Université de Bordeaux

Master 1 CSI
4TCY703U - Arithmétique
Feuille 3

Exercice 1. On pose $K = \mathbf{F}_2[Y]/\langle Y^3 + Y + 1\rangle$ et on note α la classe de Y dans K.
(1) Vérifier que K est un corps.
(2) Soit $x \in K^\times$ tel que $x \neq 1$. Montrer que le polynôme minimal de x sur $\mathbf{F}_2$ est X^3+X+1 ou X^3+X^2+1.
(3) Quel est le polynôme minimal de α^2+1 sur $\mathbf{F}_2$?
(4) Factoriser X^3+X^2+1 dans $K[X]$.

Exercice 2. (1) Soient K un corps fini de cardinal 32 et $x \in K^\times$ tel que $x \neq 1$. Montrer que x est primitif dans K.
(2) Soient L un corps fini de cardinal 27 et $x \in L^\times$ tel que $x \notin \{1,-1\}$. Prouver que x ou $-x$ est primitif dans L.

Exercice 3. Posons $K = \mathbf{F}_2[Y]/\langle Y^4+Y^3+Y^2+Y+1\rangle$ et notons α la classe de Y dans K.
(1) Démontrer que K est un corps.
(2) Calculer $(\alpha+1)^5$, puis montrer que $\alpha+1$ est primitif dans K.
(3) L'élément α est-il primitif dans K ?

Exercice 4. On pose $A = \mathbf{F}_2[Y]/\langle Y^6+Y+1\rangle$ et on note α la classe de Y dans A.
(1) Calculer α^9, α^{21} et α^{63}.
(2) Quel est l'ordre de α dans le groupe multiplicatif $A^\times$? En déduire que A est un corps.
(3) Quel est le polynôme minimal de α^{21} sur $\mathbf{F}_2$?
(4) Trouver le degré de α^9 sur $\mathbf{F}_2$.
(5) Quels sont les éléments de $\mathbf{F}_2(\alpha^9) \cap \mathbf{F}_2(\alpha^{21})$?

Exercice 5. (1) Combien y a-t-il de polynômes unitaires irréductibles de degré 2 dans $\mathbf{F}_5[X]$?
(2) Combien y a-t-il de polynômes unitaires primitifs de degré 2 dans $\mathbf{F}_5[X]$?

Exercice 6. Soient p un nombre premier, K un corps de caractéristique p et $b \in K$. Posons $Q(X) = X^p - X - b$. On choisit une extension L de K contenant une racine α de $Q(X)$.
(1) Montrer l'égalité $Q(X) = \prod_{k\in\mathbf{F}_p} (X-\alpha-k)$ dans $L[X]$ (*indication :* on pourra d'abord calculer $Q(\alpha+k)$ pour tout $k \in \mathbf{F}_p$).
(2) Soit $P(X) = X^d - a_1X^{d-1} + \cdots + (-1)^d a_d$ un facteur unitaire de $Q(X)$ dans $L[X]$. Démontrer que $a_1 - d\alpha \in \mathbf{F}_p$, puis que $a_1^p - a_1 = db$.
(3) Prouver que $Q(X)$ est irréductible dans $K[X]$ si et seulement si $Q(X)$ n'a pas de racine dans K.
(4) Soit $c \in \mathbf{F}_p^\times$. Montrer que le polynôme $X^p - X - c$ est irréductible dans $\mathbf{F}_p[X]$.