F}_7[X]$ est irréductible et en déduire que K est un corps. Quel est son cardinal ?
2. Montrer que l'on a l'identité $\alpha^{483} = 2\alpha + 1$.

Exercice 7 – D'eterminer la factorisation du polynôme $X^7 - 1$ dans $\mathbb{F}_2[X]$.

Exercice 8 – Soit $p \neq 3$ un nombre premier.

1. Montrer que le polynôme $f = X^2 + X + 1 \in \mathbb{F}_p[X]$ est irréductible si et seulement si p n'est pas congru à 1 modulo 3 (indication : utiliser le sthéorèmes de Cauchy et Lagrange).
2. En déduire que 3 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 2$ ou si p est congu à ± 1 modulo 12 (indication : utiliser le critère d'Euler de l'exercice 3).

Exercice 9 – Considérons les polynômes $f = X^9 - X + 1$ et $g = X^3 - X - 1$ sur $\mathbb{F}_3$.

1. Montrer que f n'a pas de racine dans $\mathbb{F}_9$.
2. Montrer que g est irréductible sur $\mathbb{F}_3$.
3. Vérifier que g divise f.
4. Déterminer toutes les racines de f dans $\mathbb{F}_{27}$.
5. Factoriser f dans $\mathbb{F}_3$.

Exercice 10 – Montrer que le quotient $K = \mathbb{F}_3[X]/(X^3 + 2X + 1)$ est un corps et que la classe x de X est un générateur de son groupe multiplicatif. Déterminer un entier naturel n tel que $x(x + 1) = x^n$.

Exercice 11 – Soit p un nombre premier.

1. Montrer que le polyôme $X^p - X - 1 \in \mathbb{F}_p[X]$ est irréductible (indication : utiliser le fait que si x est une racine de f dans une extension de $\mathbb{F}_p$, il en est de même pour x^p).
2. Notons K le corps $\mathbb{F}_p[X]/(f)$ et $\alpha \in K$ la classe de X. Quel est le cardinal de K ? Montrer que si p est impair, α n'est pas un générateur de $K^\times$ (indication : on pourra calculer $\alpha^{\frac{p^p-1}{p-1}}$).

Exercice 12 – Considérons le polynôme $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_3[X]$.

1. Montrer que f ne possède pas de racine dans $\mathbb{F}_9$.
2. En déduire que f est irréductible sur $\mathbb{F}_3$ et que le quotient $K = \mathbb{F}_3[X]/(f)$ est un corps.
3. Montrer que pour tout $x \in K$, en posant $y = x^9 - x$, on a la relation $y^9 = -y$. En déduire que les conditions suivantes sont équivalentes :
   - $x \notin \mathbb{F}_9$ (où l'on note $\mathbb{F}_9$ l'unique sous-corps de K de cardinal 9).
   - $y \neq 0$.
   - y est d'ordre 16.
4. Notons $\alpha \in K$ la classe de X. Montrer que l'élément $\beta = 1 - \alpha^2$ est un générateur de $K^\times$ (indication : utiliser l'identité $\beta = \alpha(\alpha^{-1} - \alpha)$ et les points précédents).
5. Alice utilise le cryptosystème El Gamal e publie la clé $(K, \beta, \alpha - 1)$. Bob transmet le cryptogramme $(1+\alpha, 1+\alpha^3)$. Calculer β^3 et en déduire la clé privée d'Alice, puis le message envoyé par Bob.

Exercice 13 – Soit p un nombre premier. Montrer que le polynôme $X^{p+1} - 1 \in \mathbb{F}_p[X]$ est scindé sur $\mathbb{F}_{p^2}$. En déduire que ses facteurs irréductibles sur $\mathbb{F}_p$ sont de degré au plus 2. Factoriser $X^6 - 1$ sur $\mathbb{F}_5$.