Université de Nice-Sophia-Antipolis
31 mars 2010
Préparation à l'agrégation (Rémy Oudompheng)

Algèbre : développement n°31
Polynômes irréductibles sur $\mathbb{F}_q$ et formule de Möbius

Références : Francinou, Perrin (III.2–3 : exercices 7 et 8).

**Exercice 1** (Convolution de Dirichlet et formule d'inversion de Möbius)**.** Soit $\mathcal{D}$ l'ensemble des suites $(a_n)_{n\in\mathbb{N}^*}$ à valeurs dans un certain anneau $A$. On définit le *produit de convolution de Dirichlet* de deux suites $(a_n)$ et $(b_n)$ par la formule

$$c_n = \sum_{pq=n} a_p b_q$$

et on note $c = a * b$.

1. Montrer que $\mathcal{D}$, muni des opérations $+$ et $*$, forme un anneau commutatif. Quelle est son unité ?
2. Cette partie est facultative.
   a) On note $\iota^{(p)}$ la suite définie par $\iota^{(p)}_n = 1$ si $n$ est une puissance de $p$ (et 0 sinon). On note $\mu^{(p)}$ la suite définie qui vaut 1 en 1, $-1$ en $p$ et 0 sinon. Montrer que $\mu^{(p)} * \iota^{(p)} = 1$.
   b) Soit un ensemble fini de nombres premiers $\mathcal{P}$. Montrer que le produit de convolution $\iota^{\mathcal{P}}$ des $\iota^{(p)}$, pour $p \in \mathcal{P}$ est la fonction indicatrice des nombres dont les facteurs premiers sont dans $\mathcal{P}$.
   c) Soit $\mu^{\mathcal{P}}$ l'inverse de $\iota^{\mathcal{P}}$. Montrer que $\mu^{\mathcal{P}}(n)$ est $(-1)^k$ si $n$ est produit de $k$ éléments distincts de $\mathcal{P}$, 0 sinon.
3. On note $\iota$ la suite constante 1. Montrer que la *fonction de Möbius* $\mu$ qui vaut $(-1)^k$ pour les nombres qui sont produit de $k$ facteurs premiers distincts, et 0 sinon, est l'inverse de $\iota$.
4. En déduire la formule d'inversion de Möbius : soient $f$ et $g$ deux fonctions $\mathbb{N}^* \to A$, alors
$$\forall n,\ f(n) = \sum_{d|n} g(d) \iff \forall n,\ g(n) = \sum_{pq=n} \mu(p) f(q)$$
5. Application : montrer que $f = \mathrm{Id}$ et $g = \phi$ (la fonction indicatrice d'Euler) vérifient la formule. Vérifier qu'on retrouve la formule $\phi(n)/n = \prod_{p \text{ premier},\, p|n}(1 - 1/p)$.

**Exercice 2** (Extensions de corps finis)**.** Soit $k$ un corps fini de cardinal $q$.

1. On note $I_n(q)$ le nombre de polynômes à coefficients dans $k$, irréductibles, unitaires, de degré $n$. Montrer que ce nombre ne dépend pas du choix de $k$.
2. Soit $K$ une extension de degré $n$ de $k$. Montrer que le polynôme minimal d'un élément de $K$ a un degré diviseur de $n$.
3. On définit une application $K \to k[X]$ qui associe à un élément de $K$ son polynôme minimal unitaire. Montrer que cette application a pour image l'ensemble des polynômes irréductibles de degré divisant $n$.

   Quel est le nombre d'antécédents d'un polynôme irréductible donné ?

**Exercice 3** (Nombre de polynômes irréductibles)**.** On note toujours $I_n(q)$ le nombre de polynômes irréductibles unitaires de degré $n$ sur un corps fini de cardinal $q$.

1. Montrer que $q^n = \sum_{d|n} d \cdot I_d(q)$. En déduire que $I_n(q) = \frac{1}{n}\sum_{n=ab} \mu(a) q^b$.
2. Donner une approximation de la probabilité pour un polynôme de degré $n$ (supposé très grand) sur un corps fini fixé soit irréductible.