Université Paris 7 **3 octobre 2016**
Algèbre

TD3 : corps finis

1 Corps

Exercice 1 :
Existe-t-il des corps à 30, à 31, à 32 éléments ? les décrire.

Exercice 2 :

1. Montrer que $\mathbb{F}_7$ et $\mathbb{F}_{13}$ contiennent chacun des éléments d'ordre 6. Combien pour chacun ?
2. Quels sont les plus petits corps qui contiennent un élément d'ordre 9 ?
3. À quelle condition $\mathbb{F}_q$ possède-t-il un élément d'ordre n ? (une racine n-ième de l'unité).

2 Irréductibles

Exercice 3 :

1. Montrer que $x^7 + x + 1$ est irréductible sur $\mathbb{F}_2$.

Exercice 4 :
On considère le polynôme $x^n - 1$ sur $\mathbb{F}_p$ pour $p \nmid n$.

1. Montrer qu'il est scindé sur $\mathbb{F}_q$ si et seulement si $n \mid q - 1$.
2. En déduire que $x^n - 1$ possède un facteur irréductible de degré k sur $\mathbb{F}_p$, où k est l'ordre de p modulo n.

Exercice 5 :
Montrer que $\text{pgcd}(x^{p^n} - x, x^{p^m} - x) = x^{p^{\text{pgcd}(m,n)}} - x$.

3 Frobenius

Exercice 6 :
On considère le corps $\mathbb{F}_q$, où $q = p^n$.

1. Montrer que le Frobenius ϕ_p est d'ordre n dans le groupe des automorphismes de $\mathbb{F}_q$.
2. En déduire le groupe des automorphisme de $\mathbb{F}_q$ est formé des puissances de ϕ_p.

Exercice 7 : Galois
Soit $P \in \mathbb{F}_p[x]$, et α une racine de P dans une extension $\mathbb{F}_q$.

1. Montrer que α^p est racine de P
2. On suppose que P est irréductible de degré k. Montrer que $\alpha, \alpha^p \dots \alpha^{p^{k-1}}$ sont les k racines distinctes de P.
3. Soit désormais P quelconque. Montrer que ϕ_p permute les racines de P dans une extension de décomposition, et que les orbites de la permutation correspondent aux facteurs irréductibles de P.

Exercice 8 :

1. Montrer que $x^p - x - 1$ n'a aucune racine dans $\mathbb{F}_p$.
2. Calculer par récurrence $x^{p^k} \bmod x^p - x - 1$.
3. En déduire que $x^p - x - 1$ est irréductible sur $\mathbb{F}_p$.
4. Montrer de même que $x^q - x - 1$ est irréductible sur $\mathbb{F}_q$.

4 EQUATIONS

Exercice 9 :

Montrer que dans un corps fini, tout élément s'écrit comme somme de deux carrés.

Exercice 10 :

On considère un polynôme $P = ax^2 + bx + c$ sur $\mathbb{F}_p$, avec $a \neq 0$ et $p \neq 2$.

1. Montrer que P est scindé dans $\mathbb{F}_{p^2}$.

2. On considère deux racines α, β de P dans $\mathbb{F}_{p^2}$, et on pose $\Delta = (\alpha - \beta)^2$. Calculer Δ en fonction de a, b, c. En déduire que $\Delta \in \mathbb{F}_p$.

3. Montrer que $\alpha \in \mathbb{F}_p$ si et seulement si $\beta \in \mathbb{F}_p$, si et seulement si Δ est un carré dans $\mathbb{F}_p$, si et seulement si $\Delta^{\frac{p-1}{2}} = 1 \bmod p$.

4. Inversement, montrer que P est irréductible si et seulement si $\Delta^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Exercice 11 :

Soient $p, q \in \mathbb{F}_4$ avec $q \neq 0$. On considère l'équation $E : x^3 + px + q = 0$ sur $\mathbb{F}_4$.

1. Montrer que l'application $f : x \mapsto x^4 + px^2 + qx$ est une application linéaire du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_4$.

2. Montrer que les solutions de l'équation E sont les vecteur non nuls du noyau de f.

3. En déduire que l'équation possède $2^d - 1$ solutions dans $\mathbb{F}_4$, où $d \in \{0, 1, 2\}$ est la dimension de $\ker(f)$.

4. Montrer que $x^3 + \alpha x + 1$ est irréductible $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$.

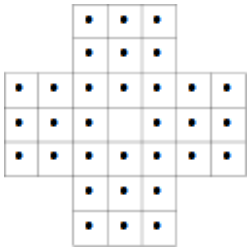
5. On considère $\mathbb{F}_8 = \mathbb{F}_2[\beta]$ où $\beta^3 = \beta + 1$. Résoudre $x^3 + \beta = 0$ dans $\mathbb{F}_8$.

5 SOLITAIRE

Exercice 12 :

On considère le jeu de solitaire, dans lequel le joueur s'efforce de ne laisser plus qu'une bille par des éliminations suivant une règle de saute-mouton.
On indice les coordonnées des cases dans $\mathbb{Z}$. En notant α un générateur de $\mathbb{F}_4$, on peut pour toute disposition de billes de coordonnées x, y former les sommes

$$A = \sum_{x,y} \alpha^{x+y} \text{ et } B = \sum_{x,y} \alpha^{x-y}.$$



1. Montrer qu'au terme d'un mouvement valide, la pair $\{A, B\}$ est conservée.

2. On part de la position où seule la bille centrale ($x = y = 0$) est enlevée. Que valent A et B ?

3. Montrer que dans une position finale la bille restante a des coordonnées dans $3\mathbb{Z}$.

4. Quelles sont les positions finales valides ? on peut montrer qu'on les atteint effectivement.