Algorithme de Berlekamp

▷ **Leçons.** 122, 123, 141, 142

▷ **Développement.** Le but est de déterminer algorithmiquement la décomposition en facteurs premiers d'un polynôme sur un corps fini. L'algorithme de Berlekamp remplit cette tâche lorsque le polynôme est sans facteur carré. En général, on se ramène à ce cas grâce à des considérations sur des pgcd.

Soit donc p un nombre premier, $m \in \mathbb{N}^*$ et $q = p^m$. On considère un polynôme P de $\mathbb{F}_q[X]$, que l'on suppose dans un premier temps sans facteur carré. Sa décomposition en irréductibles est de la forme $P = P_1...P_r$ où les P_i sont irréductibles et premiers entre eux. Notons $A = \mathbb{F}_q[X]/\langle P\rangle$. On considère l'application

$$S \left| \begin{array}{ccc} A & \to & A \\ \overline{Q} & \mapsto & \overline{Q^q} \end{array} \right. .$$

Lemme 1. L'application S est bien définie et $\mathbb{F}_q$-linéaire.

Démonstration. Nous allons montrer que $S = \overline{T}$, où $\overline{T} : \overline{Q} \mapsto \overline{Q(X^q)}$ ce qui suffira pour conclure. Puisque le morphisme d'anneaux $T : Q \mapsto Q(X^q)$ de $\mathbb{F}_q[X]$ est constant sur $\mathbb{F}_q$ et qu'on est en caractéristique p, alors $T(Q) = Q^q$. En appliquant T puis en prenant l'image dans le quotient A, on obtient un morphisme $T' : Q \mapsto \overline{Q^q}$ à valeurs dans A. De plus, $\langle P\rangle$ est dans le noyau de T', donc T' passe au quotient en un morphisme $\overline{T} : A \to A$, avec $\overline{T}(\overline{Q}) = \overline{Q^q} = S(\overline{Q})$. □

Remarque. On peut voir autrement que cette application est bien définie : si $\overline{Q} = \overline{R}$, alors P divise $Q - R$. Or, $Q - R$ divise $Q^q - R^q$ donc P divise $Q^q - R^q$, c'est-à-dire $\overline{Q^q} = \overline{R^q}$.

Ce lemme permet de considérer $\ker(S - \mathrm{id})$ comme un $\mathbb{F}_q$-espace vectoriel, autorise à parler de sa dimension et à en prendre une base.

Proposition 2. Le nombre r de facteurs irréductibles du polynôme P est exactement la dimension de $\ker(S - \mathrm{id})$:

$$r = \dim(\ker(S - \mathrm{id})).$$

Démonstration. Soit $d = \deg(P)$. Pour $Q \in \mathbb{F}_q[X]$ notons $\overline{Q}$ son image dans le quotient A. Alors A est un $\mathbb{F}_q$-espace vectoriel de dimension d, dont une base est $\mathcal{B} = (\overline{1}, \overline{X}, ..., \overline{X^{d-1}})$.

Pour $1 \leqslant i \leqslant r$, notons $d_i = \deg(P_i)$ et $K_i = \mathbb{F}_q[X]/\langle P_i\rangle$. Puisque P_i est irréductible, alors K_i est un corps. Plus précisément, c'est une extension de degré d_i de $\mathbb{F}_q$, et donc K_i est isomorphe à l'unique corps $\mathbb{F}_{q^{d_i}}$ ayant q^{d_i} éléments.

Puisque les P_i sont premiers entre eux, par théorème chinois on a un isomorphisme

$$\varphi \left| \begin{array}{ccc} A & \to & K_1 \times ... \times K_r \\ \overline{Q} & \mapsto & (Q \bmod P_1, ..., Q \bmod P_r) \end{array} \right. .$$

Notons S_i le morphisme induit par S sur K_i, c'est-à-dire $S_i(Q \bmod P_i) = Q^q \bmod P_i$. Alors le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & K_1 \times ... \times K_r \\ {\scriptstyle S}\downarrow & & \downarrow{\scriptstyle (S_1,...,S_r)} \\ A & \xrightarrow[\varphi]{} & K_1 \times ... \times K_r \end{array}$$

commute. En effet,

$$\begin{array}{rcl} \varphi(S(\overline{Q})) & = & \varphi(\overline{Q^q}) \\ & = & (Q^q \bmod P_1, ..., Q^q \bmod P_r) \\ & = & (S_1(Q \bmod P_1), ..., S_r(Q \bmod P_r)) \\ & = & (S_1, ..., S_r)(\varphi(\overline{Q})). \end{array}.$$

