Développement : Algorithme de Berlekamp.

RM

2022-2023

Référence :

1. Oral à l'agreg

Énoncé :

Théorème 1 : Soient $q = p^n$ avec p premier, $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ sans facteur carré. On pose $P = \prod_{i=1}^{r} P_i$ la décomposition de P en produit d'irréductible sur $\mathbb{F}_q[X]$. Si $r = 1$, alors P est irréductible. Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tels que $pgcd(P, V - a)$ soit un facteur non trivial de P.

On pose quelques propriétés avant :

Lemme 2 : Soit p un nombre premier. Alors p divise $\binom{p}{k}$ si $1 \leq k \leq p-1$. On en déduit que $(a+b)^p \equiv a^p + b^p [p]$.

Démonstration : On a

$$k\binom{p}{k} = k\frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{(k-1)!(p-1-(k-1))!} = p\binom{p-1}{k-1}$$

Comme p est premier, $p|k$ ou $p|\binom{p}{k}$. Or $k \leq p-1$, donc on en déduit que $p|\binom{p}{k}$. □

Proposition 3 : L'application $S : \mathbb{F}_q[X] \mapsto \mathbb{F}_q[X]$ définie par $S(Q) = Q^p$ est un $\mathbb{F}_q[X]$-endomorphisme de l'espace vectoriel $\mathbb{F}_q[X]$.

Démonstration : Pour tout $\lambda \in \mathbb{F}_q$, on a $\lambda^q = \lambda$ (Lagrange) et donc, pour tout $R \in \mathbb{F}_q[X]$, on a $S(\lambda R) = (\lambda R)^q = \lambda R^q = \lambda S(R)$. Soient $Q, R \in \mathbb{F}_q[X]$. Comme $\mathbb{F}_q$ est de caractéristique p, on a $(Q+R)^p = Q^p + R^p$. Ainsi, on montre par récurrence sur $k \in \mathbb{N}$ que $(Q+R)^{p^k} = Q^{p^k} + R^{p^k}$, et donc en particulier

$$S(Q+R) = (Q+R)^{p^n} = Q^{p^n} + R^{p^n} = S(Q) + S(R)$$

ce qui achève la preuve que S est $\mathbb{F}_q$-linéaire. □

Proposition 4 : Soit L une extension de $\mathbb{F}_q$. Alors $x \in L$ vérifie $x^q = x$ si et seulement si $x \in \mathbb{F}_q$.

Démonstration : D'après le théorème de Lagrange, pour tout $x \in \mathbb{F}_q^*$, on a $x^{q-1} = 1$, d'où $x^q = x$ pour tout élément $x \in \mathbb{F}_q$. On a donc exhibé q racines distinctes du polynômes $P = X^q - X$ sur L. Or, comme L est un corps et que P est de degré q,P possède au plus q racines, donc ce sont les seules. □

Théorème 5 : Soient $P_1, ..., P_r \in \mathbb{F}_q[X]$ des polynômes premiers entre eux, et soit $P = \prod_{i=1}^{r} P_i$. Alors, l'application suivante est un isomorphisme de $\mathbb{F}_q$-algèbres :

$$\begin{array}{rccc} f: & \mathbb{F}_q[x]/(P) & \to & \mathbb{F}_q[X]/(P_1) \times ... \times \mathbb{F}_q[X]/(P_r) \ . \\ & x[P] & \mapsto & x[P_1], ..., x[P_r] \end{array}$$

Résolution :

Démonstration : On considère l'application

$$\begin{array}{rccc} T: & \mathbb{F}_q[X] & \to & \mathbb{F}_q[X]/(P) \\ & Q & \mapsto & Q^p[P] \end{array}$$

Comme $S : Q \mapsto Q^p$ et la projection canonique sont toutes les deux $\mathbb{F}_q$-linéaires, alors T est $\mathbb{F}_q$-linéaire par composition. Pour tout polynôme $Q \in \mathbb{F}_q[X]$, on a l'égalité suivante : $T(QP) = (QP)^q \equiv 0[P]$ et donc $(P) \subseteq Ker(T)$. On peut alors factoriser T pour obtenir un $\mathbb{F}_q$-endomorphisme φ de $\mathbb{F}_q[X]/(P)$ défini par $\varphi(\overline{Q}) = \overline{Q}^p$.
Les P_i sont premiers entre eux : d'après le Théorème 5, il existe un isomorphisme de $\mathbb{F}_q$-algèbres

