Section hors-programme

L'étude des racines complexes des polynômes à coefficients réels (hors du cas des racines n-ièmes de l'unité) et des factorisations qu'elles permettent ne figure pas au programme de B/L.

4 L'apport du plan complexe

On a vu dans le cours sur les nombres complexes que même lorsqu'un polynôme du second degré à coefficients réels n'admet pas de racine réelle, il est possible d'en déterminer deux racines complexes conjuguées. Ainsi, il est toujours possible de factoriser un polynôme du second degré à coefficients réels sous la forme

$$P(X) = a(X - a_1)(X - a_2),$$

où $a \in \mathbb{R}$ et $a_1, a_2 \in \mathbb{C}$ sont deux nombres non nécessairement distincts et sont soit réels, soit conjugués. On va voir que ce fait n'est pas spécifique aux polynômes du second degré.

On peut définir un polynôme à coefficients dans $\mathbb{C}$ comme une expression de la forme

$$P(X) = \sum_{k=0}^{n} a_k X^k,$$

où $n \in \mathbb{N}$ et où $a_0, \dots, a_n$ sont des nombres complexes. On définit alors la fonction polynomiale associée comme dans le cas réel, c'est-à-dire comme une application $P : \mathbb{C} \to \mathbb{C}$ telle que

$$\forall z \in \mathbb{C}, \quad P(z) := \sum_{k=0}^{n} a_k z^k.$$

On note $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients complexes, $\mathbb{C}[x]$ l'ensemble des fonctions polynomiales à coefficients complexes et on transpose sans mal les définitions et résultats portant sur les opérations polynomiales, la division euclidienne et la factorisation des polynômes au cas complexe.

Le théorème suivant, démontré dans un exercice difficile accompagnant ce chapitre, possède des applications profondes dans de nombreux domaines des mathématiques, et notamment dans la réduction des endomorphismes, sujet que nous aborderons dans le cadre de notre cours d'algèbre linéaire. À ce titre, il est parfois appelé *théorème fondamental de l'algèbre* (voir Zoom page 6).

Théorème 1 (Théorème de d'Alembert-Gauss)**.** Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.

On en déduit (par une récurrence facile sur le degré) que tout polynôme de $\mathbb{C}[X]$ est « complètement factorisable » (c'est-à-dire *scindé*) dans $\mathbb{C}$:

Théorème 2. Si $P \in \mathbb{C}[X]$ est un polynôme non constant, alors il existe $n \in \mathbb{N}^*$, $a \in \mathbb{C}^*$, $z_1, \dots, z_n \in \mathbb{C}$ distincts deux à deux et $m_1, \dots, m_n \in \mathbb{N}^*$ tels que

$$P(X) = a \prod_{k=1}^{n} (X - z_k)^{m_k}. \tag{1}$$

On a alors $\deg(P) = \sum_{k=1}^{n} m_k$, et les racines de P sont $z_1, \dots, z_n$, d'ordres respectifs $m_1, \dots, m_n$. La décomposition du polynôme P sous la forme (1) est unique à ordre des facteurs près.

Exemple. On a vu dans le cours sur les nombres complexes que pour tout $n \in \mathbb{N}^*$, l'équation $z^n = 1$ admet exactement n solutions dans $\mathbb{C}$ (les racines n-ièmes de l'unité). Ainsi, le polynôme $X^n - 1$ admet n racines simples dans $\mathbb{C}$, et on a la factorisation

$$X^n - 1 = \prod_{k=1}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

Plus généralement, si $a \in \mathbb{C}^*$ admet un argument $\theta \in \mathbb{R}$, le polynôme $X^n - a$ admet n racines simples dans $\mathbb{C}$ (comme on l'a vu dans un complément de cours en ligne) et se factorise sous la forme

$$X^n - a = \prod_{k=1}^{n} \left(X - |a|^{\frac{1}{n}} e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)}\right).$$

Le mathématicien, physicien et philosophe Jean le Rond d'Alembert (1717 – 1783), que nous avons croisé dans le cours sur les séries, fut le premier à ressentir la nécessité de démontrer le théorème fondamental de l'algèbre pour trouver une primitive d'une fonction rationnelle. Sa preuve, lacunaire, fut complétée par Gauss dans la première moitié du XIX^e siècle, d'où le nom donné au théorème 1.
*Suite aux travaux de D'alembert sur les dérivées partielles, il fut chargé de la rédaction de la plupart des articles scientifiques de l'*Encyclopédie, *dont il codirigea la composition avec Denis Diderot.*

Dans le cas $a = 0$, il existe toujours n racines n-ièmes de a, mais celles-ci sont confondues et valent 0 : le polynôme X^n admet donc 0 pour unique racine (d'ordre de multiplicité n).

