

FEUILLE D'EXERCICES n° 7

Extensions cyclotomiques, corps finis

Exercice 1 –

- 1) Soit un entier $n > 1$. Montrer que $\Phi_n(0) = 1$.
- 2) Montrer que pour tout $n > 1$, le polynôme $\Phi_n(X)$ est palindromique (si $\Phi(X) = \sum_{i=0}^r a_i X^i$ alors $a_{r-i} = a_i$ pour tout $0 \leq i \leq r$).

Exercice 2 – Soit un entier $n > 1$.

- 1) Exprimer dans $\mathbb{Z}[X]$ les polynômes cyclotomiques $\Phi_8(X)$ et $\Phi_{12}(X)$.
- 2) Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$ si n est impair et que $\Phi_{2n}(X) = \Phi_n(X^2)$ si n est pair.
- 3) Soit p un nombre premier qui ne divise pas n . Montrer que $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.
- 4) Soit m le produit des facteurs premiers de n . Montrer que $\Phi_n(X) = \Phi_m(X^{\frac{n}{m}})$.
- 5) Exprimer dans $\mathbb{Z}[X]$ les polynômes cyclotomiques $\Phi_{10}(X)$, $\Phi_{15}(X)$, $\Phi_{36}(X)$ et $\Phi_{60}(X)$.

Exercice 3 –

- 1) Soit un entier $n > 0$. Montrer que $x_n = \cos \frac{2\pi}{n}$ est algébrique sur \mathbb{Q} et déterminer le degré de $\mathbb{Q}(x_n)/\mathbb{Q}$.
- 2) Quel est le polynôme minimal sur \mathbb{Q} de x_n pour $n = 10, 12$ et 15 ?
- ★ 3) Quel est le polynôme minimal sur \mathbb{Q} de x_n pour n premier ?

Exercice 4 – Soit $P(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$.

- 1) Montrer que $P(X)$ est irréductible dans $\mathbb{F}_2[X]$. On pose $K = \mathbb{F}_2[X]/\langle P(X) \rangle$ et on note α la classe de X dans K .
- 2) L'anneau K est-il un corps ? Quels sont le cardinal et la caractéristique de K ?
- 3) Prouver que α est un élément primitif de K .
- 4) Combien y a-t-il d'éléments primitifs dans K ?
- 5) Soit $\beta = \alpha^2 + \alpha$. Prouver que $L = \mathbb{F}_2(\beta)$ est un sous-corps strict de K .
- 6) Déterminer $Q(X)$ le polynôme minimal de β sur \mathbb{F}_2 , ainsi que le polynôme minimal de α sur L .
- 7) Prouver que L est un corps de décomposition de $Q(X)$ sur \mathbb{F}_2 .
- 8) Déterminer les polynômes minimaux de tous les éléments de K .
- 9) Donner la décomposition en produit d'irréductibles de $X^{15} + 1$ dans $\mathbb{F}_2[X]$.

Exercice 5 – Soient p un premier *impair* et $P(X)$ un diviseur irréductible de $X^4 + 1$ dans $\mathbb{F}_p[X]$. Soit d le degré de $P(X)$. On note K le corps $\mathbb{F}_p[X]/\langle P(X) \rangle$ et α la classe de X dans K .

- 1) Quelle est la caractéristique de K ? Quel est son cardinal?
- 2) Montrer que $\alpha \in K^\times$ et que $(\alpha + \alpha^{-1})^2 = 2$.
- 3) Prouver que 2 est un carré dans \mathbb{F}_p si et seulement si $\alpha + \alpha^{-1} \in \mathbb{F}_p$.
- 4) Montrer que $\alpha^3 + \alpha^{-3} \neq \alpha + \alpha^{-1}$.
- 5) En déduire que 2 est un carré dans \mathbb{F}_p si et seulement si $p \equiv \pm 1 \pmod{8}$.

Exercice 6 – Soit K un corps fini.

- 1) Montrer que pour tout $x \in K$, il existe un polynôme $P(X) \in K[X]$ tel que $P(x) = 1$ et $P(y) = 0$ pour tout $y \in K \setminus \{x\}$.
- 2) En déduire que toute fonction f de K dans K est polynomiale (il existe $P(X) \in K[X]$ tel que pour tout $x \in K$, $f(x) = P(x)$).
- 3) Soit n un entier ≥ 1 . Montrer que toute fonction f de K^n dans K est polynomiale (il existe $P(X_1, X_2, \dots, X_n) \in K[X_1, X_2, \dots, X_n]$ tel que pour tout $(x_1, x_2, \dots, x_n) \in K^n$, $f(x_1, x_2, \dots, x_n) = P(x_1, x_2, \dots, x_n)$).

Exercice 7 – Un corps K est dit *parfait* si tout polynôme irréductible de $K[X]$ est à racines simples dans une clôture algébrique de K . Soient K un corps fini de caractéristique p et $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ un polynôme irréductible de $K[X]$ où $n \geq 1$ et $a_n \neq 0$.

- 1) On suppose que $P(X)$ a une racine double dans une clôture algébrique de K .
 - a) Montrer que $P'(X) = 0$.
 - b) Prouver que p divise n et que

$$P(X) = \sum_{k=0}^{n/p} a_{kp} X^{kp}.$$

- c) En déduire qu'il existe un polynôme $Q(X) \in K[X]$ tel que $P(X) = Q(X)^p$.
- 2) Un corps fini est-il parfait?