

Factorisation dans $\mathbb{Z}[x]$

MAO et préparation à l'Agrégation
Orsay, novembre 2006
Jacques Peyrière

1 Décomposition en produit de facteurs sans facteurs carrés

On désigne par \mathcal{A} un anneau factoriel de caractéristique p .

Proposition 1. *Soit $P \in \mathcal{A}[x]$ un polynôme. Alors, on a*

$$P = \prod_{i=1}^{\nu} A_i^i,$$

où les polynômes $A_i \in \mathcal{A}[x]$ sont deux-à-deux premiers entre eux. De plus, cette décomposition est unique à multiplication près des facteurs par des unités.

Démonstration. Une telle décomposition s'obtient en regroupant dans la décomposition primaire de P les facteurs de même multiplicité. L'unicité résultera de l'algorithme de décomposition ci-après.

Si l'on a une telle décomposition, on a

$$P' = \sum_{i=1}^{\nu} i A_i' A_i^{i-1} \prod_{\substack{1 \leq j \leq \nu \\ j \neq i}} A_j^j = \sum_{\substack{1 \leq i \leq \nu \\ p \nmid i}} i A_i' A_i^{i-1} \prod_{\substack{1 \leq j \leq \nu \\ j \neq i}} A_j^j. \quad (1)$$

Si Q est un facteur irréductible de P , il existe ℓ tel que Q divise A_ℓ . Alors Q^ℓ divise le $i^{\text{ième}}$ terme de (1) et, si p ne divise pas ℓ , $Q^{\ell-1}$ divise le $\ell^{\text{ième}}$ terme, mais Q^ℓ ne le divise pas puisque A_ℓ est sans facteur multiple. En définitive on obtient

$$\text{pgcd}(P, P') = \prod_{\substack{1 \leq i \leq \nu \\ p \nmid i}} A_i^{i-1} \prod_{\substack{1 \leq i \leq \nu \\ p \mid i}} A_i^i.$$

Définissons par récurrence deux suites de polynômes :

$$\begin{aligned} P_1 &= \text{pgcd}(P, P'), \quad B_1 = P/P_1, \quad \text{et, pour } k \geq 1, \\ B_{k+1} &= \begin{cases} \text{pgcd}(P_k, B_k), & \text{si } p \nmid k, \\ B_k, & \text{si } p \mid k \end{cases} \quad \text{et } P_{k+1} = P_k/B_{k+1}. \end{aligned}$$

On vérifie par récurrence les faits suivants :

$$B_k = \prod_{\substack{k \leq i \leq \nu \\ p \nmid i}} A_i \quad \text{et} \quad P_k = \prod_{\substack{k \leq i \leq \nu \\ p \nmid i}} A_i^{i-k} \prod_{\substack{1 \leq i \leq \nu \\ p \mid i}} A_i^i.$$

A partir d'un certain rang (inférieur ou égal à $\nu + 1$), B_k est égal à 1. Si la caractéristique est nulle, on a identifié tous les facteurs A_i ($A_i = B_i/B_{i+1}$), sinon on a seulement identifié ceux dont l'indice n'est pas multiple de p , les autres facteurs étant regroupés dans P_ν .

Dans ce dernier cas, on a

$$P_\nu = \prod_{\substack{1 \leq i \leq \nu \\ p \mid i}} A_i^i = \left(\prod_{1 \leq i \leq \nu/p} A_{ip}^i \right)^p,$$

d'où $P_\nu(x) = Q(x^p)$ pour un polynôme $Q \in \mathcal{A}[x]$ convenable. Pour obtenir les facteurs manquants, on recommence les mêmes opérations avec Q au lieu de P .

2 L'algorithme de Berlekamp

Etant donné un nombre premier p , on considère le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Il s'agit de construire la décomposition primaire d'un polynôme $P \in \mathbb{F}_p[x]$ sans facteurs multiples. Soit donc $P = P_1 P_2 \cdots P_r$ (où les P_j sont des polynômes irréductibles distincts) un tel polynôme.

