3. Les polynômes irréductibles de $\mathbb{F}_p[X]$

Soient $p \in \mathbb{P}$, $n \in \mathbb{N} \setminus \{0\}$ et $q = p^n$.

1. Factorisation de $X^q - X$ dans $\mathbb{F}_p[X]$
2. La fonction de Möbius
3. Le nombre $\mathrm{Irr}_p(n)$ de polynômes irréductibles de $\mathbb{F}_p[X]$ de degré n

1. Factorisation de $X^q - X$ dans $\mathbb{F}_p[X]$

Soient $p \in \mathbb{P}$, $n \in \mathbb{N} \setminus \{0\}$ et $q = p^n$.

Théorème (factorisation de $X^q - X$ dans $\mathbb{F}_p[X]$)

$X^q - X$ est le produit de tous les polynômes $P \in \mathbb{F}_p[X]$ irréductibles, de cœfficient dominant égal à 1 et tels que $\deg(P)|n$.

Démonstration :

• Soit $P \in \mathbb{F}_p[X]$ irréductible. Alors $K = \mathbb{F}_p[X]/(P)$ est un corps de cardinal $p^{\deg(P)}$. Désignons par $\pi : \mathbb{F}_p[X] \to K$ la projection canonique du quotient, et posons $\alpha = \pi(X) \in K$.

• Supposons que $\deg(P)|n$ et montrons que $P|X^q - X$ dans $\mathbb{F}_p[X]$.

Comme $[K : \mathbb{F}_p] = \deg(P)$, on a $\mathrm{Frob}_K^{\deg(P)} = \mathrm{Id}_K$, donc aussi $\mathrm{Frob}_K^n = \mathrm{Id}_K$ et en particulier $\alpha^q = \alpha$. Mais alors $\pi(X^q - X) = 0$ et donc $P|X^q - X$ dans $\mathbb{F}_p[X]$.

Factorisation de $X^q - X$ dans $\mathbb{F}_p[X]$ (2)

Suite de la démonstration :

• Réciproquement, supposons que $P|X^q - X$ dans $\mathbb{F}_p[X]$ et montrons que $\deg(P)|n$.

On a $\pi(X^q - X) = 0$, donc $\alpha^q = \alpha$. Ainsi $\mathrm{Frob}_K^n(\alpha) = \alpha$. Par suite $\{x \in K : \ \mathrm{Frob}_K^n(x) = x\}$ est un sous-anneau de K qui contient α, donc il coïncide avec $K = \mathbb{F}_p[\alpha]$. On a donc $\mathrm{Frob}_K^n = \mathrm{Id}_K$. Comme Frob_K est d'ordre $\deg(P)$, il vient $\deg(P)|n$.

• Par ailleurs, $X^q - X$ n'a pas de facteur multiple dans $\mathbb{F}_p[X]$ puisque son polynôme dérivé est $qX^{q-1} - 1 = -1$.

• Enfin, comme $X^q - X$ est de cœfficient dominant égal à 1, il est égal au produit de ses facteurs irréductibles lorsque ceux-ci sont choisis avec leur cœfficient dominant égal à 1.

□

Conséquence pour le dénombrement des irréductibles

Soient $p \in \mathbb{P}$, $n \in \mathbb{N} \setminus \{0\}$ et $q = p^n$.
Pour tout $k \in \mathbb{N}$, désignons par $\mathrm{Irr}_p(k)$ le nombre de polynômes irréductibles de $\mathbb{F}_p[X]$ de degré k :

$$\mathrm{Irr}_p(k) \overset{\text{déf}}{=} \mathrm{card}\,\{P \in \mathbb{F}_p[X] : \quad \deg(P) = k, \text{ irréductible et de cœfficient dominant } = 1\}$$

Corollaire

$$p^n = \sum_{d|n} d \; Irr_p(d)$$

Démonstration : c'est l'égalité des degrés de $X^q - X$ et de sa factorisation donnée par le théorème précédent.

□

2. La fonction de Möbius

Définition (fonction de Möbius)

La fonction de Möbius est définie sur $\mathbb{N} \setminus \{0\}$ par :

$$\begin{array}{rrcl} & \mu(1) & = & 1 \\ (\forall n > 1) & \mu(n) & = & \left| \begin{array}{ll} 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers} \\ & \quad \text{deux à deux distincts} \end{array} \right. \end{array}$$

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad \mu(n) \in \{-1; 0; 1\}$$

Proposition (μ est multiplicative)

$$(\forall n, n' \in \mathbb{N} \setminus \{0\}) \qquad pgcd(n, n') = 1 \implies \mu(nn') = \mu(n)\mu(n')$$

Démonstration : exercice.

□

La fonction de Möbius (2)

Proposition (une formule d'Euler pour μ ?)

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad \sum_{d|n} \mu(d) = \left| \begin{array}{lll} 1 & si & n = 1 \\ 0 & si & n > 1 \end{array} \right.$$

Démonstration : Si $n = 1$, la somme se réduit à $\mu(1) = 1$.
Si $n > 1$, on factorise n en facteurs premiers distincts :

$$n = \prod_{j=1}^{m} p_j^{r_j}$$

Il y a exactement $\binom{m}{k}$ diviseurs de n qui sont produit de k nombres premiers 2 à 2 distincts, ainsi

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{m} \binom{m}{k} (-1)^k = (1-1)^m = 0$$

□

La fonction de Möbius (3)

Proposition (formule d'inversion de Möbius)

Soit une application $f : \mathbb{N} \setminus \{0\} \to \mathbb{C}$. *Alors, si pour tout* $n \in \mathbb{N} \setminus \{0\}$ *on a posé* $F(n) = \sum_{d|n} f(d)$, *on a :*

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$$

Démonstration :

$$f(n) = \sum_{d'|n} f(d') \overbrace{\left(\sum_{d|\frac{n}{d'}} \mu(d) \right)}^{=1 \text{ si } d'=n,\ 0 \text{ sinon}} = \sum_{d'|n} \sum_{d|\frac{n}{d'}} f(d')\mu(d) = \sum_{d|n} \underbrace{\sum_{d'|\frac{n}{d}} f(d')\, \mu(d)}_{=F(\frac{n}{d})}$$

□

3. Le nombre $\mathrm{Irr}_p(n)$ de polynômes irréductibles de $\mathbb{F}_p[X]$ de degré n

Corollaire

1. $(\forall n \in \mathbb{N} \setminus \{0\}) \qquad Irr_p(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$
2. $(\forall n \in \mathbb{N} \setminus \{0\}) \qquad Irr_p(n) \geq \frac{1}{n} \ > 0$
3. $Irr_p(n) \sim_{n \to \infty} \frac{p^n}{n}$

Démonstration :

1. La formule d'inversion de Möbius donne directement $n \ \mathrm{Irr}_p(n) = \sum_{d|n} \mu(\frac{n}{d}) p^d$.
2. exercice.
3. exercice.

□