16 Dénombrement des polynômes irréductibles sur un corps fini

La fonction de MÖBIUS $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ est définie par $\mu(n) = 0$ si n a un facteur carré, $\mu(n) = (-1)^s$ sinon, où s est le nombre de facteurs distincts dans la décomposition de n en irréductibles.

Lemme (Formule d'inversion de MÖBIUS)**.**
Soient f et g deux fonctions de $\mathbb{N}^*$ dans un groupe abélien G.
Si $\forall n\ f(n) = \sum_{d|n} g(d)$, alors $\forall n\ g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$.

Preuve.
Commençons par remarquer que μ est multiplicative au sens suivant : si n et m sont premiers entre eux, alors $\mu(nm) = \mu(n)\mu(m)$.

On introduit $S : \mathbb{N}^* \to G$, $n \mapsto \sum_{d|n} \mu(d)$. On a $S(1) = \mu(1) = 1$. Montrons que $S(n) = 0$ dès que $n > 1$. S est multiplicative au même titre que μ : si n et m sont premiers entre eux, alors $S(nm) = \sum_{d|nm} \mu(d) = \sum_{d|n, d'|m} \mu(dd')$ (car $d|nm \Leftrightarrow d = dd'$ avec $d|n$ et $d'|m$). De plus, deux nombres d et d' divisant respectivement n et m sont premiers entre eux (car n et m sont premiers entre eux), si bien que $S(nm) = \sum_{d|n, d'|m} \mu(d)\mu(d')$ soit encore $S(nm) = \left(\sum_{d|n} \mu(d)\right)\left(\sum_{d'|n} \mu(d')\right) = S(n)S(m)$. Il nous suffit donc de montrer que $S(p^\alpha) = 0$ dès que p est un nombre premier (et $\alpha \geqslant 1$). Il est clair que $S(p^\alpha) = \sum_{k=0}^{\alpha} \mu(p^k)$. Tous les termes de la somme sont nuls sauf le premier qui vaut 1 et le deuxième qui vaut -1. On a donc bien $S(p^\alpha) = 0$, par suite $S(n) = 0\ \forall n > 1$.

On peut maintenant montrer la formule d'inversion de MÖBIUS, partant du second membre B. Par une réindexation immédiate, on a $B = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$. En utilisant l'expression de f, il vient $B = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d')$. Or $\left(d|n \text{ et } d' \middle| \frac{n}{d}\right) \Leftrightarrow dd'|n \Leftrightarrow \left(d'|n \text{ et } d \middle| \frac{n}{d'}\right)$, on peut donc écrire $B = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d)$ soit $B = \sum_{d'|n} g(d') S\left(\frac{n}{d'}\right)$. Comme $S\left(\frac{n}{d'}\right) = 0$ sauf si $d' = n$ (et dans ce cas $S\left(\frac{n}{d'}\right) = 1$), on trouve finalement $B = g(n)$, ce qu'il fallait.

□

THÉORÈME. *Soit $\mathcal{I}_{nq}$ l'ensemble des polynômes unitaires irréductibles de degré n sur le corps fini $\mathbb{F}_q$; notons I_{nq} son cardinal. On a* $I_{nq} = \dfrac{1}{n}\sum_{d|n} \mu\left(\dfrac{n}{d}\right) q^d$.

Preuve.
On commence par montrer que $X^{q^n} - X = \prod_{P\in\mathcal{I}_{dq} \text{ où } d|n} P$. Pour clarifier les choses, toutes les extensions algébriques de $\mathbb{F}_q$ seront vues comme des sous-corps d'une clôture algébrique fixée une fois pour toutes. Remarquons déjà que la décomposition en irréductibles de $X^{q^n} - X$ sur $\mathbb{F}_q$ est sans facteurs carrés car $X^{q^n} - X$ est scindé à racines simples dans $\mathbb{F}_{q^n}$.

Soit P un facteur irréductible (unitaire) de $X^{q^n} - X$, montrons que son degré d divise n. Soit α une racine de P, alors α est racine de $X^{q^n} - X$ donc $\alpha \in \mathbb{F}_{q^n}$. Il s'ensuit que $\mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$, d'où $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. P étant irréductible sur $\mathbb{F}_q$, P est le polynôme minimal de α sur $\mathbb{F}_q$ de sorte que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. D'autre part, $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. On a donc montré que d est un diviseur de n.

Réciproquement, soit $P \in \mathcal{I}_{dq}$ avec $d|n$, et montrons que $P|X^{q^n} - X$. Soit α une racine de P, alors P est le polynôme minimal de α sur $\mathbb{F}_q$, si bien que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. On en déduit que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ car $d|n$. Ainsi toute racine de P est racine de $X^{q^n} - X$, il s'ensuit que $P|X^{q^n} - X$ car P est séparable ($\mathbb{F}_q$ est un corps parfait).

En comparant les degrés, il vient $q^n = \sum_{d|n} dI_{dq}$. La formule d'inversion de MÖBIUS donne alors $nI_{nq} = \sum_{d|n} \mu\left(\dfrac{n}{d}\right) q^d$, d'où le résultat.

□

Leçons possibles
112 Corps finis. Applications.
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
(**118** Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.)
(**120** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications)
145 Méthodes combinatoires, problèmes de dénombrement.

Références
mignotte algèbre concrète