On considère l'algèbre $\mathcal{R} = \mathbb{F}_p[x]/(P)$ et les corps $\mathcal{R}_i = \mathbb{F}_p[x]/(P_i)$, pour $i = 1, 2, \dots, r$. L'application $\Gamma : (f \bmod P) \mapsto (f \bmod P_i)_{1 \leq i \leq r}$ est un isomorphisme d'algèbres de \mathcal{R} sur $\mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_r$. Nous noterons Γ_i les applications coordonnées.

Par ailleurs l'application de Frobenius Φ_p , définie par $\Phi_p(f) = f^p$ pour $f \in \mathcal{R}$, est \mathbb{F}_p -linéaire ; en effet, l'algèbre \mathcal{R} étant de caractéristique p , on a $(f + g)^p = f^p + g^p$, puisque, si p est un nombre premier, les coefficients binomiaux $\binom{p}{j}$, pour $1 \leq j < p$ sont multiples de p .

Désignons par Id l'application identité sur \mathcal{R} . Un élément f est dans le noyau de $\Phi_p - \text{Id}$ si et seulement si, pour tout i , on a $\Gamma_i(f)^p - \Gamma_i(f) = 0$ dans

le corps \mathcal{R}_i . Cela signifie que $\Gamma_i(f)$ appartient à \mathbb{F}_p (qui est un sous-corps de \mathcal{R}_i). Autrement dit la classe modulo P d'un polynôme f est dans le noyau de $\Phi_p - \text{Id}$ si et seulement si, pour tout $i \in \{1, 2, \dots, r\}$, il existe $\alpha_i \in \mathbb{F}_p$ tel que $f \equiv \alpha_i \pmod{P_i}$. Par suite, le noyau $\ker(\Phi_p - \text{Id})$ a p^r éléments et donc est un espace vectoriel de dimension r sur \mathbb{F}_p .

Ainsi, nous avons un moyen de déterminer le nombre de facteurs irréductibles de P . Voyons maintenant comment déterminer effectivement ces facteurs, si $r > 1$.

Proposition 2. *Soit (e_1, \dots, e_r) une base de $\ker(\Phi_p - \text{Id})$ supposé de dimension strictement supérieure à 1. Pour tout couple (i, j) tel que $1 \leq i < j \leq r$ il existe $k \in \{1, 2, \dots, r\}$ tel que*

$$e_k \not\equiv (e_k \pmod{P_i}) \pmod{P_j}.$$

Démonstration. Raisonnons par l'absurde. Supposons fautive la conclusion de cette proposition : il existe i, j , avec $i < j$ tels que, pour tout k , il existe $\alpha_k \in \mathbb{F}_k$ tel que $e_k \equiv \alpha_k \pmod{P_i}$ et $e_k \equiv \alpha_k \pmod{P_j}$. Alors, si f appartient au noyau de $\Phi_p - \text{Id}$, c'est-à-dire $f = \lambda_1 e_1 + \dots + \lambda_r e_r$, on a $f \equiv \sum \lambda_k \alpha_k \pmod{P_i}$ et P_j , ce qui contredit le fait que le noyau soit de dimension r .

Paraphrasons cette proposition : avec les mêmes notations, cela signifie qu'il existe $\alpha \in \mathbb{Z}$ tel que $e_k - \alpha$ soit divisible par P_i mais non par P_j .

Ainsi on obtiendra un facteur non trivial de P parmi les polynômes $\text{pgcd}(e_\ell - \alpha, P)$, où $1 \leq \ell \leq r$ et $\alpha \in \mathbb{F}_p$.

3 Factorisation modulo p^k : lemme de Hensel

Dans cette section, p désigne un nombre premier fixé.

Lemme 3 (Hensel). *Soit P, A_1 et B_1 des polynômes à coefficients entiers rationnels en la variable x tels que*

1. $P \equiv A_1 B_1 \pmod{p}$,
2. A_1 est unitaire, $\deg A_1 > 0$ et $\deg A_1 + \deg B_1 \leq \deg P$,
3. les polynômes A_1 et B_1 sont premiers modulo p .

