Chapitre 13

Polynômes et fractions rationnelles

13.1 Introduction historique

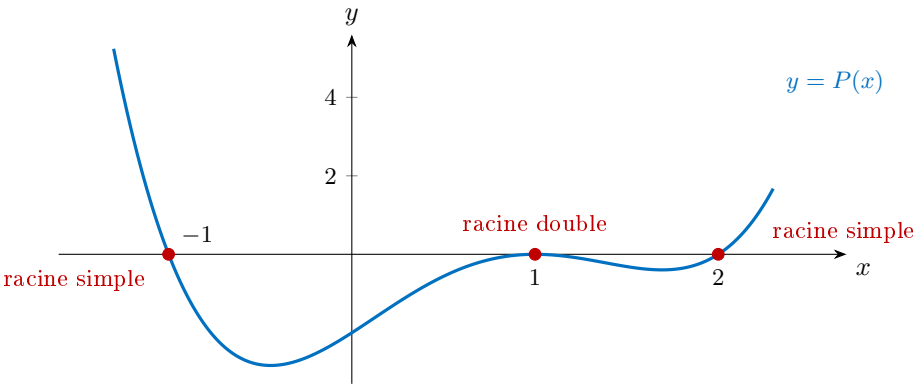
> *Scachés donc qu'en chasque Equation, autant que la quantité inconnue a de dimensions, autant peut il y auoir de diuerses racines, c'est à dire de valeurs de cete quantité.*
>
> René Descartes - *La Géométrie*, livre III, 1637 (*Œuvres*, éd. Adam et Tannery, t. VI, p. 444)

13.1.1 Des équations aux polynômes

Vers 820, le traité d'**al-Khwârizmî** sur « le calcul par la restauration et la comparaison » (*al-jabr wa-l-muqâbala*) résout les équations du second degré par des règles rédigées en mots ; le mot *algèbre* vient de son titre. En 1545, l'*Ars magna* de **Cardan** publie la résolution du troisième degré, due à del Ferro et Tartaglia, et celle du quatrième, due à Ferrari. En 1591, **François Viète** désigne par des lettres les inconnues et les paramètres, ce qui permet d'écrire une équation générale ; il relie les coefficients aux racines, relations qu'**Albert Girard** énonce en toute généralité en 1629, en affirmant qu'une équation de degré n a n racines. Descartes le redit en 1637, dans le passage cité ci-dessus. Il faut attendre **d'Alembert** (1746), puis **Gauss** (1799) et **Argand** (1814), pour une démonstration de ce « théorème fondamental de l'algèbre ». Enfin, en 1824, **Abel** montre qu'aucune formule par radicaux ne résout l'équation générale du cinquième degré, et **Galois** explique, vers 1830, quelles équations peuvent l'être. Le chapitre étudie ces objets pour eux-mêmes : un polynôme n'est plus une fonction, mais une suite finie de coefficients, que l'on peut additionner, multiplier et diviser comme des entiers.

13.1.2 Ce que voit la courbe

La courbe de $P(x) = (x+1)(x-1)^2(x-2) = x^4 - 3x^3 + x^2 + 3x - 2$ coupe l'axe des abscisses en -1 et en 2, mais elle est seulement tangente à cet axe en 1. Le facteur $(x-1)^2$ en est la cause : 1 est une racine « double », et P ne change pas de signe en la traversant. La section 13.5 traduira cette observation par la dérivée : 1 est racine de P et de P', mais -1 et 2 ne sont racines que de P.



13.2 L'anneau $\mathbb{K}[X]$

Dans tout le chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Les seules propriétés de $\mathbb{K}$ utilisées sont celles d'un corps commutatif (chapitre 11), sauf aux sections 13.7 et 13.10, propres à $\mathbb{R}$ et à $\mathbb{C}$, et sauf lorsqu'on divise par un entier $k!$, ce qui est permis dans $\mathbb{R}$ et dans $\mathbb{C}$.

13.2.1 Construction

Au lycée, un polynôme était une fonction $x \mapsto a_0 + a_1 x + \cdots + a_n x^n$. On veut ici un objet défini par ses seuls coefficients, sur lequel on puisse calculer sans évaluer : c'est une suite qui s'arrête.

