* Algorithme de Berlekamp: leçons 123; 125; 141; 142; 148 (122)

[Beck Malick Peyré] I.8.2

[Demazure] Cours d'algèbre IX.6

Soit $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ avec $P_1, \dots, P_r$ irréductibles 2 à 2 premiers entre eux.

On note $S_p : \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P)$, c'est une application linéaire.

$$\bar{Q} \longmapsto \bar{Q}^q = \overline{Q(X^q)}$$

Alors:

$$r = \dim \ker(S_p - id) = \deg P - \operatorname{rg}(S_p - id)$$

Si de plus $r \geq 2$ et $\bar{V} \in \ker(S_p - id) \setminus \mathbb{F}_q$, alors:

$$P = \prod_{\alpha \in \mathbb{F}_q} P_1(V - \alpha)$$ est une décomposition non triviale de P

Déc. Alg 5

Lemme :

Soit $P \in \mathbb{F}_q[X]$.

Alors :

1) $P \wedge P' = 1 \iff P$ sans facteur carré

2) $P \wedge P' = P \iff P' = 0 \iff \exists R \in \mathbb{F}_q[X],\ P = R^p$ (les coeffs de R sont les racines p-ième de ceux de P)

3) Si on est dans aucun des deux cas précédents, $P = P \wedge P' \cdot \frac{P}{P \wedge P'}$ est une décomposition non triviale de P.

Algorithme dans le cas général :

Soit $P \in \mathbb{F}_q[X]$:

Si P est constant :

Fin de l'algo.

Sinon :

On calcule $P \wedge P'$

Si $P \wedge P' = 1$:

On applique Berlekamp à P

Si $P \wedge P' = P$:

On trouve $R \in \mathbb{F}_q[X]$ tq $P = R^p$

On applique l'algo. à R

Sinon :

On applique l'algo. à $P \wedge P'$ et $\frac{P}{P \wedge P'}$

Preuve :

• Si est linéaire et on a bien $\bar{Q}^q = \overline{Q(X^q)}$.

$A := \mathbb{F}_q[X]/(P)$ est un anneau de caractéristique p donc $\begin{array}{ccc} A & \longrightarrow & A \\ \bar{Q} & \longmapsto & \bar{Q}^p \end{array}$ est une application linéaire.

Sa est simplement la composée n fois de cette application.

Notons $\alpha := \bar{X} \in A$. $(1, \alpha, \dots, \alpha^{d-1})$ est alors une base de la $\mathbb{F}_q$-algèbre A, où $d = \deg P$.

De plus : $\forall \bar{Q} = \sum_{k=0}^{d-1} a_k \alpha^k \in A$, $\bar{Q}^q = \sum_{k=0}^{d-1} a_k^q \alpha^{qk} = \sum_{k=0}^{d-1} a_k \alpha^{qk} = \overline{Q(X^q)}$ car $\forall a \in \mathbb{F}_q$, $a^q = a$.

preuve de Berlekamp:

Pour $i \in [\![1;r]\!]$, notons $K_i := \mathbb{F}_q[X]/(P_i)$. C'est un corps car P_i irréductible.

De plus, le théorème chinois nous donne un isomorphisme de $\mathbb{F}_q$-algèbres

$$\varphi : A \longrightarrow K_1 \times \dots \times K_r \qquad \text{où } \bar{Q} \text{ est la classe de } Q \text{ modulo } P.$$
$$\bar{Q} \longmapsto (\bar{Q}, \dots, \bar{Q})$$

Soit $\bar{Q} \in A$, on a:

$$\bar{Q} \in \ker(S_p - id) \iff \bar{Q}^q = \bar{Q}$$
$$\iff \varphi(\bar{Q})^q = \varphi(\bar{Q})$$
$$\iff \forall i \in [\![1;r]\!] : (\bar{Q}^i)^q = \bar{Q}^i$$

Or, pour $i \in [\![1;r]\!]$, K_i est une extension (finie) de $\mathbb{F}_q$ et le théorème de Lagrange nous indique:

$\mathbb{F}_q \subseteq Z_{K_i}(X^q - X)$ $X^q - X$ est de degré q donc a au plus q racines dans K_i et donc, comme $|\mathbb{F}_q| = q$, on a l'égalité: $\mathbb{F}_q = Z_{K_i}(X^q - X)$. i.e.: $\forall \alpha \in K_i : \alpha^q = \alpha \iff \alpha \in \mathbb{F}_q$.

