Algèbre — Année 2011/2012
ENS Cachan — Dimitri Ara

TD 6
Corps finis

Exercice 1 (Description du corps à 16 éléments).

1. Déterminer tous les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.
2. Pourquoi les anneaux
$$\mathbb{F}_2[X]/(X^4+X^3+X^2+X+1) \quad \text{et} \quad \mathbb{F}_2[X]/(X^4+X+1)$$
sont-ils isomorphes ?
3. Calculer l'ordre multiplicatif de la classe de X dans chacun de ces quotients.
4. Construire un isomorphisme explicite.

Exercice 2 (Irréductibilité modulo p). Soient p un nombre premier et $f \in \mathbb{F}_p[X]$ un polynôme irréductible de degré d sur le corps à p éléments.

1. Soit $n \geq 1$. Montrer que les conditions suivantes sont équivalentes :
   (a) f divise $X^{p^n} - X$;
   (b) f a une racine dans $\mathbb{F}_{p^n}$;
   (c) d divise n.
2. En déduire que si f admet une racine dans $\mathbb{F}_{p^n}$ alors f est scindé dans $\mathbb{F}_{p^n}$.
3. Montrer que les racines de f sont distinctes.

Exercice 3 (Théorème de l'élément primitif – cas fini).

1. Notons φ la fonction indicatrice d'Euler. Rappeler pourquoi pour $n \geq 1$, on a
$$n = \sum_{d|n} \varphi(d).$$
2. Soit G un groupe d'ordre fini n. On suppose que pour tout diviseur d de n, l'ensemble des x tels que $x^d = 1$ a au plus d éléments. Montrer que G est cyclique.
3. Soient K un corps et G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.
4. En déduire que toute extension finie d'un corps fini est monogène.

Exercice 4 (Polynômes cyclotomiques dans les corps finis). Soient p un nombre premier et d un entier premier à p. On notera Φ_d le d-ième polynôme cyclotomique et φ la fonction indicatrice d'Euler.

1. Soit Ω un corps algébriquement clos de caractéristique p. Montrer que les racines de Φ_d dans Ω sont les racines primitives d-ième de l'unité.
2. Soit $n \geq 1$. Montrer que les conditions suivantes sont équivalentes :
   (a) d divise $p^n - 1$;
   (b) Φ_d est scindé dans $\mathbb{F}_{p^n}$;
   (c) Φ_d a une racine dans $\mathbb{F}_{p^n}$.
3. Soit m l'ordre de p dans $(\mathbb{Z}/d\mathbb{Z})^*$. Montrer que Φ_d se décompose dans $\mathbb{F}_p$ en un produit de $\varphi(d)/m$ polynômes irréductibles de degré m.
4. En déduire que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais est réductible modulo tout nombre premier p.

Exercice 5 (Un « petit » théorème de Dirichlet). Soit n un entier supérieur ou égal à 2.

1. Soit k un entier et p un facteur premier de $\Phi_n(k!)$. Montrer que p est congru à 1 modulo n et que $p > k$.
2. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

Exercice 6 (Automorphismes d'un corps fini). Soit K un corps fini. Déterminer le groupe des automorphismes de K.

Exercice 7 (Théorème de Chevalley-Warning). Soit K un corps fini de caractéristique p.

1. Soit d un entier positif ou nul. Montrer qu'on a
$$\sum_{x \in K} x^d = \begin{cases} -1 & \text{si } d \geq 1 \text{ et } q-1 \text{ divise } d, \\ 0 & \text{sinon.} \end{cases}$$
(On conviendra que $0^0 = 1$.)
2. Soit $f \in K[X_1, \ldots, X_n]$ un polynôme à n indéterminées sur K de degré strictement inférieur à n. Montrer que le nombre de zéros de f est divisible par p. (On pourra chercher à exprimer la fonction indicatrice des zéros de f de manière polynômiale.)
3. En déduire que toute forme quadratique sur K d'au moins trois variables admet un zéro non trivial.

Exercice 8 (Théorème de Wedderburn). Soit K une algèbre à division de cardinal fini. On se propose de montrer que K est commutative, *i.e.* que K est un corps.

1. Soit
$$Z = \{x \in K ; \forall y \in K \ xy = yx\}$$
le centre de K. Vérifier que Z est un corps. On notera q son cardinal et n la dimension de K sur Z.
2. Soit d un diviseur strict de n. Montrer que $\Phi_n(q)$ divise $(q^n - 1)/(q^d - 1)$.
3. On fait agir K^* sur lui-même par conjugaison. Écrire l'équation aux classes. En déduire que $\Phi_n(q)$ divise $q - 1$.
4. En déduire que $n = 1$ et donc que K est un corps.