# 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 $\Phi_n(X) = \sum_{i=0}^{r} a_i X^i$ alors $a_{r-i} = a_i$ pour tout $0 \leqslant i \leqslant r$).

**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 $15$ ?

**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 $\alpha$ 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 $\alpha$ 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 $L = \mathbb{F}_2(\beta)$ est un sous-corps strict de $K$.

**6)** Déterminer $Q(X)$ le polynôme minimal de $\beta$ sur $\mathbb{F}_2$, ainsi que le polynôme minimal de $\alpha$ 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 $\alpha$ 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 $p \equiv \pm 1 \bmod 8$.

**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 $\geqslant 1$. 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 7.** 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 $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme irréductible de $K[X]$ où $n \geqslant 1$ et $a_n \neq 0$. On suppose que $P$ a une racine double dans une clôture algébrique de $K$.

**1)** Montrer que $P' = 0$. En déduire que tout corps de caractéristique 0 est parfait.

**2)** 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 ?

**3)** On prend $K = \mathbb{F}_p(Y^p)$, sous-corps du corps des fractions rationnelles $\mathbb{F}_p(Y)$ ($p$ premier). Montrer que le polynôme $P_0(X) = X^p - Y^p \in K[X]$ est irréductible et en déduire que $K$ n'est pas parfait [on pourra observer que $\mathbb{F}_p(Y)$ est un corps de décomposition de $P_0$].