

La méthode de Berlekamp

On se place sur $\mathbb{F}_q$, le corps fini à q éléments, où q est une puissance entière d'un nombre premier p . On considère un polynôme $P \in \mathbb{F}_q[X]$ séparable (ie P et P' sont premiers entre eux) dont la décomposition en facteurs irréductibles est :

$$P = P_1 \dots P_r$$

On note

$$\alpha : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X] \quad P \mapsto P^q \quad \text{et} \quad A = \mathbb{F}_q[X]/(P), \quad A_i = \mathbb{F}_q[X]/(P_i).$$

Par le théorème des restes chinois, on a un isomorphisme de $\mathbb{F}_q$ -algèbre, noté ϕ qui donne l'identification

$$A \simeq A_1 \times \dots \times A_r.$$

Soit $Q \in \mathbb{F}_q[X]$, considérons l'application $\mathbb{F}_q$ -linéaire $\mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(Q) \quad R \mapsto \overline{\alpha(R)}$. Comme on a

$$\alpha(Q)(X) = Q(X^q) = (Q(X))^q \equiv 0 \pmod{Q},$$

on en déduit que cette application passe au quotient, on définit ainsi un endomorphisme de $\mathbb{F}_q[X]/(Q)$, encore notée α , de $\mathbb{F}_q[X]/(Q)$. Par ce procédé, on peut définir α sur A et A_i et donc sur $A_1 \times \dots \times A_r$. On remarque que α commute avec ϕ , c'est à dire que $\alpha(\phi(x)) = \phi(\alpha(x)) \quad \forall x \in A$. On note $A^\alpha = \{x \in A \mid \alpha(x) = x\}$ les invariants de A sous α . On a

$$A^\alpha \simeq A_1^\alpha \times \dots \times A_r^\alpha,$$

Or A_i est un corps (car $\mathbb{F}_q[X]$ est principal et P_i irréductible) de degré $\deg(P_i)$ sur $\mathbb{F}_q$. En particulier, les invariants de A_i sous α est $\mathbb{F}_q$ (le sous-corps de base de A_i). On en déduit donc que

$$A^\alpha \simeq \mathbb{F}_q^r$$

Ainsi, $\dim_{\mathbb{F}_q} A^\alpha = r$ et on vient de caractériser le nombre de facteurs irréductibles de P en terme de dimension d'un $\mathbb{F}_q$ -espace vectoriel. On va donner une autre description de A^α qui est plus exploitable : c'est l'ensemble des $x \in A$ tels que $\alpha(x) = x$, c'est à dire le sous-espace propre de α associé à la valeur propre 1, ainsi, on a prouvé que le nombre de facteur irréductible de P est

$$r = \dim_{\mathbb{F}_q} (\text{Ker}(\alpha - Id)).$$

Cette méthode permet aussi de trouver les facteurs irréductibles. Soit $Q \in A^\alpha$, alors on a l'égalité dans A :

$$0 = \alpha(Q) - Q = Q^q - Q = \prod_{a \in \mathbb{F}_q} (Q - a).$$

On rappelle que dans un anneau factoriel, si b et c sont premiers entre eux, alors $\text{pgcd}(a, bc) = \text{pgcd}(a, b) \text{pgcd}(a, c)$. Or ici les facteurs $Q - a$ sont premiers entre eux, donc on a

$$P = \text{pgcd}(P, Q^q - Q) = \prod_{a \in \mathbb{F}_q} \text{pgcd}(P, Q - a).$$

Lorsque $\text{pgcd}(P, Q - a)$ est non trivial on obtient une factorisation. Cette étude suggère la méthode suivante :

Soit P un polynôme séparable.

– On calcule la matrice de α dans la base $1, x, \dots, x^{d-1}$, où d est le degré de P et x est l'image de X dans le quotient A . Il suffit pour cela de réduire modulo P les monomes x^{qi} , par exemple par division euclidienne dans $\mathbb{F}_q[X]$.

– On calcule le rang de $\alpha - id$ et on en déduit la dimension du noyau, donc le nombre de facteur irréductible.

– On détermine le sous-espace propre associé à 1, on choisit des éléments Q de ce sous-espace et on teste $\text{pgcd}(f, Q - a)$ pour $a \in \mathbb{F}_q$. On s'arrête lorsque l'on trouve le bon nombre de facteurs propres

premier entre eux, qui sont alors necessairement irréductibles.

Exemples :

1. Essayons cette méthode avec le polynôme $P = X^5 + X^4 + 1$ sur $\mathbb{F}_2$. Soit x l'image de X dans la projection canonique de $\mathbb{F}_2[X]$ sur $\mathbb{F}_2[X]/(P)$. On a

$$\begin{aligned}\alpha(1) &= 1 \mod P \\ \alpha(x) &= x^2 \mod P \\ \alpha(x^2) &= x^4 \mod P \\ \alpha(x^3) &= x^4 + x + 1 \mod P \\ \alpha(x^4) &= x^4 + x^3 + x^2 + x + 1 \mod P\end{aligned}$$

L'application $\alpha : Q \mapsto Q^2$ a pour matrice dans la base $(1, x, x^2, x^3, x^4)$ de $\mathbb{F}_2[X]/(P)$:

$$M_\alpha = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \text{donc } M_\alpha - I = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

On voit tout de suite que le rang de $M_\alpha - I$ est trois, donc P possède exactement deux polynômes irréductibles. On voit que le vecteur $x^2 + x^3 + x^4$ est dans le noyau de $M_\alpha - I$ donc

$$\text{Ker}(M_\alpha - I) = \langle 1, x^2 + x^3 + x^4 \rangle.$$

On trouve

$$\text{pgcd}(P, X^2 + X^3 + X^4) = X^2 + X + 1 \quad \text{et} \quad \text{pgcd}(P, 1 + X^2 + X^3 + X^4) = X^3 + X + 1,$$

d'où le résultat.

2. Factorisons $P = X^6 + 7$ sur $\mathbb{F}_{11}$. On note encore x l'image de X et α l'application qui consiste à élever à la puissance 11. On a

$$\begin{aligned}\alpha(1) &= 1 \mod P \\ \alpha(x) &= 4x^5 \mod P \\ \alpha(x^2) &= -2x^4 \mod P \\ \alpha(x^3) &= x^3 \mod P \\ \alpha(x^4) &= 5x^2 \mod P \\ \alpha(x^5) &= 3x \mod P\end{aligned}$$

d'où

$$M_\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{donc } M_\alpha - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 3 \\ 0 & 0 & -1 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & -1 & 0 \\ 0 & 4 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Le rang de $M_\alpha - I$ est 2 donc il y a quatre facteurs irréductibles et le noyau de $M_\alpha - I$ est $\langle 1, x^3, 3x + x^5, 5x^2 + x^4 \rangle$. On a :

$$\text{pgcd}(X^6 + 7, 3X + X^5 + 1) = X^2 + 4X + 5, \quad \text{pgcd}(X^6 + 7, 3X + X^5 + 2) = X + 4,$$

$$\text{pgcd}(X^6 + 7, 3X + X^5 + 9) = X + 7, \quad \text{pgcd}(X^6 + 7, 3X + X^5 + 10) = X^2 + 7X + 5.$$