

Soit $P \in \mathbf{F}_q[X]$ non constant. L'objectif est de calculer la décomposition de P en produit de polynômes irréductibles. On note $V := \mathbf{F}_q[X]/(P)$ et $W := \{f \in V \mid f^q = f\}$.

1- W est un $\mathbf{F}_q$ -sev de V .

Considérons l'application

$$\Phi: \begin{cases} V \longrightarrow V \\ f \longmapsto f^q - f. \end{cases}$$

Pour tous $f, g \in V$, $\Phi(f + g) = (f + g)^q - (f + g) = f^q + g^q - f - g = (f^q - f) + (g^q - g) = \Phi(f) + \Phi(g)$. De plus si $\alpha \in \mathbf{F}_q$ alors $\Phi(\alpha f) = (\alpha f)^q - (\alpha f) = \alpha^q f^q - \alpha f = \alpha(f^q - f) = \alpha\Phi(f)$ d'après le théorème de Lagrange ($\alpha^q = \alpha$). Ainsi Φ est $\mathbf{F}_q$ -linéaire, et $W = \text{Ker } \Phi$.

2- Un critère d'irréductibilité.

On se ramène facilement au cas où P est sans facteur carré. Soit alors $P = P_1 \cdots P_r$ la décomposition de P en polynômes irréductibles sur $\mathbf{F}_q$ deux à deux non associés. Les quotients $V_i := \mathbf{F}_q[X]/(P_i)$ de l'anneau principal $\mathbf{F}_q[X]$ par les idéaux maximaux (P_i) , $1 \leq i \leq r$, sont des corps de rupture, donc des extensions finies de $\mathbf{F}_q$. D'après le théorème chinois l'application

$$\Psi: \begin{cases} V \longrightarrow V_1 \times \cdots \times V_r \\ Q \bmod P \longmapsto (Q \bmod P_1, \dots, Q \bmod P_r), \end{cases}$$

définit un isomorphisme d'anneaux, donc de $\mathbf{F}_q$ -ev, et $W = \text{Ker } \Phi$ est alors isomorphe au produit $\Psi(W) = \text{Ker } \Psi \circ \Phi \circ \Psi^{-1} = \prod_{i=1}^r \{f \in V_i \mid f^q = f\} = \mathbf{F}_q^r$. D'où P est irréductible si et seulement si $\dim_{\mathbf{F}_q} W = r$ vaut 1, ce que l'on peut déterminer effectivement en calculant le rang de Φ .

3- L'algorithme.

Si $r = \dim_{\mathbf{F}_q} W > 1$ alors il existe (et on peut calculer) $Q \in \mathbf{F}_q[X]$ tel que $Q \bmod P$ est dans $W \setminus \mathbf{F}_q 1$. Alors $(\alpha_1, \dots, \alpha_r) := \Psi(Q \bmod P) \in \mathbf{F}_q^r$ et les α_i ne sont pas tous égaux : il existe $1 \leq k < \ell \leq r$ tels que $\alpha_k \neq \alpha_\ell$.

Soit $\alpha \in \mathbf{F}_q$. $\gcd(P, Q - \alpha)$ divise P donc il existe $I_\alpha \subseteq \{1, \dots, r\}$ tel que $\gcd(P, Q - \alpha) = \prod_{i \in I_\alpha} P_i$. Or $i \in I_\alpha \iff P_i \mid (Q - \alpha) \iff Q = \alpha \bmod P_i \iff \alpha_i = \alpha$. Ainsi

$$\forall \alpha \in \mathbf{F}_q, \quad \gcd(P, Q - \alpha) = \prod_{\substack{1 \leq i \leq r \\ \alpha_i = \alpha}} P_i, \quad (1)$$

$$\text{et} \quad \prod_{\alpha \in \mathbf{F}_q} \gcd(P, Q - \alpha) = \prod_{\alpha \in \mathbf{F}_q} \prod_{\substack{1 \leq i \leq r \\ \alpha_i = \alpha}} P_i = \prod_{1 \leq i \leq r} \prod_{\substack{\alpha \in \mathbf{F}_q \\ \alpha_i = \alpha}} P_i = \prod_{i=1}^r P_i = P. \quad (2)$$

Comme $\alpha_k \neq \alpha_\ell$ les polynômes $\gcd(P, Q - \alpha_k)$ et $\gcd(P, Q - \alpha_\ell)$ sont deux facteurs non triviaux de P d'après (1). On applique alors récursivement l'algorithme à chacun des facteurs non triviaux apparaissant dans la décomposition (2) de P pour aboutir à la factorisation recherchée. ■

Références. [BMP, p. 244]

123 Corps finis. Applications.

141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

[BMP] Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ : *Objectif Agrégation*. 2^{ème} édition.