Alors, pour tout $k \geq 2$ il existe deux polynômes A_k et B_k , uniques modulo p^k , tels que

1. $P \equiv A_k B_k \pmod{p^k}$,
2. $A_k \equiv A_{k-1} \pmod{p^{k-1}}$ et $B_k \equiv B_{k-1} \pmod{p^{k-1}}$,

3. $\deg A_k + \deg B_k \leq \deg P$ (avec égalité dès que p^k ne divise pas le premier coefficient de P).

Démonstration. Puisque A_1 et B_1 sont premiers entre eux modulo p il existe deux polynômes U et V à coefficients entiers tels que $A_1U + B_1V \equiv 1 \pmod p$, $\deg U < \deg B_1$ et $\deg V < \deg A_1$.

Supposant établie l'existence de A_k et B_k , construisons A_{k+1} et B_{k+1} . On les cherche sous la forme $A_{k+1} = A_k + p^k C$ et $B_{k+1} = B_k + p^k D$, avec $C, D \in \mathbb{Z}[x]$. On doit donc avoir

$$A_k D + B_k C \equiv (P - A_k B_k) / p^k \pmod p. \quad (2)$$

Or, évidemment, $A_k U + B_k V \equiv 1 \pmod p$. Par suite toutes les solutions de l'équation (??) sont de la forme $D = UQ + WB_k$, $C = VQ - WA_k$, où $W \in \mathbb{Z}[x]$ et où l'on a posé $Q = (P - A_k B_k) / p^k$. De plus, il y a une seule solution telle que $\deg C \leq \deg A$; elle est obtenue lorsque C est le reste modulo p de la division euclidienne de VQ par A_k .

Choisissons pour W le quotient de la division euclidienne de VQ par le polynôme A_k (dont on rappelle qu'il est unitaire). Posons

$$C = VQ - WA_k \pmod p \quad \text{et} \quad D = UQ + WB_k \pmod p.$$

Alors, on a $\deg C < \deg A_k$, $A_k D + B_k C \equiv (P - A_k B_k) / p^k \pmod p$ et $\deg D \leq \deg B_k$. Il suffit alors de poser $A_{k+1} = A_k + p^k C$ et $B_{k+1} = B_k + p^k D$.

Le lemme de Hensel permet donc de relever certaines factorisations modulo p en factorisations modulo p^k pour tout $k \geq 1$. Autrement dit une telle factorisation donne lieu à une factorisation du polynôme de départ considéré comme élément de $\mathbb{Z}_p[x]$.

4 Majoration des coefficients des facteurs d ; un polynôme

Soit $P \in \mathbb{C}[x]$ un polynôme de degré n dont les racines sont z_1, z_2, \dots, z_n :

$$P = a_n \prod_{j=1}^n (x - z_j) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0. \quad (3)$$

Définitions 4. On appelle *mesure* de P le nombre

$$M(P) = |a_n| \prod_{1 \leq j \leq n} \max(1, |z_j|).$$

On posera aussi $\|P\|_2 = (|a_0|^2 + |a_1|^2 \dots + |a_n|^2)^{1/2}$.

Il est facile de vérifier que l'on a $M(x^n P(1/x)) = M(P)$ et $M(PQ) = M(P)M(Q)$.

L'un des intérêts de cette notion est la majoration des coefficients qu'elle fournit.

Proposition 5. *Soit P un polynôme comme en (??). On a*

$$\max_{0 \leq j \leq n} |a_j| \leq \binom{n}{[n/2]} M(P).$$

Démonstration. Cela résulte de l'expression des coefficients d'un polynôme comme fonctions symétriques des racines :

$$a_{n-j} = (-1)^{n-j} a_n \sum_{1 \leq k_1 < \dots < k_j \leq n} z_{k_1} \dots z_{k_j}.$$

On obtient $|a_{n-j}| \leq \binom{n}{j} M(P)$, d'où l'assertion.

Reste maintenant à donner une majoration aisément calculable de $M(P)$.

Lemme 6. *Pour tout polynôme P comme en (??) et pour tout nombre complexe z , on a*

$$\|(x - z)P\|_2 = \|(\bar{z}x - 1)P\|_2.$$

Démonstration. On sait que $\|P\|_2^2 = \frac{1}{2\pi} \int_0^{2\pi} |P(e^{it})|^2 dt$. La conclusion vient de $|e^{it} - z| = |e^{-it} - \bar{z}| = |1 - \bar{z}e^{it}|$.