De manière alternative, le théorème de D'Alembert-Gauss peut être exprimé sous la forme suivante : tout polynôme non nul $P \in \mathbb{C}[X]$ admet $\deg(P)$ racines *comptées avec leur ordre de multiplicité* dans $\mathbb{C}$. Examinons les conséquences de ce théorème pour les polynômes à coefficients réels.

Remarquons que l'intérêt (considérable) de ce résultat est essentiellement théorique. En effet, le théorème donne bien l'existence d'une factorisation de la forme (1), mais il ne dit pas comment la trouver (et en particulier comment déterminer les racines $z_1, \dots, z_n$) !

La proposition suivante généralise à un degré quelconque le résultat sur les racines complexes des polynômes de degré 2 à coefficients réels :

Proposition 3 (Racines complexes d'un polynôme de $\mathbb{R}[X]$)**.**
Soit P un polynôme à coefficients **réels** (*i.e.* $P \in \mathbb{R}[X]$). Alors :

- P admet $\deg(P)$ racines dans $\mathbb{C}$ comptées avec leur ordre de multiplicité.
- Si $z \in \mathbb{C} \setminus \mathbb{R}$ est racine de P de multiplicité $k \in \mathbb{N}$, alors $\overline{z}$ l'est aussi.

Démonstration de la proposition 3 — Le premier point est une conséquence du théorème fondamental de l'algèbre puisque $P \in \mathbb{C}[X]$.

Soit à présent $z \in \mathbb{C} \setminus \mathbb{R}$ une racine de P d'ordre de multiplicité $k \in \mathbb{N}$. On a alors

$$\forall i \in [\![0, k-1]\!], \quad P^{(i)}(z) = 0, \quad \text{et } P^{(k)}(z) \neq 0.$$

En passant au conjugué, on obtient

$$\forall i \in [\![0, k-1]\!], \quad \overline{P^{(i)}(z)} = 0, \quad \text{et } \overline{P^{(k)}(z)} \neq 0.$$

Or P et ses dérivées successives sont à coefficients réels, donc pour tout $i \in [\![0, k]\!]$ on a $\overline{P^{(i)}(z)} = P^{(i)}(\overline{z})$. Ainsi, on a :

$$\forall i \in [\![0, k-1]\!], \quad P^{(i)}(\overline{z}) = 0, \quad \text{et } P^{(k)}(\overline{z}) \neq 0,$$

ce qui montre que z est racine de P d'ordre de multiplicité k. □

En effet, si $Q \in \mathbb{R}[X]$ s'écrit

$$Q(X) = \sum_{k=0}^{n} a_k X^k$$

avec les a_k **réels**, alors

$$\overline{Q(z)} = \sum_{k=0}^{n} \overline{a_k z^k} = \sum_{k=0}^{n} a_k \overline{z}^k,$$

donc $\overline{Q(z)} = Q(\overline{z})$.

Exemple. Par exemple, $X^4 + 2X^2 + 1 = (X - i)^2(X + i)^2$ admet exactement deux racines conjuguées, i et $-i$, chacune d'ordre 2.

Exemple. Sans même développer $(X - 1 - i)^3(X - 1 + i)^2$, on sait que ce polynôme n'est pas à coefficients réels puisqu'il admet $1 + i$

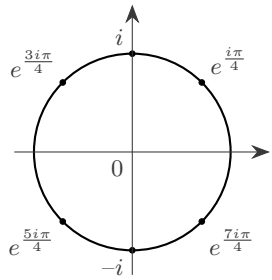
pour racine triple et son conjugué $1-i$ pour racine double, ce qui ne lui permet pas d'être dans $\mathbb{R}[X]$ d'après le deuxième point de la proposition 3.