Définition : Un **polynôme** à coefficients dans $\mathbb{K}$ est une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang ; les a_k sont ses **coefficients**. L'ensemble des polynômes est noté $\mathbb{K}[X]$. Deux polynômes sont égaux s'ils ont les mêmes coefficients. Pour $P = (a_k)$ et $Q = (b_k)$ dans $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on pose

$$P + Q = (a_k + b_k)_{k\in\mathbb{N}}, \qquad \lambda P = (\lambda a_k)_{k\in\mathbb{N}}, \qquad PQ = (c_n)_{n\in\mathbb{N}} \quad \text{avec} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Ces suites sont encore nulles à partir d'un certain rang : si $a_k = 0$ pour $k > p$ et $b_k = 0$ pour $k > q$, alors $c_n = 0$ pour $n > p+q$, car chaque terme $a_k b_{n-k}$ a un indice $k > p$ ou un indice $n-k > q$. Le coefficient c_n rassemble tous les produits $a_i b_j$ avec $i + j = n$, comme on les obtient en développant au lycée.

	a_0	a_1	a_2	a_3
b_0	a_0b_0	a_1b_0	a_2b_0	a_3b_0
b_1	a_0b_1	a_1b_1	a_2b_1	a_3b_1
b_2	a_0b_2	a_1b_2	a_2b_2	a_3b_2

les cases d'une même antidiagonale ont la même somme d'indices $i + j = n$; la case colorée donne $c_2 = a_0b_2 + a_1b_1 + a_2b_0$

Chaque coefficient du produit est la somme d'une antidiagonale du tableau des $a_i b_j$: c'est exactement ce que fait le développement, une fois les termes regroupés par degré.

Proposition 1 : Muni de ces lois, $(\mathbb{K}[X], +, \times)$ est un anneau commutatif, dont le neutre multiplicatif est la suite $(1, 0, 0, \dots)$. L'application $\lambda \mapsto (\lambda, 0, 0, \dots)$ est un morphisme d'anneaux injectif de $\mathbb{K}$ dans $\mathbb{K}[X]$.

∘ Démonstration :

▷ *Addition.* Les propriétés de $(\mathbb{K}, +)$ se transmettent terme à terme : $(\mathbb{K}[X], +)$ est un groupe abélien, de neutre la suite nulle, l'opposé de (a_k) étant $(-a_k)$.

▷ *Multiplication.* La commutativité vient du changement d'indice $k \mapsto n-k$ dans c_n. Pour l'associativité, le coefficient d'indice n de $(PQ)R$, avec $R = (d_k)$, vaut

$$\sum_{m=0}^{n} \Big(\sum_{i+j=m} a_i b_j \Big) d_{n-m} = \sum_{i+j+\ell=n} a_i b_j d_\ell,$$

somme sur les triplets d'entiers naturels de somme n, et l'on obtient la même somme pour $P(QR)$: c'est une sommation par paquets du chapitre 3. La distributivité vient de l'égalité

$$\sum_{k=0}^{n} a_k (b_{n-k} + d_{n-k}) = \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k d_{n-k}.$$

Enfin, si $E = (1, 0, 0, \dots)$, le coefficient d'indice n de EP est $1 \times a_n$, donc $EP = P$.

▷ *Constantes.* On vérifie directement, avec la définition du produit, que

$$(\lambda + \mu, 0, \dots) = (\lambda, 0, \dots) + (\mu, 0, \dots) \qquad \text{et} \qquad (\lambda\mu, 0, \dots) = (\lambda, 0, \dots)(\mu, 0, \dots),$$

et l'application est évidemment injective. □

On identifie désormais le scalaire λ au **polynôme constant** $(\lambda, 0, 0, \dots)$, ce qui fait de $\mathbb{K}$ un sous-anneau de $\mathbb{K}[X]$; le produit λP défini plus haut est alors le produit des polynômes λ et P. On note X le polynôme $(0, 1, 0, 0, \dots)$, appelé l'**indéterminée**.