Théorème 7. *On a $M(P)^2 + |a_0 a_n| M(P)^{-2} \leq \|P\|_2^2$.*

Démonstration. Soit $(z_j)_{1 \leq j \leq n}$ les racines de P de modules ≥ 1 . Considérons le polynôme

$$Q = a_n \prod_{j=1}^n (\bar{z}_j x - 1) \prod_{\ell < j \leq n} (x - z_j) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0.$$

Un application répétée du lemme précédent montre que l'on a $\|Q\|_2 = \|P\|_2$. En outre

$$\|Q\|^2 \geq |b_0|^2 + |b_n|^2 = |a_0 a_n|^2 M(P)^{-2} + M(P)^2,$$

en effet $|b_0| = |a_n| \prod \min(1, |z_j|) = |a_n| \prod |z_j| / \prod \max(1, |z_j|) = |a_0 a_n| / M(P)$.

Corollaire 8. *Soit $P = QR$ un produit de deux polynômes à coefficients entiers rationnels de degrés m et n . Si $H(Q)$ désigne le maximum des valeurs absolues des coefficients de Q , on a*

$$H(Q) \leq \binom{m}{[m/2]} M(P) \leq \binom{m}{[m/2]} \|P\|_2.$$

Démonstration. Il suffit de remarquer que l'on a $M(Q) \leq M(P)$.

5 Conclusion

Maintenant, nous pouvons donner un algorithme de factorisation d'un polynôme P sur \mathbb{Z} . On réduit d'abord le problème à la recherche des facteurs d'un polynôme sans facteurs multiples.

Si le polynôme P de degré n n'est pas irréductible, il a un facteur Q de degré inférieur ou égal à $n/2$. Les valeurs absolues des coefficients de Q sont inférieures à $\binom{\lfloor n/2 \rfloor}{\lfloor n/4 \rfloor} \|P\|_2$.

Choisissons un nombre premier p tel que $P \pmod p$ soit sans facteur multiple dans $\mathbb{F}_p[x]$. Pour ce faire, il suffit de choisir pour p un nombre premier ne divisant pas le résultant de P et P' (ou, si l'on préfère, un nombre premier ne divisant pas le discriminant de P). Certainement, $Q \pmod p$ est un facteur non trivial (non nécessairement irréductible, même si Q l'est) de $P \pmod p$ dans $\mathbb{F}_p[x]$.

Prenons un nombre entier k tel que $p^k > 2 \binom{\lfloor n/2 \rfloor}{\lfloor n/4 \rfloor} \|P\|_2$ et utilisons le lemme de Hensel pour obtenir à partir de $Q \pmod p$ une factorisation de P modulo p^k . Si l'on prend comme représentants des éléments de $\mathbb{Z}/p^k\mathbb{Z}$ les nombres entiers compris entre $-\lfloor (p^k - 1)/2 \rfloor$ et $\lfloor p^k/2 \rfloor$, vu l'unicité de la factorisation modulo p^k et la borne sur les coefficients de Q , nécessairement Q sera l'un des termes de cette factorisation.

Pour trouver une factorisation, on peut procéder comme suit. On factorise d'abord P modulo p :

$$P \equiv C_1 C_2 \dots C_r \pmod p,$$

où les C_i sont des éléments irréductibles distincts de $\mathbb{F}_p[x]$.

Si $r = 1$ le polynôme P est irréductible. Si $r \geq 2$, on considère tour à tour les partitions $I \cup J$ de l'ensemble $\{1, 2, \dots, r\}$. On pose $A = c \prod_{i \in I} C_i$ et $B = c^{-1} \prod_{i \in J} C_i$ de façon que A soit unitaire. On effectue un certain nombre de remontées de Hensel pour obtenir une factorisation $A_k B_k$ à deux termes modulo p^k (en ayant choisi comme ci-dessus les représentants modulo p^k). Si l'un des polynômes A_k ou B_k a un facteur commun avec P , on a trouvé un facteur non trivial de P . Si l'on a épuisé toutes les partitions sans trouver de facteur, c'est que P est irréductible.