Exemple. Pour trouver les racines complexes du polynôme $P(X) = X^6 + X^4 + X^2 + 1$, on écrit que pour tout $z \in \mathbb{C} \setminus \{-1, 1\}$ on a

$$P(z) = 1 + z^2 + z^4 + z^6 = \frac{1 - z^8}{1 - z^2},$$

si bien que z est racine de P si et seulement si $z^8 = 1$. Par ailleurs, -1 et 1 ne sont pas racines de P puisque $P(-1) = P(1) = 4$. Ainsi, les six racines de P dans $\mathbb{C}$ sont les racines huitièmes de l'unité différentes de -1 et 1, c'est-à-dire $e^{\frac{i\pi}{4}}$, $e^{\frac{2i\pi}{4}} = i$, $e^{\frac{3i\pi}{4}}$, $e^{\frac{5i\pi}{4}}$, $e^{\frac{6i\pi}{4}} = -i$ et $e^{\frac{7i\pi}{4}}$, qui sont bien deux à deux conjuguées.

On utilise ici la formule donnant la valeur d'une somme géométrique de raison z^2.



Racines (conjuguées) de P

On peut à présent résoudre intégralement la question de la factorisabilité des polynômes à coefficients réels. Pour cela, on remarque tout d'abord que si $a \in \mathbb{C}$, alors le polynôme

$$(X-a)(X-\overline{a}) = X^2 - (a+\overline{a})X + a\overline{a} = X^2 - 2\mathrm{Re}(a) + |a|^2$$

est à coefficients réels. Si $P \in \mathbb{R}[X]$, en décomposant P dans $\mathbb{C}[X]$ sous la forme (1) et en rassemblant deux à deux les facteurs associés à des racines non réelles conjuguées, on obtient donc une écriture de P sous la forme d'un produit de polynômes de $\mathbb{R}[X]$ de degré 1 et de polynômes de $\mathbb{R}[X]$ de degré 2 sans racines réelles. On a donc démontré le théorème suivant :

Théorème 4 (Factorisation des polynômes à coefficients réels)**.** Tout polynôme non constant $P \in \mathbb{R}[X]$ s'écrit comme produit de polynômes de $\mathbb{R}[X]$ de degré 1 et de polynômes de $\mathbb{R}[X]$ de degré 2 à discriminant strictement négatif. Cette écriture est unique à un facteur multiplicatif réel et à l'ordre des facteurs près.

On remarquera que ce théorème ne fait aucune référence aux nombres complexes. Sa démonstration s'appuie pourtant fortement sur le caractère scindé des polynômes de $\mathbb{C}[X]$ (et donc de $\mathbb{R}[X]$) dans $\mathbb{C}$; il s'agit d'un exemple parmi tant d'autres de problème purement réel traité grâce à l'intervention des nombres complexes.

Exemple. Le polynôme $P(X) = X^6 + X^4 + X^2 + 1$ étudié dans l'exemple ci-dessus se factorise dans $\mathbb{C}[X]$ sous la forme

$$P(X) = (X-i)(X+i)(X-e^{\frac{i\pi}{4}})(X-e^{-\frac{i\pi}{4}})(X-e^{\frac{3i\pi}{4}})(X-e^{-\frac{3i\pi}{4}}).$$

En calculant les produits de facteurs correspondant à deux racines

conjuguées (par exemple $(X-i)(X+i) = X^2 - i^2 = X^2+1$), on obtient sa factorisation dans $\mathbb{R}[X]$:

$$P(X) = (X^2+1)(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1).$$

Exemple. On peut montrer que le polynôme

$$P(X) = X^6 - 4X^5 + 6X^4 - 8X^3 + 9X^2 - 4X + 4$$

admet i, $-i$ et 2 pour racines doubles. Ainsi, on a

$$P(X) = (X-i)^2(X+i)^2(X-2)^2 = (X^2+1)^2(X-2)^2.$$

Vérifiez-le à l'aide du critère portant sur les dérivées successives de P !

Achevons notre discussion par l'énoncé d'un théorème permettant de comprendre l'arithmétique des polynômes à coefficients réels.

Définition 5 (Polynôme irréductible)**.** Si $P \in \mathbb{R}[X]$, P est dit *irréductible* (sur $\mathbb{R}$) s'il n'existe pas $A, B \in \mathbb{R}[X]$ non constants tels que $P = AB$.

Un polynôme irréductible est donc un polynôme non décomposable en produit de polynômes de degré strictement inférieur. La notion de polynôme irréductible est l'analogue dans la théorie des polynômes de celle de nombre premier en arithmétique.