Proposition 2 : Pour tout $k \in \mathbb{N}$, X^k est la suite dont le seul coefficient non nul est celui d'indice k, égal à 1. Tout polynôme $P = (a_k)$ nul au-delà du rang n s'écrit donc de façon unique

$$P = \sum_{k=0}^{n} a_k X^k, \qquad \text{que l'on note aussi} \qquad \sum_{k=0}^{+\infty} a_k X^k,$$

la seconde écriture étant une somme finie, puisque presque tous ses termes sont nuls.

∘ Démonstration : Par récurrence : $X^0 = 1$, et si X^k a pour seul coefficient non nul 1 en position k, dans le coefficient d'indice n de $X^{k+1} = X^k \times X$, seul le produit des coefficients d'indices k et 1 peut être non nul : ce coefficient vaut 1 si $n = k+1$, et 0 sinon. Le polynôme $\sum a_k X^k$ a donc pour coefficient d'indice k le nombre a_k, ce qui donne l'existence, et l'unicité vient de la définition de l'égalité de deux suites. □

Remarque : L'unicité de l'écriture est ce que l'on appelle souvent « identifier les coefficients » : si $\sum a_k X^k = \sum b_k X^k$, alors $a_k = b_k$ pour tout k. Elle est vraie par définition ; pour les fonctions polynomiales, c'est un théorème, qui sera établi à la section 13.4. C'est l'intérêt de la construction : la lettre X n'est pas un nombre que l'on aurait oublié de préciser, mais un objet nouveau.

13.2.2 Degré

Définition : Soit $P = \sum a_k X^k$ un polynôme non nul. Son **degré** est le plus grand entier n tel que $a_n \neq 0$, noté $\deg P$; le coefficient a_n est son **coefficient dominant**, et P est **unitaire** si ce coefficient vaut 1. Par convention, $\deg 0 = -\infty$. Pour $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus n.

Avec la convention $-\infty + n = -\infty$ et $-\infty < n$ pour tout entier n, les règles suivantes valent sans exception.

Proposition 3 : Soit P et Q deux polynômes.

(i) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$, avec égalité si $\deg P \neq \deg Q$.

(ii) $\deg(PQ) = \deg P + \deg Q$, et si P et Q sont non nuls, le coefficient dominant de PQ est le produit de ceux de P et de Q.

∘ Démonstration :

▷ *(i)* Si $k > \max(\deg P, \deg Q)$, les coefficients d'indice k de P et de Q sont nuls, donc aussi celui de $P+Q$. Si par exemple $\deg P > \deg Q$, le coefficient d'indice $\deg P$ de $P+Q$ est celui de P, qui est non nul.

▷ *(ii)* Si l'un des polynômes est nul, les deux membres valent $-\infty$. Sinon, soit $p = \deg P$ et $q = \deg Q$. On a vu après la définition du produit que $c_n = 0$ pour $n > p+q$; et dans $c_{p+q} = \sum a_k b_{p+q-k}$, seul le terme $k = p$ peut être non nul, donc $c_{p+q} = a_p b_q \neq 0$, car $\mathbb{K}$ est intègre. □

Théorème 1 : Intégrité et inversibles de $\mathbb{K}[X]$:
L'anneau $\mathbb{K}[X]$ est **intègre** : si $PQ = 0$, alors $P = 0$ ou $Q = 0$. Ses inversibles sont les **constantes non nulles** : $\mathbb{K}[X]^\times = \mathbb{K}^*$.

∘ Démonstration :

▷ *Intégrité.* Si P et Q sont non nuls, $\deg(PQ) = \deg P + \deg Q \geqslant 0$, donc $PQ \neq 0$. L'anneau $\mathbb{K}[X]$ est commutatif et non nul, il est donc intègre au sens du chapitre 11.

