Factorisation de Lagrange pour les racines multiples d'un polynôme

Roland Ven, Nicolas Boulenguez

janvier 2020

Résumé

Le résultat le plus célèbre de Galois rend improbable un algorithme explicite, basé sur des opérations élémentaires, décomposant un polynôme quelconque en facteurs de degré 1. À défaut, cet article présente une décomposition due à Lagrange en facteurs *à racines simples*.

Il reprend, en plus détaillé, un extrait d'un livre de Georges Valiron.

Mots-clefs : factorisation polynômiale, racine simple, racine multiple.

Étant donné un polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, $n \geqslant 3$, a_i complexes, la méthode de Lagrange permet de déterminer effectivement des polynômes $P_1(X), P_2(X), \cdots, P_q(X)$ tels que

$$P(X) = P_1(X) \times (P_2(X))^2 \times \cdots \times (P_q(X))^q$$

où chacun des $P_j(X)$ n'a que des racines *simples* ou est égal à 1, tout ceci *sans qu'il soit nécessaire de calculer les racines* de $P(X)$.

On reviendra après l'exposé de la méthode sur le problème de la séparation des racines lorsque $P(X)$ est à coefficients *réels*.

Notation PGCD$(U(X), V(X))$ désigne, à un coefficient multiplicatif près, un PGCD des polynômes (non nuls) $U(X)$ et $V(X)$.

Prérequis

— Les techniques élémentaires de calcul polynômial, par exemple décrites par `wikipedia`, suffisent pour appliquer la méthode, à savoir dérivation (terme à terme), division euclidienne (suivant les puissances décroissantes) et calcul de PGCD (par l'algorithme d'Euclide). De nombreux logiciels effectuent ces calculs efficacement, mais on les pratique sans difficulté à la main pour des degrés raisonnables.

— Pour suivre les justifications et la démonstration finale : les propriétés classiques dans $\mathbb{C}[X]$, en particulier lien entre racines multiples et dérivation, caractérisation d'un PGCD de deux polynômes non nuls.

1 Présentation de la méthode

1.1 Définition des polynômes $P_j(X)$

Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, $n \geqslant 3$, a_i complexes.
Soient $x_1, \cdots, x_r$ les racines (distinctes) de $P(X)$.
Sans qu'il soit nécessaire de calculer ces racines, on a donc

$$P(X) = (X - x_1)^{h(1)} \times \cdots \times (X - x_r)^{h(r)} \quad \text{où } h(k) \text{ est l'ordre de la racine } x_k.$$

Désignons par q le plus grand des $h(k)$ présents dans cette égalité, autrement dit le plus grand des ordres des racines de $P(X)$.

Pour tout entier j de 1 à q, on définit alors $P_j(X)$ selon les trois seuls cas possibles :
— si $P(X)$ n'a aucune racine d'ordre j, $P_j(X) = 1$;
— si x_i est la *seule* racine d'ordre j de $P(X)$, $P_j(X) = (X - x_i)$;
— si $P(X)$ a au moins deux racines d'ordre j, $P_j(X) = \prod_i (X - x_i)$, produit étendu à tous les x_i racines d'ordre j de $P(X)$.

Dans l'égalité $P(X) = (X - x_1)^{h(1)} \times \cdots \times (X - x_r)^{h(r)}$, si au moins deux x_i ont le même ordre j, on considère $\prod_i (X - x_i)^j$, produit étendu à *tous* les x_i racines d'ordre j de $P(X)$, on a alors

$$\prod_i (X - x_i)^j = \left(\prod_i (X - x_i) \right)^j = \left(P_j(X) \right)^j.$$

On en déduit : $P(X) = P_1(X) \times (P_2(X))^2 \times \cdots \times \left(P_q(X) \right)^q$, où q est le plus grand des ordres des racines de $P(X)$.

Remarque. Dans le cas particulier où $P(X)$ n'a que des racines simples, cette égalité se lit $P(X) = P_1(X)$.

Remarque. La définition de $P_j(X)$ rend clair que $P_j(X)$ ne peut avoir que des racines simples, et que, pour $j \neq k$, $P_j(X)$ et $P_k(X)$ n'ont aucune racine commune.

1.2 Propriété principale

Dans la suite, abrégeons $P = P(X)$, $P_1 = P_1(X)$, *etc*, et notons P' le polynôme dérivé de P. Avec ces notations, $P = P_1 P_2^2 \cdots P_q^q$.

Propriété 1 ((démontrée en fin d'article)). *Avec les définitions ci dessus pour les* P_j, $P = P_1 P_2^2 \cdots P_q^q = \prod_{j=1}^{q} P_j^j$ *implique que*

$$\mathrm{PGCD}(P, P') = P_2 P_3^2 \cdots P_q^{q-1} = \prod_{j=2}^{q} P_j^{j-1}.$$

Remarque. Dans le cas particulier où P n'a que des racines simples, l'égalité ci dessus se lit $\mathrm{PGCD}(P, P') = 1$.

