Fiche 4
26 février 2014

Exercice 1 (Caractéristique non nulle).
On définit le polynôme $f(X) = X^p - X - t$ dans $\mathbb{F}_p(t)[X]$, avec t transcendant sur $\mathbb{F}_p$.

1. Montrer que si α est une racine de f, alors $\alpha + i$ en est une aussi ($i \in \mathbb{Z}$).
2. Montrer que $f(X)$ est irréductible sur $\mathbb{F}_p(t)$.
3. Montrer que le groupe de Galois de $f(X)$ sur $\mathbb{F}_p(t)$ est cyclique d'ordre p.

Exercice 2 (Caractéristique non nulle).
Soit k un corps de caractéristique non nulle p. Soit F une extension galoisienne cyclique de degré p de k. Soit σ un générateur du groupe de Galois de F sur k.
(a) Montrer que l'endomorphisme $k-$linéaire de F :

$$S : \alpha \mapsto \alpha - \sigma(\alpha)$$

est nilpotent.
(b) Soit $\alpha \in \ker S^2 \setminus \ker S$. Montrer que $\beta = \frac{\alpha}{\sigma(\alpha)-\alpha}$ vérifie $\sigma(\beta) = \beta + 1$.
(c) En déduire que β vérifie une équation de la forme $X^p - X - a = 0$ avec $a \in k$.

Exercice 3 (Corps finis).

1. Déterminer tous les polynômes de degré 2 ou 3 irréductibles sur le corps $\mathbb{F}_2$. Donner les tables d'addition et de multiplication d'un corps à 4 éléments.
2. Déterminer les polynômes de degré 2 irréductibles sur le corps $\mathbb{F}_3$. Donner les tables d'addition et de multiplication d'un corps à 9 éléments.
3. Construire un corps ayant 8 éléments.

Exercice 4 (Groupes d'automorphismes d'un corps fini).

1. Soit K un corps fini de caractéristique p et de cardinal $q = p^n$. Montrer que le groupe d'automorphismes de K est d'ordre n, cyclique engendré par l'autmorphisme de Frobenius $x \longmapsto x^p$.
2. On peut construire un corps à 8 éléments de deux manières différentes. Expliciter tous les isomorphismes possibles entre les deux corps.

Exercice 5 (Carrés dans un corps fini).
I.

1. Montrer que dans un corps fini de caractéristique 2, tout élément est un carré.
   A partir de maintenant, p est supposé être un nombre premier impair et $q = p^n$ avec $n \in \mathbb{N}^*$.
2. Montrer que les carrés non nuls de $\mathbb{F}_q$ forment un sous-groupe du groupe multiplicatif de $\mathbb{F}_q$. En déduire le cardinal de l'ensemble des carrés de $\mathbb{F}_q$.
3. Montrer que les carrés non nuls de $\mathbb{F}_q$ forment le noyau de l'endomorphisme du groupe multiplicatif défini par l'association $x \mapsto x^{\frac{q-1}{2}}$.
4. En déduire que -1 est un carré dans $\mathbb{F}_q^*$ si et seulement si $q \equiv 1(\mod 4)$.
5. En déduire qu'il existe une infinité de nombres premiers de la forme $4k+1$.
6. Montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$.
   A partir de maintenant, on fixera un corps fini K de caractéristique impaire.
7. Montrer que pour toute paire d'éléments (α, β) dans $K^* \times K^*$, il existe $(a, b) \in K \times K$ tels que $\alpha a^2 + \beta b^2 = 1$.
8. Si maintenant E est un K-espace vectoriel de dimension finie n et que Q est une forme quadratique non dégénérée sur E, alors il existe une base de E dans laquelle Q se représente par une matrice diagonale de la forme $(1, \ldots, 1, d)$ avec $d \in K^*$.

II. Montrer que dans un corps fini arbitraire, le polynôme $X^4 + aX^2 + b^2$ est toujours irréductible quelles que soient les valeurs de a et de b.

Exercice 6 (Polynômes sur un corps fini, irréductibilité, ordre).

1. Montrer que X^4+2 est irréductible sur $\mathbb{F}_5$. Trouver son ordre e. Déterminer la décomposition en facteurs irréductibles du polynôme $X^e - 1$.
2. Ecrire la factorisation de $X^9 - X$ en facteurs irréductibles dans $\mathbb{F}_3[X]$, et déterminer les facteurs primitifs. Même question pour $X^8 - X$ dans $\mathbb{F}_2[X]$.

Exercice 7 (Quand 2 est un carré).
Soit p un nombre premier impair. Montrer que le polynôme $X^4 + 1$ admet une racine α dans $\mathbb{F}_{p^2}$. Montrer que $y = \alpha + \alpha^{-1}$ vérifie $y^2 = 2$. En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.

Exercice 8 (Somme des puissances).
Soit K un corps fini à au moins 4 éléments. Montrer que $\sum_{x \in K} x^2 = 0$. Quelle conclusion est-ce qu'on peut tirer si on remplace 2 par $s \in \mathbb{N}^*$?