▷ *Inversibles.* Toute constante non nulle λ a pour inverse λ^{-1}. Réciproquement, si $PQ = 1$, alors $\deg P + \deg Q = 0$, ces deux degrés étant positifs car P et Q sont non nuls ; donc $\deg P = 0$. □

Remarques :

- L'erreur la plus répandue est de croire que $\deg(P+Q) = \max(\deg P, \deg Q)$ dans tous les cas : pour $P = X^2 + X$ et $Q = -X^2 + 1$, on a $P + Q = X + 1$, de degré 1. Les termes dominants peuvent se compenser.
- L'ensemble $\mathbb{K}_n[X]$ est stable par addition et par multiplication par un scalaire, mais pas par produit : $X^n \times X^n$ est de degré $2n$. Le chapitre 14 dira que c'est un espace vectoriel.
- Comme $\mathbb{Z}$, l'anneau $\mathbb{K}[X]$ est intègre sans être un corps : X n'est pas inversible. C'est cette ressemblance qui va permettre d'y reproduire l'arithmétique du chapitre 12, les constantes non nulles jouant le rôle de ± 1.

13.2.3 Composition

Définition : Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes. La **composée** de P et Q est le polynôme $P \circ Q = \sum_{k=0}^{n} a_k Q^k$, que l'on note aussi $P(Q)$.

Proposition 4 : Si Q n'est pas constant, $\deg(P \circ Q) = \deg P \times \deg Q$.

∘ Démonstration : Si $P = 0$, les deux membres valent $-\infty$. Sinon, soit $n = \deg P$. Par la proposition 3, $\deg(a_k Q^k) \leqslant k \deg Q$, avec égalité pour $k = n$, puisque $a_n \neq 0$. Comme $\deg Q \geqslant 1$, le terme $a_n Q^n$ est de degré strictement plus grand que tous les autres, et le point (i) de la proposition 3 donne $\deg(P \circ Q) = n \deg Q$. □

Exemple : Avec $P = X^2 + 1$ et $Q = X - 1$, on obtient $P \circ Q = (X-1)^2 + 1 = X^2 - 2X + 2$, mais $Q \circ P = X^2$. La composition n'est pas commutative. En revanche, $P(X) = P \circ X$: la notation $P(X)$ désigne simplement P.

13.3 Divisibilité et division euclidienne

13.3.1 Divisibilité

Définition : Soit A et B deux polynômes. On dit que B **divise** A, et l'on note $B \mid A$, s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$; on dit aussi que B est un **diviseur** de A, ou que A est un **multiple** de B.

Les règles de la proposition 1 du chapitre 12 se transposent mot pour mot : la divisibilité est réflexive et transitive, et un diviseur commun de A et B divise $AU + BV$ pour tous polynômes U et V. Le degré remplace la valeur absolue : si $B \mid A$ et $A \neq 0$, alors $\deg B \leqslant \deg A$, puisque $A = BQ$ avec $Q \neq 0$.

Proposition 5 : *(Polynômes associés.)* Soit A et B deux polynômes. On a $A \mid B$ et $B \mid A$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $B = \lambda A$. On dit alors que A et B sont **associés**. Tout polynôme non nul est associé à un unique polynôme unitaire.

∘ Démonstration : Si $B = \lambda A$, alors $A = \lambda^{-1} B$. Réciproquement, si $A = 0$, alors B, multiple de A, est nul. Sinon, $B = AU$ et $A = BV$ donnent $A = AUV$, donc $A(1 - UV) = 0$, puis $UV = 1$ par intégrité : U est une constante non nulle par le théorème 1. Enfin, si $A \neq 0$ a pour coefficient dominant a, les associés unitaires de A sont les λA avec $\lambda a = 1$: il n'y en a qu'un, $a^{-1} A$. □

Le choix d'un polynôme unitaire parmi les associés joue le rôle du choix d'un entier positif parmi $\pm n$: c'est ainsi que l'on rendra le PGCD unique à la section 13.6.

13.3.2 Division euclidienne

Théorème 2 : Division euclidienne :
Soit A et B deux polynômes, avec $B \neq 0$. Il existe un unique couple (Q, R) de polynômes tel que

$$A = BQ + R \qquad \text{et} \qquad \deg R < \deg B.$$

Le polynôme Q est le **quotient**, et R le **reste**, de la division euclidienne de A par B.