On peut définir la notion de *polynôme irréductible sur* $\mathbb{C}$ de la même façon que sur $\mathbb{R}$. Le théorème de d'Alembert-Gauss, ou plus exactement le théorème 2, implique alors que les polynômes irréductibles sur $\mathbb{C}$ sont exactement les polynômes de degré 1 de $\mathbb{C}[X]$.

Exemple 6 (Polynômes de degré 2 irréductibles sur $\mathbb{R}$)**.** On souhaite déterminer les polynômes de degré 2 irréductibles sur $\mathbb{R}$.

Si $P \in \mathbb{R}[X]$ est de degré 2 et si P n'est pas irréductible, il existe $A, B \in \mathbb{R}[X]$ non constants tels que $P = AB$. Mais alors on a forcément $\deg(A) = \deg(B) = 1$, si bien que $A(X)$ s'écrit $a(X-a_1)$ avec $a \in \mathbb{R}^*$ et $a_1 \in \mathbb{R}$, et $B(X)$ s'écrit $b(X-a_2)$ avec $b \in \mathbb{R}^*$ et $a_2 \in \mathbb{R}$. On a donc $P(X) = ab(X-a_1)(X-a_2)$, si bien que P admet deux racines réelles (éventuellement confondues) a_1 et a_2. Le discriminant de P est donc nécessairement positif.

Réciproquement, on a vu que si un polynôme $P \in \mathbb{R}[X]$ de degré 2 est de discriminant positif, alors on peut factoriser P sous la forme $P(X) = a(X-a_1)(X-a_2)$ avec $a \in \mathbb{R}^*$ et $a_1, a_2 \in \mathbb{R}$ éventuellement identiques, si bien que P n'est pas irréductible.

On a donc démontré que les polynômes de degré 2 irréductibles sur $\mathbb{R}$ sont exactement ceux dont le discriminant est strictement négatif.

On déduit de ce résultat et du théorème 4 la classification des polynômes irréductibles de $\mathbb{R}[X]$:

Proposition 7. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Les théorèmes 2 et 4 se réécrivent ainsi de la façon suivante :

Théorème 8 (Théorème fondamental de l'arithmétique dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$)**.** Tout polynôme non constant $P \in \mathbb{R}[X]$ (resp. $\mathbb{C}[X]$) s'écrit comme produit de polynômes irréductibles de $\mathbb{R}[X]$ (resp. de $\mathbb{C}[X]$), et cette écriture est unique à un facteur multiplicatif et à l'ordre des facteurs près.

À des fins de comparaison, rappelons le résultat connu sous le nom de *théorème fondamental de l'arithmétique* (dans $\mathbb{Z}$) : tout nombre entier positif s'écrit comme un produit de nombres premiers, et cette écriture est unique à l'ordre des facteurs près.

Le théorème fondamental de l'algèbre

La présentation formelle adoptée dans ce cours est l'aboutissement d'une longue évolution dans l'approche des polynômes par les mathématiciens.

Initialement introduits par les mathématiciens grecs et arabes pour résoudre des équations issues de la géométrie mobilisant des aires et des volumes, et donc des quantités réelles mises au carré ou au cube, les polynômes furent longtemps étudiés en tant que fonctions polynomiales. Lors du développement de l'algèbre générale, les polynômes s'affranchirent peu à peu de leur aspect analytique. Les polynômes formels prirent ainsi une place fondamentale en algèbre linéaire, mais aussi dans la théorie des extensions de corps, qui permit de résoudre par des méthodes algébriques des problèmes géométriques millénaires de constructibilité des nombres réels à la règle et au compas comme la quadrature du cercle et la duplication du cube.

On comprend alors mieux le nom un peu pompeux de « théorème fondamental de l'algèbre » donné au théorème de d'Alembert-Gauss, pierre angulaire de la théorie des polynômes à coefficients réels ou complexes. Il a d'ailleurs été dit que c'est l'existence de ce résultat qui a achevé de faire reconnaître l'utilité et la légitimité des nombres complexes à la communauté mathématique du XIX$^{\text{e}}$ siècle !

Signalons au passage un fait curieux au sujet de ce grand théorème d'algèbre : parmi les dizaines de démonstrations de ce résultat proposées au fil des siècles, aucune n'est parvenue à se passer du recours à l'analyse, qu'il s'agisse du théorème des valeurs intermédiaires assurant l'existence de racines pour les polynômes à coefficients réels de degré impair, du théorème de Bolzano-Weierstrass (voir l'exercice 32) ou d'outils plus sophistiqués...