**ENS Lyon** 2011 - 2012
Agrégation

# Algèbre

## Corps finis

---

## Corps finis

**Exercice 1.** Répéter dix fois «$\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$».

**Exercice 2.** Construire les tables d'addition et de multiplication de $\mathbf{F}_9$ et $\mathbf{F}_{16}$ .

**Exercice 3.** Combien le groupe $\mathbf{F}_q^\times$ possède-t-il de générateurs ?

**Exercice 4. (Théorème de Wedderburn par les polynômes cyclotomiques)**
Soit $A$ une algèbre à division ($c$-$à$-$d$ un corps non commutatif) de cardinal fini.

1. Montrer que $A$ est de cardinal $q^n$, où $q$ est une puissance d'un nombre premier, égale au cardinal du centre $k$ de $A$.
2. Montrer que $A-\{0\}$ agit sur lui-même par automorphismes intérieurs. Montrer que si $x \in A - \{0\}$, alors $\mathrm{Stab}_x \cup \{0\}$ est un sous-$k$-espace vectoriel de $A$.
3. On suppose désormais que $A$ n'est pas commutatif. Montrer que les orbites de l'action précédemment décrite sont de cardinal $\frac{q^n-1}{q^d-1}$, avec $d \mid n$.
4. Montrer que pour $d \mid n$, $d \neq n$, on a $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$, où $\Phi_n$ est le $n$-ième polynôme cyclotomique.
5. En appliquant la formule des classes, déduire des question précédentes que $|\Phi_n(q)| \leq q-1$.
6. En déduire une contradiction, et donc que $A$ est un corps commutatif.

**Exercice 5. (Sur le huitième polynôme cyclotomique)**
On rappelle que le polynôme $\Phi_8(X) = X^4 + 1$ est irréductible sur $\mathbb{Z}$. Le but de cet exercice est de montrer (de deux manières différentes) qu'il est réductible dans tout corps fini.

1. Écrire la décomposition de $\Phi_8$ en facteurs irréductibles dans $\mathbb{F}_2[X]$.

Dans toute la suite, $p$ désigne un nombre premier différent de 2.

2. (a) Donner toutes les manières possibles d'écrire $\Phi_8$ comme produit de deux polynômes de degré 2 dans $\mathbb{C}[X]$.
   (b) Montrer qu'au moins l'un des trois éléments $-1$, 2 et $-2$ est un carré dans $\mathbb{F}_p$.
   (c) En déduire que $\Phi_8$ est réductible dans $\mathbb{F}_p[X]$.
3. (a) Montrer que $\Phi_8$ est réductible si et seulement si il possède une racine dans $\mathbb{F}_{p^2}$.

(b) Montrer que $\Phi_8$ possède une racine dans $\mathbb{F}_{p^2}$ si et seulement si 8 divise $p^2-1$.

(c) En déduire que $\Phi_8$ est réductible dans $\mathbb{F}_p[X]$.

**Exercice 6. (Un critère d'irréductibilité)**
Soit $k$ un corps fini de cardinal $q$, et $\overline{k}$ une clôture algébrique de $k$.
Soit $P$ un polynôme à coefficients dans $k$, de degré $d \geq 1$. Montrer que $P$ est irréductible dans $k[X]$ si et seulement si il vérifie les deux conditions suivantes :

(i) $P$ divise $X^{q^d} - X$,

(ii) pour tout nombre premier $p$ divisant $d$, $P$ et $X^{q^{d/p}} - X$ sont premiers entre eux.

**Exercice 7. (Théorème de Chevalley-Warning)**

Soient $f_k \in \mathbf{F}_q[X_1, \ldots, X_n]$ des polynômes à $n$ variables à coefficients dans $\mathbf{F}_q$ (avec $q = p^m$) tels que $\sum_k \deg(f_k) < n$ et $V$ l'ensemble de leurs zéros communs dans $\mathbf{F}_q^n$. Le but de l'exercice est de montrer la congruence $\mathrm{card}(V) \equiv 0 \pmod{p}$.

1. Calculer pour tout $h \in \mathbf{N}$ la somme $S_q(h) = \sum_{x \in \mathbf{F}_q} x^h$, où l'on a posé $x^0 = 1$, même si $x = 0$.
2. Montrer que $\mathrm{card}(V) \equiv \sum_{x \in \mathbf{F}_q^n} \prod_k (1 - f_k(x_1, \ldots, x_n)^{q-1}) \pmod{p}$.
3. Montrer enfin que lorsque $j_1, \ldots, j_n \in \mathbf{N}$ sont des entiers qui vérifient $j_1 + \cdots + j_n < n(q-1)$, on a $\sum_{(x_1,\ldots,x_n) \in \mathbf{F}_q^n} x_1^{j_1} \cdots x_n^{j_n} = 0$ puis conclure.
4. Soit $P$ homogène de degré $d < n$. Montrer que $P$ admet un zéro dans $\mathbf{F}_q^n$ différent de $(0, \ldots, 0)$.
5. Si $\sum_k \deg f_k < n$ et si les $f_k$ sont sans terme constant, montrer que les $f_k$ on un zéro non trivial commun.

**Exercice 8. (Interpolation de Lagrange)**
Montrer qu'une fonction $f : \mathbf{F}_q \to \mathbf{F}_q$ est de manière unique la fonction associée à un polynôme de degré au plus $q-1$.
De même, montrer que tout fonction $g : \mathbf{F}_q^n \to \mathbf{F}_q$ est de manière unique la fonction associée à un polynôme $P$ de $\mathbf{F}_q[X_1, \ldots, X_n]$ tel que $\deg_{X_i} P \leq q-1$.

**Exercice 9. (Un lien avec la théorie des groupes)**
Déterminer les groupes dont le groupe d'automorphismes est trivial.