∘ Démonstration :

▷ *Existence.* On note $m = \deg B$ et b le coefficient dominant de B, et l'on raisonne par récurrence forte sur le degré de A. Si $\deg A < m$, le couple $(0, A)$ convient. Sinon, soit $n = \deg A \geqslant m$ et a le coefficient dominant de A. Le polynôme

$$A_1 = A - \frac{a}{b} X^{n-m} B$$

est de degré strictement inférieur à n, puisque les termes de degré n se compensent. Par hypothèse de récurrence, $A_1 = BQ_1 + R$ avec $\deg R < m$, et $A = B\big(Q_1 + \frac{a}{b}X^{n-m}\big) + R$.

▷ *Unicité.* Si $A = BQ + R = BQ' + R'$ avec $\deg R, \deg R' < m$, alors $B(Q - Q') = R' - R$. Le membre de droite est de degré strictement inférieur à m, alors que le membre de gauche est de degré $m + \deg(Q - Q')$: il faut $Q - Q' = 0$, puis $R = R'$. □

La démonstration d'existence est un algorithme : on retranche à chaque étape le multiple de B qui fait disparaître le terme dominant. Le calcul se dispose comme une division d'entiers, dans une « potence ».

♡ **Méthode : Pour effectuer la division euclidienne de A par B :**

- ▶ On écrit A et B selon les puissances décroissantes, en laissant une place pour chaque coefficient nul de A.
- ▶ On divise le terme dominant du dividende courant par celui de B : on obtient un terme du quotient.
- ▶ On retranche au dividende le produit de B par ce terme, et l'on recommence avec la différence, tant que son degré est au moins celui de B.

Le dernier dividende obtenu est le reste.

$$\begin{array}{rrrrr|l}
X^4 & +2X^3 & & -X & +3 & X^2+X+1 \\
\cline{6-6}
-X^4 & -X^3 & -X^2 & & & X^2+X-2 \\
\cline{1-3}
 & X^3 & -X^2 & -X & +3 & \\
 & -X^3 & -X^2 & -X & & \\
\cline{2-4}
 & & -2X^2 & -2X & +3 & \\
 & & +2X^2 & +2X & +2 & \\
\cline{3-5}
 & & & & 5 &
\end{array}$$

Chaque colonne correspond à une puissance de X. Les lignes orange sont les opposés des multiples X^2B, XB et $-2B$ que l'on retranche : les termes X^2, X et -2 forment le quotient, et le calcul s'arrête sur un reste constant, de degré $0 < 2$. On a donc

$$X^4 + 2X^3 - X + 3 = (X^2 + X + 1)(X^2 + X - 2) + 5,$$

ce que l'on vérifie en développant.

Remarque : L'algorithme divise par le coefficient dominant b de B. Si A et B sont à coefficients entiers et B unitaire, le quotient et le reste sont donc encore à coefficients entiers ; ce n'est plus vrai en général, comme le montre la division de X par $2X$, de quotient $\frac{1}{2}$. C'est une raison de travailler sur un corps $\mathbb{K}$.

13.4 Fonctions polynomiales et racines

13.4.1 Évaluation

Définition : Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme et $x \in \mathbb{K}$. On note $P(x) = \sum_{k=0}^{n} a_k x^k$ la **valeur** de P en x, et l'on appelle **fonction polynomiale** associée à P l'application $\widetilde{P} : x \mapsto P(x)$ de $\mathbb{K}$ dans $\mathbb{K}$.

Proposition 6 : Pour tous polynômes P et Q, tous scalaires λ, μ, et tout $x \in \mathbb{K}$:

$$(\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x), \qquad (PQ)(x) = P(x)\,Q(x), \qquad (P \circ Q)(x) = P\big(Q(x)\big).$$

∘ Démonstration : La première égalité découle de la définition. Pour la deuxième, avec $P = \sum a_i X^i$ et $Q = \sum b_j X^j$, le développement d'un produit de deux sommes finies dans $\mathbb{K}$ (chapitre 3), regroupé selon la valeur de $i + j$, donne

$$P(x)\,Q(x) = \sum_{i,j} a_i b_j x^{i+j} = \sum_{n} \Big(\sum_{i+j=n} a_i b_j \Big) x^n = (PQ)(x).$$

