Feuille d'exercices n° 6

Extensions cyclotomiques, corps finis

Exercice 1

Soit un entier $n > 1$.

(1) Montrer que $\Phi_n(0) = 1$.

(2) Montrer que le polynôme $\Phi_n(X)$ est palindromique (si $\Phi_n(X) = \sum_{i=0}^{r} a_i X^i$ alors $a_{r-i} = a_i$ pour tout $0 \leqslant i \leqslant r$).

(3) Exprimer dans $\mathbf{Z}[X]$ les polynômes cyclotomiques $\Phi_8(X)$ et $\Phi_{12}(X)$.

(4) 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.

(5) Soit p un nombre premier qui ne divise pas n. Montrer que $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.

(6) Soit m le produit des facteurs premiers de n. Montrer que $\Phi_n(X) = \Phi_m(X^{\frac{n}{m}})$.

(7) Exprimer dans $\mathbf{Z}[X]$ les polynômes cyclotomiques $\Phi_{10}(X)$, $\Phi_{15}(X)$, $\Phi_{36}(X)$ et $\Phi_{60}(X)$.

Exercice 2

(1) Soit un entier $n > 0$. Montrer que $x_n = \cos\frac{2\pi}{n}$ est algébrique sur $\mathbf{Q}$ et déterminer le degré de $\mathbf{Q}(x_n)/\mathbf{Q}$.

(2) Quel est le polynôme minimal sur $\mathbf{Q}$ de x_n pour $n = 10, 12$ et 15 ?

Exercice 3

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

(1) Montrer que $P(X)$ est irréductible dans $\mathbf{F}_2[X]$. On pose $K = \mathbf{F}_2[X]/\langle P(X)\rangle$ 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 engendre le groupe multiplicatif $(K^\times, \times)$ de K.

(4) Combien y a-t-il de générateurs de $(K^\times, \times)$?

(5) Soit $\beta = \alpha^2 + \alpha$. Prouver que $L = \mathbf{F}_2(\beta)$ est un sous-corps strict de K.

(6) Déterminer $Q(X)$ le polynôme minimal de β sur $\mathbf{F}_2$, ainsi que le polynôme minimal de α sur L.

(7) Prouver que L est un corps de décomposition de $Q(X)$ sur $\mathbf{F}_2$.

(8) Déterminer les polynômes minimaux de tous les éléments de K.

(9) Donner la décomposition en produit d'irréductibles de $X^{15} + 1$ dans $\mathbf{F}_2[X]$.

Exercice 4

Soient p un premier *impair* et $P(X)$ un diviseur irréductible de $X^4 + 1$ dans $\mathbf{F}_p[X]$. Soit d le degré de $P(X)$. On note K le corps $\mathbf{F}_p[X]/\langle P(X)\rangle$ 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 $\mathbf{F}_p$ si et seulement si $\alpha + \alpha^{-1} \in \mathbf{F}_p$.

(4) Montrer que $\alpha^3 + \alpha^{-3} \neq \alpha + \alpha^{-1}$.

(5) En déduire que 2 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

Exercice 5

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 $y \in K\backslash\{x\}$.

(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 $\geqslant 1$. Montrer que toute fonction f de K^n dans K est polynomiale (il existe $P(X_1, X_2, \ldots, X_n) \in K[X_1, X_2, \ldots, X_n]$ tel que pour tout $(x_1, x_2, \ldots, x_n) \in K^n$, $f(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$).

Exercice 6

Un corps commutatif K est dit *parfait* si tout polynôme irréductible de $K[X]$ est à racines simples dans une clôture algébrique de K.
Soit K un corps commutatif et soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ un polynôme irréductible de $K[X]$ où $n \geqslant 1$ et $a_n \neq 0$. On suppose que $P(X)$ a une racine double dans une clôture algébrique de K.

(1) Montrer que $P'(X) = 0$.

(2) En déduire que tout corps de caractéristique 0 est parfait.

(3) Dans cette question K est fini de caractéristique p.

(a) Prouver que p divise n et que

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

(b) En déduire qu'il existe un polynôme $Q(X) \in K[X]$ tel que $P(X) = Q(X)^p$.

(c) Un corps fini est-il parfait ?

(4) Soient p un nombre premier et K le sous-corps de $\mathbf{F}_p(Y)$ défini par $K = \mathbf{F}_p(Y^p)$. Montrer que le polynôme $R(X) = X^p - Y^p$ est irréductible dans $K[X]$ et en déduire que K n'est pas parfait (on pourra observer que $\mathbf{F}_p(Y)$ est un corps de décomposition de $R(X)$).