Obj Agreg p. 244

Algorithme de Berlekamp

122, (141), 142

<u>Théorème</u> : Soit $P \in \mathbb{F}_q[X]$ dont la décomposition en polynômes irréductibles et sans facteur carré. Posons $x = \overline{X}$ dans $\mathbb{F}_q[X]/(P)$. Considérons $\mathcal{B} = \{1, x, \dots, x^{\deg P - 1}\}$ base de $\mathbb{F}_q[X]/(P)$.
L'algorithme suivant termine en un nombre fini d'étapes :

* Calculer la matrice de $S_P - id$ où $S_P : \begin{array}{rcl} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ \overline{Q} & \longmapsto & \overline{Q}(X^q) \end{array}$
* Le nombre de facteurs irréductibles de P est $r = \dim(\ker(S_P - id))$.
$= \deg P - rg(S_P - id)$.

Si $r = 1$, P est irréductible. Sinon :

* On calcule V non constant dans $\mathbb{F}_q[X]/(P)$ tq $\overline{V} \in \ker(S_P - id)$.

Alors $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha)$. On redémarre avec chaque terme.

<u>Lemme</u> : Soit $p \in \mathbb{P}$. Soit $q = p^s$, $s \in \mathbb{N}$. L'application S_P est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$.

Par propriété universelle, il existe un unique morphisme d'anneaux
$\delta : \begin{array}{rcl} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X] \\ Q & \longmapsto & Q(X^q) \end{array}$ i.e. $\begin{cases} \delta(a) = a \text{ si } a \in \mathbb{F}_q \\ \delta(X) = X^q \end{cases}$
[$\forall a \in \mathbb{F}_q$, $a^q = a$ donc l'élévation à la puissance q est un morphisme]
et $\delta(Q) = Q(X^q) = \sum \alpha_k (X^q)^k = \sum (\alpha_k X^k)^q = (\sum \alpha_k X^k)^q = Q^q$.
Notons $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(P)$ la projection canonique, $\overline{\delta} = \pi \circ \delta$.
π est un morphisme donc $\overline{\delta}(P) = \pi(P^q) = \pi(P)^q = 0$.
Donc $\overline{\delta}$ passe au quotient, ce qui donne S_P.
Enfin, $S_P(\overline{Q}) = S_P(\pi(Q)) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q = \overline{Q}^q$.
Donc S_P coïncide avec l'élévation à la puissance q.

Notons $P = P_1 \dots P_r$ avec les P_i irréd. 2 à 2 p.e.e. par hypothèse et $K_i = \mathbb{F}_q[X]/(P_i)$ corps. Le théorème chinois donne l'isomorphisme
$\varphi : \begin{array}{rcl} \mathbb{F}_q[X]/(P) & \longrightarrow & K_1 \times \dots \times K_r \\ Q & \longmapsto & (Q \bmod P_1, \dots, Q \bmod P_r) \end{array}$
Soit $\tilde{S}_P = \varphi \circ S_P \circ \varphi^{-1}$, élévation à la puissance q dans $K_1 \times \dots \times K_r$.
$(x_1, \dots, x_r) \in \ker(\tilde{S}_P - id) \Leftrightarrow \forall i \in \{1, \dots, r\}, x_i^q = x_i$ dans K_i.
Soit K une extension de corps de $\mathbb{F}_q$. L'image de $\mathbb{F}_q$ dans K est l'ensemble des éléments vérifiant $x^q = x$ (car ceux de $\mathbb{F}_q$ le vérifient et il y en a au plus q).

Or K_i est une extension de $\mathbb{F}_q$, donc $(x_1, \dots, x_r) \in \ker(\tilde{S}_P - id) \Leftrightarrow \forall i \in \{1, \dots, r\}, x_i \in \mathbb{F}_q$.

Ainsi, $\ker(\tilde{S}_P - id) = \mathbb{F}_q^r$. Or $\ker(\tilde{S}_P - id) = \varphi(\ker(S_P - id))$

Donc, puisque un isomorphisme de $\mathbb{F}_q$-ev, $\dim(\ker(S_P - id)) = r$.

Supposons $r > 1$.

$\dim \ker(S_P - id) > 1$ donc, puisque l'ensemble des $U \in \mathbb{F}_q[X]/(P)$ constants est engendré par $1 \pmod P$, il existe $V \in \mathbb{F}_q[X]$ tq $\begin{cases} \overline{V} \text{ non constant dans } \mathbb{F}_q[X]/(P) \\ \overline{V} \in \ker(S_P - id). \end{cases}$

i.e. $(V \bmod P_1, \dots, V \bmod P_r) \in \mathbb{F}_q^r$; que l'on note $(\alpha_1, \dots, \alpha_r)$.

- Soit $\alpha \in \mathbb{F}_q$. $\mathrm{pgcd}(P, V-\alpha) \mid P$ donc s'écrit $\prod_{i \in I_\alpha} P_i$.

Les P_i étant p.e.e., le lemme de Gauss assure $I_\alpha = \{i \in \{1, \dots, r\}, P_i \mid V - \alpha\}$

Or $P_i \mid V - \alpha \Leftrightarrow V - \alpha \equiv 0 \bmod P_i \Leftrightarrow \alpha = \alpha_i$.

Donc, $\mathrm{pgcd}(P, V-\alpha) = \prod_{i, \alpha_i = \alpha} P_i$.

Ainsi, $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{i, \alpha_i = \alpha} P_i = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha)$. $(*)$

on partitionne $\{1, \dots, r\}$ en les I_α.

De plus, puisque $\overline{V}$ non constant, $\exists i, j$, $\alpha_i \neq \alpha_j$ (sinon on aurait $P \mid V - \alpha$ donc $\overline{V} = \alpha$) donc il y a au moins deux facteurs non triviaux dans $(*)$ ce qui fait diminuer r strictement.

Lemme des noyaux d caq