ENS Lyon 2011 - 2012
Master 1

Algèbre Approfondie

27.09.2011

TD 2

Corps finis

Exercice 1.

1. Rappeler pourquoi l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

   Si p est un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.
2. (a) Soit K un corps fini. Montrer :
      i. la caractéristique de K est un nombre premier p ;
      ii. le corps K contient $\mathbb{F}_p$.
   (b) En déduire que tout corps fini est de cardinal p^n, pour un nombre premier p et un entier positif n.
3. Réciproquement, soit p un nombre premier et soit $q = p^n$ une puissance de p. On note L le corps de décomposition du polynôme $X^q - X \in \mathbb{F}_p[X]$ dans une clôture algébrique fixée de $\mathbb{F}_p$.
   (a) Soit M l'ensemble des racines du polynôme $X^q - X$ dans L. Montrer que M est un corps qui contient $\mathbb{F}_p$, puis que $M = L$.
   (b) Montrer que le corps L contient exactement q éléments.
   (c) Montrer que tout corps fini à q éléments est isomorphe à L.

   On note alors $\mathbb{F}_q$ le corps fini à q éléments, unique à isomorphisme près.

Exercice 2.

Soit p un nombre premier et soit K un corps de caractéristique p.

1. Montrer la relation : pour tous $a, b \in K$, $(a+b)^p = a^p + b^p$.
2. En déduire que l'application $F : x \mapsto x^p$ est un endomorphisme du corps K dont les éléments fixes sont précisément les éléments du sous-corps $\mathbb{F}_p$. On l'appelle l'endomorphisme de Frobenius. Montrer que si K est de plus fini, l'application F est un automorphisme.

Exercice 3.

Soit K un corps. Montrer que tout sous-groupe fini du groupe multiplicatif K^* est cyclique.

On pourra montrer et utiliser la question suivante :
– Soit G un groupe fini d'ordre n. On suppose que pour tout diviseur d de n, le groupe G a au plus un sous-groupe cyclique d'ordre d. Montrer que G est cyclique.

Exercice 4.

Soit p un nombre premier.

1. Soit $n \geq 1$ un entier. Déterminer les sous-corps du corps fini $\mathbb{F}_{p^n}$.
2. *Exemple.* Dessiner le treillis des sous-corps de $\mathbb{F}_{p^{12}}$.
3. Soit Ω une clôture algébrique de $\mathbb{F}_p$. Soient $\mathbb{F}_{p^a}$ et $\mathbb{F}_{p^b}$ deux extensions finies de $\mathbb{F}_p$ dans Ω. Montrer :

$$\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b} \quad \Leftrightarrow \quad a|b.$$

Exercice 5.

1. (a) Montrer que tout corps fini est isomorphe à un quotient $\mathbb{F}_p[X]/P(X)$ pour un certain nombre premier p et un certain polynôme $P \in \mathbb{F}_p[X]$ irréductible.
   (b) En déduire que pour tout corps fini K et pour tout entier n, il existe dans $K[X]$ au moins un polynôme irréductible unitaire de degré n.
2. *Exemples.*
   (a) Déterminer les polynômes irréductibles de degré ≤ 4 de $\mathbb{F}_2[X]$.
   (b) Construire un corps fini à 8 éléments, à 9 élements, à $343 = 7^2$ éléments.

Exercice 6.

Soit p un nombre premier.

1. Montrer que sur $\mathbb{F}_p$ il y a exactement $(p^2-2)/2$ polynômes irréductibles unitaires de degré 2, et $(p^3-p)/3$ polynômes irréductibles unitaires de degré 3.
2. Soit q une puissance de p. Pour tout entier $d \geq 1$, notons $I(d,q)$ l'ensemble des polynômes irréductibles unitaires de degré d dans $\mathbb{F}_q[X]$. Montrer :

$$\forall n \geq 1, \quad X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P.$$

   En particulier, $q^n = \sum_{d|n} d\,\gamma(d,q)$, où $\gamma(d,q)$ est le cardinal de $I(d,q)$.

Exercice 7.

Soit p un nombre premier, soit K un corps fini de cardinal p^n, $n \geq 1$.

1. Montrer que les automorphismes de K sont les puissances de l'automorphisme de Frobenius F, et qu'ils forment un groupe cyclique d'ordre n.
2. Pour tout entier $r \geq 1$, montrer que les éléments fixés par F^r forment un sous-corps de K.

Exercice 8.

Soit p un nombre premier, soit q une puissance de p. On appelle *racine primitive* du corps $\mathbb{F}_q$ tout générateur du groupe cyclique $\mathbb{F}_q^\times$.

1. Trouver une racine primitive du corps $\mathbb{F}_{25}$.
2. Soit $n \geq 1$ un entier. On appelle *polynôme primitif* de $\mathbb{F}_p[X]$ tout polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ dont une racine au moins est une racine primitive de $\mathbb{F}_{p^n}$.
   (a) Montrer que tout générateur de $\mathbb{F}_{p^n}^*$ est racine d'un unique polynôme irréductible de $\mathbb{F}_p[X]$, de degré n.
   (b) En déduire que dans $\mathbb{F}_p[X]$, il y a $\varphi(p^d-1)/d$ polynômes primitifs de degré d.