Ainsi, $\ker(S - \mathrm{id})$ est isomorphe, comme espace-vectoriel, à $\ker(S_1, ..., S_r) = \ker(S_1) \times ... \times \ker(S_r)$. Or dans le corps K_i, extension de $\mathbb{F}_q$, les seuls éléments vérifiant $\alpha^q = \alpha$ sont exactement ceux de $\mathbb{F}_q$. On a donc

$$\ker(S - \mathrm{id}) \simeq \mathbb{F}_q \times ... \times \mathbb{F}_q = (\mathbb{F}_q)^r$$

et $\dim(\ker(S - \mathrm{id})) = r$. □

Proposition 3. Soit $Q \in \mathbb{F}_q[X]$ tel que $\overline{Q} \in \ker(S - \mathrm{id})$. Alors

$$P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, Q - \alpha).$$

Démonstration. Notons $\alpha_i = Q \bmod P_i$. Puisque $\overline{Q} \in \ker(S - \mathrm{id})$, alors $\alpha_i \in \mathbb{F}_q$. Soit $\alpha \in \mathbb{F}_q$ quelconque, et

$$R_\alpha = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{r} P_i.$$

Alors R_α divise P. Puisque les P_i sont premiers entre eux, et que P_i divise $Q - \alpha_i$, alors R_α divise également $Q - \alpha$. Donc R_α divise $\mathrm{pgcd}(P, Q - \alpha)$. Réciproquement, ce pgcd doit diviser P donc s'écrit comme un produit de P_i. Il doit également diviser $Q - \alpha$. Or, P_i ne divise $Q - \alpha$ que si $\alpha_i = \alpha$. En définitive, on a $\mathrm{pgcd}(P, Q - \alpha) = R_\alpha$. Il s'ensuit

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

□

Notons $\mathcal{B} = (\overline{1}, \overline{X}, ..., \overline{X^{d-1}})$ une base de A. On peut maintenant énoncer l'algorithme de Berlekamp, et prouver qu'il est correct.

Théorème 4 (Algorithme de Berlekamp). Soit $P \in \mathbb{F}_q[X]$ sans facteur carré. L'algorithme suivant permet de déterminer la décomposition en produit d'irréductibles de P. On rappelle que $d = \deg(P)$.

1. Pour $0 \leqslant i \leqslant d - 1$, calculer $S(\overline{X^i}) = (X^i)^q \bmod P$, en déduire $\mathrm{Mat}_{\mathcal{B}}(S - \mathrm{id})$.

2. Calculer $\ker(S - \mathrm{id})$ ainsi que $r = \dim(\ker(S - \mathrm{id}))$.
3. Si $r = 1$, renvoyer P.
4. Sinon, prendre $\overline{Q} \in \ker(S - \mathrm{id})$ non-constant et calculer $\mathrm{pgcd}(P, Q - \alpha)$ pour tout $\alpha \in \mathbb{F}_q$. On recommence depuis le début avec chacun des $\mathrm{pgcd}(P, Q - \alpha)$ qui sont différents de 1 et de P.

Démonstration. La proposition 2 montre que si $r = 1$, alors P est irréductible. Le troisième point est donc correct. Si $r > 1$, alors il existe $\overline{Q} \in \ker(S - \mathrm{id})$ non-constant. La proposition 3 montre que $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, Q - \alpha)$. Comme $\overline{Q}$ est pris non-constant il existe $i \neq j$ tel que $\alpha_i \neq \alpha_j$ (où on note comme précédemment $\alpha_i = Q \bmod P_i$). Alors $\mathrm{pgcd}(P, Q - \alpha_i)$ et $\mathrm{pgcd}(P, Q - \alpha_j)$ donnent deux facteurs non-triviaux différents, puisque l'un contient P_i mais pas P_j et inversement. Ainsi, il existe des $\mathrm{pgcd}(P, Q - \alpha)$ différent de 1 et de P. Le quatrième point relance donc l'algorithme sur des polynômes sans facteurs carrés (car ce sont des diviseurs de P) de degré strictement inférieur à d, de sorte que la procédure termine. □

Remarque. Alternativement, on peut dans l'étape 2 calculer une base $(Q_1, ..., Q_r)$ de $\ker(S - \mathrm{id})$. Puis, partant de $\{P\}$, on applique l'étape 4 avec $Q = Q_1$ (s'il n'est pas constant) pour obtenir des facteurs $R_1, ..., R_k$ non-triviaux de P. On remplace $\{P\}$ par $\{R_1, ..., R_k\}$ et on applique l'étape 4 à ces facteurs, en prenant $Q = Q_2$ (s'il n'est pas constant). On continue jusqu'à obtenir l'ensemble des r facteurs irréductibles. Puisqu'au moins $r - 1$ éléments parmi $Q_1, ..., Q_r$ ne sont pas constants, et puisque le cardinal de l'ensemble qu'on construit croît strictement, on est sûr d'obtenir les r facteurs après avoir appliqué l'étape 4 avec chacun des éléments non-constants de la base.

On sait maintenant factoriser un polynôme P sur un corps fini n'ayant pas de facteur carré. Pour appliquer l'algorithme de Berlekamp, il faut donc s'assurer que P vérifie cette condition.

Proposition 5. Soit $P \in \mathbb{F}_q[X]$. Alors le polynôme P est sans facteur carré si et seulement si $\mathrm{pgcd}(P, P') = 1$.