On en déduit par récurrence que $Q^k(x) = Q(x)^k$, puis, par linéarité,

$$(P \circ Q)(x) = \sum_{k} a_k Q(x)^k = P\big(Q(x)\big).$$

□

Dans le langage du chapitre 11, l'application $P \mapsto P(x)$ est un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}$. Pour calculer $P(x)$, il est maladroit de calculer séparément chaque puissance x^k ; on factorise plutôt de proche en proche :

$$a_3x^3 + a_2x^2 + a_1x + a_0 = \big((a_3x + a_2)x + a_1\big)x + a_0.$$

♡ **Méthode : Schéma de Horner, pour calculer $P(a)$ avec $P = \sum_{k=0}^{n} a_k X^k$:**

- On pose $b_{n-1} = a_n$, puis, de proche en proche, $b_{k-1} = a_k + a\,b_k$ pour $k = n-1, \dots, 1$.
- La dernière étape donne la valeur : $P(a) = a_0 + a\,b_0$.

On dispose les calculs sur trois lignes : les coefficients de P, les produits par a, et les sommes. Le calcul demande n multiplications, au lieu d'environ $\frac{n^2}{2}$ par le calcul direct des puissances.

Exemple : Pour $P = 2X^3 - 3X^2 + X - 5$ et $a = 2$:

coefficients de P	2	-3	1	-5
produits par 2		4	2	6
sommes	2	1	3	1

On lit $P(2) = 1$. Les sommes intermédiaires 2, 1, 3 ne sont pas des auxiliaires sans signification : la proposition suivante montre que ce sont les coefficients du quotient de P par $X - 2$, soit $P = (X-2)(2X^2 + X + 3) + 1$.

13.4.2 Racines

Définition : Soit $P \in \mathbb{K}[X]$. Un élément a de $\mathbb{K}$ est une **racine**, ou un **zéro**, de P si $P(a) = 0$.

Proposition 7 : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de P par $X - a$ est la constante $P(a)$. En particulier, a est racine de P si et seulement si $X - a$ divise P.

∘ Démonstration : La division euclidienne donne $P = (X-a)Q + R$ avec $\deg R < 1$: R est une constante r. En évaluant en a par la proposition 6, $P(a) = 0 \times Q(a) + r = r$. □

C'est la proposition 19 du chapitre 4, démontrée alors pour les fonctions polynomiales complexes ; le schéma de Horner en donne le quotient, puisque l'identité $P = (X-a)\sum b_k X^k + P(a)$ se vérifie en identifiant les coefficients.

Proposition 8 : Soit $P \in \mathbb{K}[X]$ et $a_1, \dots, a_r$ des racines de P deux à deux distinctes. Alors $(X-a_1)\cdots(X-a_r)$ divise P.

∘ Démonstration : Par récurrence sur r, le cas $r = 1$ étant la proposition 7. Si le résultat est vrai pour $r-1$ racines, on écrit

$$P = (X-a_1)\cdots(X-a_{r-1})\,Q.$$

En évaluant en a_r, on obtient $0 = (a_r-a_1)\cdots(a_r-a_{r-1})\,Q(a_r)$, et les facteurs $a_r - a_i$ sont non nuls ; comme $\mathbb{K}$ est intègre, $Q(a_r) = 0$, et $X - a_r$ divise Q. □

Théorème 3 : Nombre de racines :
Un polynôme non nul de degré n possède **au plus n racines** distinctes. En conséquence :

- un polynôme de $\mathbb{K}_n[X]$ qui a au moins $n+1$ racines est nul ;
- deux polynômes de $\mathbb{K}_n[X]$ qui prennent les mêmes valeurs en $n+1$ points distincts sont égaux ;
- deux polynômes dont les fonctions polynomiales associées sont égales sont égaux : $\widetilde{P} = \widetilde{Q} \implies P = Q$.

