7 Dénombrement des polynômes irréductibles sur $\mathbb{F}_p$

Leçons 123, 125, 141, 142, 144, 190

Ref : [Gozard] Lemme VII.26, Th VII.27, Déf VII.33

Le but de ce développement est de donner une idée du nombre de polynômes irréductibles unitaires sur les corps finis. On introduit pour cela la fonction de Möbius, dont on va donner quelques propriétés, avant de s'intéresser à la structure des polynômes sur les corps finis.

Il faut moduler ce développement en fonction de la leçon. Pour les leçons 141, 142 et 144, on peut admettre le théorème d'inversion et parler presque uniquement de polynômes, de racines et de pgcd. Pour la 190 au contraire, il faut absolument passer du temps sur Möbius. Pour les leçons sur les corps, on peut passer du temps sur les deux dernières étapes de la démonstration, et et choisir ce que l'on préfère entre le lemme d'arithmétique et les propriétés de Möbius qui sont décrites ci-dessous.

On se place dans la $\mathbb{C}$-algèbre [1] $\mathcal{S} = \mathbb{C}^{\mathbb{N}^*}$, où le produit interne est défini par

$$u * v(n) := \sum_{d|n} u\left(\frac{n}{d}\right) v(d) = \sum_{d|n} u(d) v\left(\frac{n}{d}\right).$$

C'est une algèbre commutative unitaire, dont le neutre est $\chi = \delta_1$.

Définition 1 On définit la fonction de Möbius μ par les axiomes suivants

(i) $\mu(1) = 1$,

(ii) si les p_i sont deux à deux distincts, $\mu(p_1 \cdots p_k) = (-1)^k$,

(iii) si n a un facteur carré, $\mu(n) = 0$.

Alors μ est l'inverse dans $\mathcal{S}$ de la fonction $\mathbb{1}$ constante égale à 1.

Démonstration. Comme le produit est commutatif, il suffit de montrer $\mu * \mathbb{1} = \chi$. Tout d'abord, l'axiome (i) justifie le calcul suivant :

$$\mu * \mathbb{1}(1) = \mu(1)\mathbb{1}(1) = 1 = \chi(1).$$

On doit maintenant montrer que si $n > 1$, $\mu * \mathbb{1}(n) = 0$. Soit $p \in \mathfrak{P}$ et $k \in \mathbb{N}^*$. On a grâce aux trois axiomes

$$\mu * \mathbb{1}(p^k) = \sum_{d|p^k} \mu(d) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) = 0.$$

Maintenant, si $n = \prod_{j=1}^{r} p_j^{k_j}$, on a

$$\mu * \mathbb{1}(n) = \sum_{i_1 \leq k_1, .., i_r \leq k_r} \mu(p_1^{i_1} \cdots p_r^{i_r}).$$

La somme ci-dessus possède en fait 2^r termes non nuls : ce sont les termes tels que $i_j \in \{0, 1\}$ pour tout j, et qui sont donc en bijection avec $\mathcal{P}(\llbracket 1, r \rrbracket)$. Finalement,

$$\mu * \mathbb{1}(n) = \sum_{A \in \mathcal{P}(\llbracket 1, r \rrbracket)} (-1)^{|A|} = \sum_{l=0}^{r} \binom{r}{l} (-1)^l = 0.$$

□

On en déduit immédiatement le théorème suivant.

Théorème 2 (Inversion de Möbius) Soient u et v dans $\mathcal{S}$, tels que

$$u(n) = \sum_{d|n} g(d).$$

Alors on a pour tout $n \in \mathbb{N}^*$

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

1. Si on n'a pas envie de recevoir trop de questions poussées sur la notion d'algèbre, on peut juste dire que c'est un espace vectoriel avec un produit sympatique.

On en vient aux polynômes irréductibles sur le corps $\mathbb{F}_p$. On note $\mathcal{I}_n(p)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p$, et $I_n(p) = |\mathcal{I}_n(p)|$.

Application 3 Pour $n \in \mathbb{N}^*$, on a

$$I_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

En particulier, $I_n(p) \sim \dfrac{p^n}{n}$.

Démonstration.

Étape 1. Un lemme dans les anneaux euclidiens.

On commence par montrer le lemme suivant.

Lemme 4 Soit A un anneau euclidien. On se donne $a \in A^\times$. Alors pour tout couple (m, n) d'entiers naturels non nuls, m divise n dans $\mathbb{Z}$ si et seulement si $a^m - 1$ divise $a^n - 1$ dans A.

