Master CSI 1 — 2006-2007

Arithmétique 1

Feuille d'exercices n° 4.

1

1. Faire la liste des polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.
2. Quels sont ceux qui sont primitifs ?
3. Soit $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ avec $\alpha^2 + \alpha - 1 = 0$. En utilisant le Frobenius, déterminez le polynôme minimal sur $\mathbb{F}_3$ de chacune des puissances de α

2 Si $q = p^k$ et $\alpha \in \mathbb{F}_q$, on appelle classe de conjugaison de α l'ensemble $C(\alpha) = \{\sigma^i(\alpha) : i \geq 0\}$ des conjugués de α.

1. Expliquez pourquoi le corps F_{2^6} contient toutes les racines du polynôme $X^{21} - 1 \in \mathbb{F}_2[X]$.
2. Soit $\alpha \in F_{2^6}$ un élément d'ordre multiplicatif 21. Déterminez les classes de conjugaison de tous les α^k, $0 \leq k \leq 20$, et expliquez pourquoi elles forment une partition de l'ensemble des racines du polynôme $X^{21} - 1 \in \mathbb{F}_2[X]$.
3. Expliquez pourquoi les éléments d'une même classe de conjugaison ont même ordre multiplicatif. Déterminez celui-ci dans le cas particulier précédent.

3 (Le Frobenius relatif). Soit $K \subset L$, avec $K = \mathbb{F}_q$, $q = p^k$ et $L = \mathbb{F}_{q'}$, $q' = p^l$. Le Frobenius σ est défini par $\sigma(x) = x^p$. On pose $\sigma_q := \sigma^k$ et on l'appelle le Frobenius relatif à K.

1. Montrez que k divise l
2. Montrez que, pour tout $\alpha \in L$, $\alpha \in K \iff \sigma_q(\alpha) = \alpha$.
3. Montrez que, pour tout $\alpha \in L$, $\sigma_q(\alpha)$ est racine du polynôme minimal de α sur K.
4. Application : $K = \mathbb{F}_8$ et $[L : K] = 2$. Soit $\beta \in L$ d'ordre multiplicatif 9.
   (a) Partitionez l'ensemble des puissances de β en classes de conjugaison relativement à K.
   (b) Montrez que β^3 appartient à un sous-corps à 4 éléments de L. Quel est son polynôme minimal sur $\mathbb{F}_2$? En utilisant le Frobenius, montrez que $\beta^6 + \beta^3 = 1$ et en déduire le polynôme minimal de β sur $\mathbb{F}_2$.
5. On suppose que $K = \mathbb{F}_q$, $q = p^k$, et que $[L : K] = 2$. Soit $\beta \in L$, on suppose que $\beta \notin K$. Montrez que le polynôme minimal de β sur K est le polynôme $(X - \beta)(X - \beta^q)$. En déduire que $\beta + \beta^q$ et β^{1+q} appartiennent à K.

4 Soit α un élément non nul d'une extension K de $\mathbb{F}_2$, d'ordre r dans K^*. Soit k le plus petit entier tel que $\alpha \in \mathbb{F}_{2^k}$.

1. Montrez que k est l'ordre de 2 dans le groupe $(\mathbb{Z}/r\mathbb{Z})^*$.
2. Montrez que $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^k}$ et que α n'est pas nécessairement primitif.
3. On suppose $r = 3(4^m + 1)$ avec $m \geq 1$. Montrez que $k = 4m$.
4. Quel est le cardinal de la classe de conjugaison de α ?
5. Quel est l'ordre multiplicatif de α^3 ?
6. Quel est le cardinal de la classe de conjugaison de α^3 ?
7. Montrez que α et α^3 ne sont pas conjugués mais que α^3 et α^{-3} le sont.
8. Montrez que α et α^{-1} ne sont pas conjugués.