1.3 Algorithme

Posons

$$\begin{aligned} Q_0 = P &= P_1 P_2^2 \cdots P_q^q && \text{et} \\ Q_1 = \mathrm{PGCD}(Q_0, Q_0') &= P_2 \cdots P_q^{q-1} && \text{d'après la propriété ci dessus.} \end{aligned}$$

On avait déjà remarqué que P_j ne peut avoir que des racines simples et que, pour $j \neq k$, P_j et P_k n'ont aucune racine commune, ce qui fait que les racines de P_2 sont les racines d'ordre 1 de Q_1, et ainsi de suite… les racines de P_q sont les racines d'ordre $q-1$ de Q_1. La propriété 1 s'applique donc à $Q_1 = P_2 \cdots P_q^{q-1}$ (avec un décalage d'indice).

$$\begin{aligned} Q_2 = \mathrm{PGCD}(Q_1, Q_1') &= P_3 \cdots P_q^{q-2} && \text{et ainsi de suite jusque} \\ Q_{q-2} = \mathrm{PGCD}(Q_{q-3}, Q_{q-3}') &= P_{q-1} P_q^2 && \\ Q_{q-1} = \mathrm{PGCD}(Q_{q-2}, Q_{q-2}') &= P_q && \text{et enfin} \\ Q_q = \mathrm{PGCD}(Q_{q-1}, Q_{q-1}') &= 1 && \text{car } P_q \text{ est à racines simples} \end{aligned}$$

Les polynômes Q_i sont tous calculés par dérivation de polynômes et recherche d'un PGCD de deux polynômes non nuls (par exemple, en utilisant l'algorithme d'Euclide), tout ceci *sans qu'il soit nécessaire* de calculer les racines de P(X) ou de connaître les P_j a priori. L'algorithme s'arrête lorsque le PGCD est une constante. L'entier q est alors connu par le *nombre d'étapes franchies*, et le polynôme P_q comme *dernier PGCD* non constant.

Par construction, $Q_t = P_{t+1} \cdots P_q Q_{t+1}$ pour t de 0 à $q-2$. Adoptons une

notation pour le quotient de Q_t par son successeur.

$$\begin{aligned}
R_1 = \frac{Q_0}{Q_1} &= P_1 \cdots P_q \\
R_2 = \frac{Q_1}{Q_2} &= P_2 \cdots P_q && \text{et ainsi de suite jusque} \\
R_{q-1} = \frac{Q_{q-2}}{Q_{q-1}} &= P_{q-1} P_q, && \text{avec enfin} \\
R_q = \frac{Q_{q-1}}{Q_q} &= P_q && \text{déjà connu, et cohérent puisque } Q_q = 1
\end{aligned}$$

On obtient alors les P_j en divisant chaque R_j par R_{j+1}, pour j de 1 à $q-1$.

$$\begin{aligned}
P_1 &= \frac{R_1}{R_2} \\
P_2 &= \frac{R_2}{R_3} && \text{puis ainsi de suite jusque} \\
P_{q-1} &= \frac{R_{q-1}}{R_q} \\
P_q &= R_q && \text{est déjà connu}
\end{aligned}$$

Ce procédé effectif factorise ainsi P sous la forme $P_1 P_2^2 \cdots P_q^q$, *q étant connu, ainsi que chacun des* P_j. La recherche des racines de P se ramène à la recherche de celles des P_j, qui sont toutes des racines simples (il va de soi que, dans le résultat final, on omet les facteurs pour lesquels $P_j = 1$). De plus, si P présente au moins une racine multiple, le degré des P_j est strictement inférieur à celui de P, ce qui offre de nouvelles opportunités de calcul des racines de P.

L'algorithme se résume formellement par

$$Q_0 = P \qquad Q_{i+1} = \mathrm{PGCD}(Q_i, Q_i') \qquad R_{i+1} = \frac{Q_i}{Q_{i+1}} \qquad P_{i+1} = \frac{R_{i+1}}{R_{i+2}}$$

et le pseudo-code suivant, paramétrisé par le polynôme `p` à factoriser et une procédure `traiter` décrivant ce qu'il faut faire des facteurs obtenus.

```
q1 := pgcd (p, derivée (p));
r1 := division_exacte (p, q1);
répéter
   q2 := pgcd (q1, derivée (q1));
   r2 := division_exacte (q1, q2);
   traiter (division_exacte (r1, r2));
   arrêter quand degré (q1) = 0;
   q1 := q2;
   r1 := r2;
fin répéter;
```

En pratique, il est utile de savoir que la plupart des bibliothèques logicielles fournissent une division polynômiale alternative, plus rapide mais seulement applicable lorsqu'il est connu à l'avance que le reste est nul.

1.4 Exemple

L'exemple suivant est une addition à l'ouvrage de Georges Valiron. Le polynôme étudié étant de degré 4, on pourrait péniblement calculer ses racines directement.

