Université de Bordeaux

Master 1 CSI
4TCY703U - Arithmétique
Feuille 4

Exercice 1. (1) Calculer le produit des polynômes irréductibles de degré 4 dans $\mathbf{F}_2[X]$.
(2) Combien y a-t-il de polynômes irréductibles de degré 6 dans $\mathbf{F}_2[X]$?
(3) Combien y a-t-il de polynômes primitifs de degré 6 dans $\mathbf{F}_2[X]$?

Exercice 2. Soit K un corps fini de cardinal q. Soit $P(X) = X^2 - bX + c \in K[X]$ irréductible.
(1) Soit L une extension de K contenant une racine α de $P(X)$. Exprimer b en fonction de α.
(2) En déduire que $P(X)$ divise $X^q + X - b$.

Exercice 3. (1) On choisit un corps K de cardinal 64. Montrer que le polynôme $X^{21} - 1$ est scindé dans $K[X]$.
(2) Déterminer la liste des degrés des facteurs irréductibles de $X^{21} - 1$ dans $\mathbf{F}_2[X]$.

Exercice 4. Soit p un nombre premier. Soit K une extension finie de $\mathbf{F}_p$ de degré r. Soit $\alpha \in K$.
(1) Notons $P(X) = X^d - a_1 X^{d-1} + \cdots + (-1)^d a_d$ le polynôme minimal de α sur $\mathbf{F}_p$. Montrer que $\mathsf{Tr}(\alpha) = \frac{r}{d} a_1$.
(2) Posons $K = \mathbf{F}_2[Y]/\langle Y^6 + Y + 1\rangle$ et désignons par α la classe de Y dans K. On sait que K est un corps. Calculer $\mathsf{Tr}(\alpha^k)$ pour tout $k \in \{0, 1, 2, 3, 4, 5\}$.

Exercice 5. Factoriser le polynôme $X^{11} - 1$ dans $\mathbf{F}_2[X]$.

Exercice 6. Soit K un corps fini de caractéristique 2.
(1) Soient m un entier $\geqslant 1$ et $x \in K^\times$ d'ordre $2^m + 1$. Déterminer le degré de x sur $\mathbf{F}_2$.
(2) Soit $x \in K^\times$ d'ordre 9. Trouver le polynôme minimal de x sur $\mathbf{F}_2$.

Exercice 7. Soient K un corps fini de cardinal q et L une extension finie de K de degré r. On pose $n = \frac{q^r - 1}{q - 1} = q^{r-1} + \cdots + q + 1$. On note $\mathsf{N}\colon L^\times \to L^\times$ l'application qui à x associe x^n.
(1) Vérifier que N est un morphisme de groupes et que $N(x^q) = N(x)$ pour tout $x \in L^\times$.
(2) Démontrer que $\mathsf{N}(L^\times) \subset K^\times$.
(3) Prouver que $\#\,\mathsf{N}^{-1}(y) = n$ pour tout $y \in K^\times$.