Ainsi:

$$\bar{Q} \in \ker(S_p - id) \iff \forall i \in [\![1;r]\!] : \bar{Q}^i \in \mathbb{F}_q$$
$$\iff \bar{Q} \in \varphi^{-1}(\mathbb{F}_q^r)$$

Donc

$$\dim(\ker(S_p - id)) = \dim(\varphi^{-1}(\mathbb{F}_q^r)) = \dim(\mathbb{F}_q^r) = r$$

- Supposons maintenant $r \geq 2$:

$\mathbb{F}_q$ est une droite vectorielle incluse dans $\ker(S_p - id)$ donc $\exists \bar{V} \in \ker(S_p - id) \setminus \mathbb{F}_q$

Par ce qu'on a dit avant: $\varphi(\bar{V}) = (\alpha_1, \dots, \alpha_r)$ avec $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q$.

Or, $\varphi(\mathbb{F}_q) = \{(\alpha, \dots, \alpha),\ \alpha \in \mathbb{F}_q\}$ donc $\exists i_0, j_0$ tq $\alpha_{i_0} \neq \alpha_{j_0}$. (*)

Soit $\alpha \in \mathbb{F}_q$:

Fr: $P_i \mid V - \alpha \iff \bar{V}^i = \alpha \iff \alpha_i = \alpha$

Donc: $$P_\alpha(V - \alpha) = \prod_{\substack{i \in [\![1;r]\!] \\ \alpha_i = \alpha}} P_i$$

Donc: $$P = \prod_{\alpha \in \mathbb{F}_q} P_\alpha(V - \alpha)$$

Or, par (*): $P_{i_0} \mid P_\alpha(V - \alpha_{i_0})$ et $P_{j_0} \mid P_\alpha(V - \alpha_{j_0})$ et ces deux éléments sont distincts dans la décomp

$\rightsquigarrow$ la décomp est non triviale.

• preuve du lemme :

- Soit P_i un facteur premier de P.

On écrit $P = P_i^{m_i} Q$ avec $Q \wedge P_i = 1$.

$P' = m_i P_i^{m_i - 1} Q + P_i^{m_i} Q'$

$= P_i^{m_i - 1} (m_i Q + P_i Q')$

On a donc $P_i^{m_i - 1} \mid P \wedge P'$ et $P_i^{m_i} \mid P \wedge P' \Leftrightarrow P_i \mid m_i Q + P_i Q' \Leftrightarrow P_i \mid m_i Q$ ($\wedge Q = 1$) $\Leftrightarrow P_i \mid m_i \Leftrightarrow m_i = 0 \Leftrightarrow p \mid m_i$

Ainsi : $P \wedge P' = 1 \Leftrightarrow \forall i \in [\![1; r]\!] : m_i = 1$.

- Par ailleurs : $P \wedge P' = P \Leftrightarrow P \mid P' \Leftrightarrow P' = 0$ car $\deg P' < \deg P$ ($\wedge P \neq 0$)

Si $P = R^p$, alors $P' = p(R')^{p-1} = 0$

Réciproquement, si $P' = 0$: On note $P = \sum_{k=0}^{d} a_k X^k$.

On a : $P' = \sum_{k=1}^{d} k a_k X^{k-1}$ donc $\forall k \in [\![1; d]\!] : k a_k = 0$.

donc : $\forall k \in [\![1; d]\!], p \nmid k \cdot a_k = 0$.

$\rightsquigarrow P = \sum_{k=0}^{d'} a_{pk} X^{pk}$ où $d' = \left\lfloor \frac{d}{p} \right\rfloor$

Le morphisme de Frobenius est surjectif donc $\forall k, \exists b_k, a_{pk} = b_k^p$ ($b_k = a_{pk}^{p^{n-1}}$ par ex.)

$\rightsquigarrow P = \sum_{k=0}^{d'} b_k^p X^{pk} = \underbrace{\left(\sum_{k=0}^{d'} b_k X^k \right)}_{=R}^p$

CQFD.