Démonstration. Soit $P = \prod_i^r P_i^{m_i}$ la décomposition en irréductibles de P. On a

$$P' = \sum_{i=1}^{r} m_i P_i' P_i^{m_i - 1} \prod_{k \neq i} P_k^{m_k}.$$

Si $m_i \neq 0$ dans $\mathbb{F}_q$, alors P' est divisible par $P_i^{m_i - 1}$ mais pas par $P_i^{m_i}$. Si $m_i = 0$ dans $\mathbb{F}_q$, alors P' est divisible par $P_i^{m_i}$. Ainsi,

$$\mathrm{pgcd}(P, P') = \prod_{i=1}^{r} P_i^{m_i'}$$

avec $m_i' = m_i$ si $m_i = 0$ dans $\mathbb{F}_q$ et $m_i' = m_i - 1$ sinon. Donc $\mathrm{pgcd}(P, P') = 1$ si et seulement si tous les m_i valent 1, c'est-à-dire si et seulement si P est sans facteur carré. □

Lemme 6. Soit $P \in \mathbb{F}_q[X]$. Alors $P' = 0$ si et seulement s'il existe $Q \in \mathbb{F}_q[X]$ tel que $P = Q^p$.

Démonstration. En écrivant $P = \sum_i a_i X^i$, on a $P' = \sum_i i a_i X^{i-1}$. Donc $P' = 0$ si et seulement si tous les ia_i sont nuls. Puisque $\mathbb{F}_q$ est de caractéristique p (avec $q = p^m$), alors pour les i non-multiples de p on a $a_i = 0$. Ainsi, $P = \sum_k a_{kp} X^{kp}$. Or, l'application $x \mapsto x^p$ est un automorphisme du corps $\mathbb{F}_q$ donc pour tout k il existe b_k tel que $a_{kp} = b_k^p$. On a donc

$$P = \sum_k a_{kp} X^{kp} = \sum_k (b_k X^k)^p = \left(\sum_k b_k X^k \right)^p = Q^p.$$

Réciproquement, si $P = Q^p$ alors $P' = pQ'Q^{p-1} = 0$ car $\mathbb{F}_q$ est de caractéristique p. □

Ceci suggère l'algorithme suivant de factorisation dans $\mathbb{F}_q[X]$.

Proposition 7 (Factorisation dans les corps finis). Soit $P \in \mathbb{F}_q[X]$. L'algorithme suivant permet de déterminer la décomposition en produit d'irréductibles de P.

1. Calculer $\text{pgcd}(P, P')$.
2. Si $\text{pgcd}(P, P') = 1$, appliquer l'algorithme de Berlekamp à P.
3. Sinon, si $\text{pgcd}(P, P') = P$, calculer $Q \in \mathbb{F}_q[X]$ tel que $P = Q(X^p) = Q^p$ et revenir au point 1 avec Q.
4. Sinon, revenir au point 1 avec $\text{pgcd}(P, P')$ et $\frac{P}{\text{pgcd}(P,P')}$.

▷ Questions possibles.

Question. Quelle est la complexité de l'algorithme de Berlekamp ?

Réponse. Voir votre cours d'option C ! □

Question. Peut-on utiliser cet algorithme pour factoriser un polynôme dans $\mathbb{Z}[X]$? Dans $\mathbb{Q}[X]$?

Réponse. Si $P \in \mathbb{Z}[X]$, on peut imaginer choisir p suffisamment grand et factoriser dans $\mathbb{F}_p[X]$. Le "suffisamment grand" signifie que les coefficients des facteurs de P ne doivent pas être plus grand que p en valeurs absolues. Il existe des résultats type borne de Landau-Mignotte qui permettent de majorer la taille des coefficients d'un diviseur de P. On peut aussi imaginer factoriser dans plusieurs $\mathbb{F}_p[X]$ et utiliser le théorème chinois. Il existe également une méthode de remontée passant par les $\mathbb{F}_{p^n}[X]$, basée sur un lemme de Hensel.

Si $P \in \mathbb{Q}[X]$ on s'appuie sur le lemme de Gauss. On peut chasser les dénominateurs et se ramener à décomposer $\alpha Q \in \mathbb{Z}[X]$. En effet, si Q est réductible dans $\mathbb{Q}[X]$ alors αQ l'est aussi, et l'est donc dans $\mathbb{Z}[X]$ car il est à coefficients entiers. On trouve les facteurs irréductibles de αQ dans $\mathbb{Z}[X]$, et ces facteurs sont aussi irréductibles dans $\mathbb{Q}[X]$. □

▷ **Références.** Personnellement j'aime bien la rédaction concise de [Dem08]. On trouve une version plus détaillée dans [BMP05] et une présentation un peu différente dans [But12].

[BMP05] Vincent Beck, Jérôme Malick et Gabriel Peyré : *Objectif agrégation*. H&K, 2005.

[But12] Frédéric Butin : *Algèbre - Polynômes, théorie de Galois et applications informatiques*. Hermann, 2012.

[Dem08] Michel Demazure : *Cours d'algèbre*. Cassini, 2008.