$$\psi : \mathbb{F}_q[X]/(P) \to K_1 \times ... \times K_r.$$

où $K_i = \mathbb{F}_q[X]/(P_i)$ est un corps car P_i est irréductible. On pose alors l'application linéaire $\tilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$, qui vérifie $\tilde{\varphi}(Q) = (Q_1^q, ..., Q_r^q)$ pour tout $Q = (Q_1, ..., Q_r) \in K_1 \times ... \times K_r$ car l'application ψ préserve la multiplication.
Ainsi, on a $Q \in Ker(\tilde{\varphi} - Id)$ si et seulement si $Q_i^q = Q_i$ pour tout $i \in [\![1\,;r]\!]$. Or, pour tout $i \in [\![1\,;r]\!]$,K_i est une extension de $\mathbb{F}_q$, donc on a, d'après la Proposition 4, $Q_i^q = Q_i$ si et seulement si $Q_i \in \mathbb{F}_q$. On a donc $Q \in Ker(\tilde{\varphi} - Id)$ si et seulement Q est un r-uplet d'éléments de $\mathbb{F}_q$, donc $|Ker(\tilde{\varphi} - Id)| = q^r$ et donc on a $dim(Ker(\varphi - Id)) = dim(Ker(\tilde{\varphi} - Id)) = r$ car ψ est un isomorphisme.
Supposons que r soit supérieur ou égale à 2. Les polynômes constants modulo P forment un sous espace vectoriel de $\mathbb{F}_q[X]/(P)$ de dimension 1 engendré par 1 qui est dans le noyau de $\varphi - Id$. Comme $dim(Ker(\varphi - Id)) = r \geq 2$, il existe donc $V \in \mathbb{F}_q[X]$ non constant modulo P tel que $V^q \equiv V[P]$. En particulier, pour tout $i \in [\![1\,;r]\!]$, on a $V^q = V[P_i]$ (car si $V^q - V$ est divisible par P, il est aussi divisible par P_i) et on pose donc $\alpha_i \equiv V[P_i]$ (soit $\psi(V) = (\alpha_1, ..., \alpha_r)$) qui appartient à $\mathbb{F}_q$ d'après la proposition 4. Si pour tout $i, j \in [\![1\,;r]\!]$, on avait $\alpha_i = \alpha_j$, alors il existerait $\alpha \in \mathbb{F}_q$ tel que $V \equiv \alpha[P_i]$ pour tout $i \in [\![1\,;r]\!]$, et donc $V \equiv \alpha[P]$ (par injectivité de ψ), ce qui est impossible car on a supposé que V n'était pas constant modulo P. Ainsi il existe $i, j \in [\![1\,;r]\!]$ distincts tels que $\alpha_i \neq \alpha_j$. On pose alors $Q = \text{pgcd}(P, V - \alpha_i)$. Comme P_i divise P et $V - \alpha_i$, il divise aussi Q. De plus, P_j ne divise pas Q car il ne divise pas $V - \alpha_i$ puisque $\alpha_i \neq \alpha_j$. Ainsi, $Q \neq 1$ et $Q \neq P$, donc Q est un facteur non trivial de P. □

La preuve de ce théorème est constructive puisqu'elle fournit une manière de trouver un tel V : il suffit de calculer le noyau de l'application linéaire $\varphi - Id$. On en déduit un algorithme itératif puisque pour trouver un nouveau facteur, il suffit de recommencer ce procédé avec P/Q où $Q = \text{pgcd}(P, V - \alpha)$ le facteur non trivial trouvé précédemment (calculable par Euclide). L'algorithme s'arrête lorsque $dim(Ker(\varphi - Id)) = 1$, ce qui signifie que le polynôme est irréductible.

> Si P possède des facteurs carrés et $P' \neq 0$, on peut les récupérer en calculant $Q = \text{pgcd}(P, P')$. On peut alors utiliser l'algorithme pour factoriser P/Q qui est bien sans facteur carré. En réitérant le processus pour factoriser Q, on obtient ainsi la factorisation complète de P.
> Dans la cas $P' = 0$, il existe alors un polynôme $Q \in \mathbb{F}_q[X]$ tel que $P(X) = Q(X^p)$. D'après l'isomorphisme de Frobenius, il existe un polynôme $R \in \mathbb{F}_q[X]$ tel que $Q(X^p) = R(X)^p$: les coefficients de R sont les racines p-ièmes des coefficients de Q. Il suffit alors de factoriser R pour obtenir la factorisation de P.