On note $n = qm + r$ la division euclidienne de n par m. Alors on a

$$a^n - 1 = (a^{qm} - 1)a^r + a^r - 1 = (a^m - 1) \sum_{i=0}^{q-1} a^{im+r} + a^r - 1.$$

Ainsi, les diviseurs communs à $a^n - 1$ et $a^m - 1$ sont les diviseurs communs à $a^m - 1$ et $a^r - 1$. On applique alors l'algorithme d'Euclide pour calculer le pgcd de m et n. On construit alors une suite de restes $r_1, .., r_N, 0$, où r_N est donc le pgcd recherché. En itérant le raisonnement fait plus haut, on voit que $a^n - 1$ et $a^m - 1$ ont les mêmes diviseurs communs que $a^{r_N} - 1$ et $a^{r_{N+1}} - 1 = 0$. Donc le pgcd de $a^n - 1$ et $a^m - 1$ est $a^{\mathrm{pgcd}(m,n)} - 1$. Finalement, on a

$$\begin{array}{cc} & m|n \\ \iff & \mathrm{pgcd}(m, n) = m \\ \iff & a^{\mathrm{pgcd}(m,n)} - 1 = a^m - 1 \\ \iff & \mathrm{pgcd}\left(a^n - 1, a^m - 1\right) = a^m - 1 \\ \iff & a^m - 1 | a^n - 1 \end{array}$$

La seconde équivalence est vraie (son sens réciproque) car l'anneau est intègre et a non inversible.

Étape 2. Facteurs irréductibles de $X^{p^n} - X$.

On note $q = p^n$. On veut montrer le résultat suivant :

$$X^q - X = \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

On applique pour cela le lemme à $A = \mathbb{Z}$, pour déduire que d divise n si et seulement si $p^d - 1$ divise $p^n - 1$, puis en réappliquant le lemme dans $A = \mathbb{F}_p[X]$, en obtient que d divise n si et seulement si $X^{p^d-1} - 1$ divise $X^{q-1} - 1$ dans $\mathbb{F}_p[X]$.

Or, si $Q \in \mathcal{I}_d(p)$ est différent de X, comme $\mathbb{F}_{p^d} = \mathbb{F}_p[X]/(Q)$, en fixant l'image α du polynôme X dans $\mathbb{F}_{p^d}$, $\alpha^{p^d-1} = 1$ (par théorème de Lagrange) donc Q divise $X^{p^d-1} - 1$, et donc $X^{q-1} - X$. Finalement, tout polynôme qui se trouve dans l'un des $\mathcal{I}_d(p)$ divise $X^q - X$. Comme tous ces polynômes sont irréductibles, ils sont premiers entre eux, donc leur produit divise aussi $X^q - X$.

On note donc

$$X^q - X = P \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

On veut montrer que $P = 1$. On suppose par l'absurde que $P \neq 1$, c'est-à-dire (comme tous les polynômes considérés sont unitaires) que P est au moins de degré 1. Soit F un facteur irréductible de P, et d le degré de ce facteur. Alors $F \in \mathcal{I}_d(p)$, donc F divise $X^q - X$, et aussi $X^{p^d} - X$ (par le même raisonnement que précédemment). Donc il divise leur pgcd, que l'on note Δ. D'après le lemme, on a en notant $\delta = \mathrm{pgcd}(n, d)$

$$\Delta = X \,\mathrm{pgcd}(X^{q-1} - 1, X^{p^d-1} - 1) = X(X^{\mathrm{pgcd}(p^n-1, p^d-1)} - 1) = X^{p^\delta} - X.$$

Donc Δ est un polynôme de degré p^δ à coefficients dans $\mathbb{F}_p$, donc dans le corps de rupture $\mathbb{F}_p[X]/(F) = \mathbb{F}_{p^d}$, et il est nul dans ce corps (car divisible par F), donc il y a p^d racines. Ainsi, $p^d \leq p^\delta$, et donc $d = \delta$.

Ainsi, d divise n. Finalement, $F \in \mathcal{I}_d(p)$ donc F^2 divise $X^{p^n} - X$. Ceci est absurde, puisque $X^{p^n} - X$ est sans facteur carré. Donc $P = 1$. Finalement, on a montré

$$X^q - X = \prod_{d|n} \prod_{Q \in \mathcal{I}_d(p)} Q.$$

Étape 3. Conclusion par inversion.

On passe au degré dans l'égalité précédente. On en déduit

$$p^n = \sum_{d|n} dI_d(p).$$

Il suffit alors d'utiliser le théorème d'inversion de Möbius pour conclure : on obtient

$$nI_n(p) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

L'équivalent se déduit immédiatement. □