$P = X^4 + X^3 - 3X^2 - 5X - 2 = Q_0$, ainsi $Q_0' = 4X^3 + 3X^2 - 6X - 5$.
$Q_1 = \mathrm{PGCD}(Q_0, Q_0') = X^2 + 2X + 1$ (par logiciel de calcul, ou algorithme d'Euclide si on n'en dispose pas), $Q_1' = 2X + 2$
$Q_2 = \mathrm{PGCD}(Q_1, Q_1') = X + 1$, $Q_2' = 1$.
$Q_3 = \mathrm{PGCD}(Q_2, Q_2') = 1$, on reconnaît $q = 3$, et $P_3 = Q_2 = X + 1$.

En résumé $P = Q_0 = X^4+X^3-3X^2-5X-2$, $Q_1 = X^2+2X+1$, $Q_2 = X+1 = P_3$ et $q = 3$, ce qui permet de poursuivre :

$$R_1 = \frac{Q_0}{Q_1} = X^2 - X - 2$$
$$R_2 = \frac{Q_1}{Q_2} = X + 1 \qquad \text{et pour terminer}$$
$$R_3 = P_3 = X + 1$$

On obtient :

$$P_1 = \frac{R_1}{R_2} = \frac{X^2 - X - 2}{X + 1} = X - 2$$
$$P_2 = \frac{R_2}{R_3} = \frac{X + 1}{X + 1} = 1 \qquad \text{et}$$
$$P_3 = X + 1 \qquad \text{est déjà connu}$$

Conclusion : $P = (X - 2).(X + 1)^3$ (on omet $P_2 = 1$).

> *La suite de l'article n'est pas une reprise de l'extrait du livre de Georges Valiron, mais il se peut que ce soit évoqué ailleurs dans ce livre, la totalité du livre n'étant pas à disposition.*

2 Cas d'un polynôme réel

2.1 Applicabilité de la méthode

Le procédé décrit ne nécessite que des dérivations, des divisions euclidiennes et des calculs de plus petit commun diviseur. Or ces opérations produisent des résultats réels lorsque leurs arguments sont réels. Ainsi, lorsque P a des coefficients réels, chaque résultat intermédiaire aussi, et en particulier les P_j finaux.

2.2 Séparation des racines

La connaissance des P_j peut simplifier le problème de la séparation des racines de $P(X) \in \mathbb{R}[X]$.

Par exemple, lors de l'application du théorème de Sturm, une pratique commune est de remplacer P par

$$R_1 = \frac{P}{PGCD(P, P')}$$

afin d'éviter les racines multiples. Le polynôme R_1 a les mêmes racines que P, mais pour R_1 ce sont toutes des racines simples.

La méthode de Lagrange prolonge cette idée, en décomposant si possible R_1 en polynômes réels de degrés moindres, auxquels le théorème de Sturm peut s'appliquer séparément. Bien entendu, un degré inférieur offre de nouvelles opportunités, comme la détermination d'une formule exacte pour certaines racines.

2.3 Approximation des racines

De nombreuses méthodes de résolution approchée d'équations numériques, par exemple la méthode de Newton, posent des problèmes de stabilité numérique en présence d'une tangente horizontale. Pour une équation polynômiale, la méthode de Lagrange transforme ce cas problématique en optimisation, puisqu'alors la méthode numérique s'applique séparément à des polynômes de degré strictement moindre et sans racine multiple.

3 Démonstration de la propriété 1

On utilisera les propriétés classiques dans $\mathbb{C}[X]$.

1. Si P n'a que des racines simples, P et P′ n'ont aucune racine commune. Or, dans $\mathbb{C}[X]$, deux polynômes sans racines communes ont un PGCD égal à 1, donc $PGCD(P, P') = 1$.
2. Si P a une racine d'ordre au moins deux, posons $D(X) = \prod_i (X - x_i)^{h(i)-1}$ produit étendu à toutes les racines x_i de P d'ordre $h(i) \geqslant 2$. Dans le cas particulier où x_i est la seule racine de P d'ordre $h(i) \geqslant 2$, D(X) se réduit à $(X - x_i)^{h(i)-1}$
   (a) Les racines communes à P et P′ sont exactement les racines de P d'ordre au moins deux.
   (b) Chaque racine x_i d'ordre $h(i) \geqslant 2$ du polynôme P est alors racine d'ordre $h(i) - 1$ de la dérivée P′.

(c) Il résulte de ces deux propriétés que $P = D \times H$ et $P' = D \times N$, où H et N sont deux polynômes non nuls sans racine commune. Dans $\mathbb{C}[X]$, ces deux polynômes sont donc premiers entre eux.

(d) En résumé $P = D \times H$ et $P' = D \times N$, où H et N sont deux polynômes premiers entre eux, D est donc un PGCD de P et P'.

(e) Enfin, on regroupe les $(X - x_i)^j$ dans D(X) comme on l'avait fait dans P(X) au 1, il résulte de la définition des P_j que

$$D = P_2 P_3^2 \cdots P_q^{q-1} = \prod_{j=2}^{q} P_j^{j-1}.$$