∘ Démonstration : Si $P \neq 0$ a r racines distinctes, la proposition 8 donne $P = (X-a_1)\cdots(X-a_r)\,Q$ avec $Q \neq 0$, donc $n = r + \deg Q \geqslant r$. Le premier point en découle par contraposée. Pour le deuxième, on l'applique à $P - Q$, qui est de degré au plus n. Pour le troisième, $P - Q$ a alors une infinité de racines, puisque $\mathbb{K}$ est infini : il est nul. □

Remarques :

- Le dernier point justifie l'abus courant qui confond P et $\widetilde{P}$, et donc la notation $P(x)$; il établit aussi le principe d'identification des coefficients des fonctions polynomiales, utilisé depuis le lycée. Il repose sur le fait que $\mathbb{K}$ est infini : sur l'ensemble $\{0,1\}$, le polynôme non nul $X^2 - X$ s'annule partout.
- Le théorème est faux dans un anneau qui n'est pas intègre. Dans l'anneau $\mathcal{F}(\mathbb{R},\mathbb{R})$ du chapitre 11, l'équation $f^2 = f$ a une infinité de solutions : toutes les fonctions indicatrices.

13.4.3 Multiplicité

Un polynôme non nul P n'est divisible que par un nombre fini de puissances de $X - a$, puisque $\deg(X-a)^m = m$ ne peut dépasser $\deg P$.

Définition : Soit P un polynôme non nul et $a \in \mathbb{K}$. La **multiplicité** de a dans P est le plus grand entier m tel que $(X-a)^m$ divise P. Si $m = 1$, on dit que a est racine **simple** ; si $m \geqslant 2$, racine **multiple** (double, triple, etc.). La multiplicité est nulle si et seulement si a n'est pas racine de P.

Proposition 9 : Soit $P \neq 0$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors a est de multiplicité m dans P si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ et $Q(a) \neq 0$.

∘ Démonstration : Si la multiplicité vaut m, on écrit $P = (X-a)^m Q$. Si l'on avait $Q(a) = 0$, la proposition 7 donnerait $Q = (X-a)Q_1$, et $(X-a)^{m+1}$ diviserait P. Réciproquement, si $P = (X-a)^m Q$ avec $Q(a) \neq 0$ et si $P = (X-a)^{m+1}S$, la simplification par $(X-a)^m$, permise dans l'anneau intègre $\mathbb{K}[X]$, donne $Q = (X-a)S$, d'où $Q(a) = 0$: c'est absurde. □

Proposition 10 : Soit $P \neq 0$, et $a_1, \dots, a_r$ des éléments deux à deux distincts de $\mathbb{K}$, de multiplicités au moins $m_1, \dots, m_r$ dans P. Alors $(X-a_1)^{m_1}\cdots(X-a_r)^{m_r}$ divise P, et $m_1 + \cdots + m_r \leqslant \deg P$.

∘ Démonstration :

▷ *Un lemme.* Si $b \neq a$ et si $(X-b)^k$ divise $(X-a)^m Q$, alors $(X-b)^k$ divise Q. On le montre par récurrence sur k, le cas $k=0$ étant clair. En évaluant en b l'égalité $(X-a)^m Q = (X-b)^k S$, avec $k \geqslant 1$, on obtient $(b-a)^m Q(b) = 0$, donc $Q(b) = 0$ et $Q = (X-b)Q_1$. On simplifie par $X-b$: $(X-b)^{k-1}$ divise $(X-a)^m Q_1$, donc Q_1 par hypothèse de récurrence, et $(X-b)^k$ divise Q.

▷ *Le résultat.* Par récurrence sur r : on écrit

$$P = (X-a_1)^{m_1} \cdots (X-a_{r-1})^{m_{r-1}} Q.$$

Comme $(X-a_r)^{m_r}$ divise P, le lemme, appliqué $r-1$ fois, montre qu'il divise Q. L'inégalité vient de la comparaison des degrés. □

Définition : Un polynôme non constant P est **scindé** sur $\mathbb{K}$ s'il s'écrit $P = \lambda(X-x_1)\cdots(X-x_n)$, avec $\lambda \in \mathbb{K}^*$ et $x_1, \ldots, x_n \in \mathbb{K}$, non nécessairement distincts.

Dans ce cas, λ est le coefficient dominant et n le degré de P. Chaque racine a figure dans la liste $(x_1, \ldots, x_n)$ autant de fois que sa multiplicité, par la proposition 9 et la proposition 10 : on dit que $x_1, \ldots, x_n$ sont les racines de P *comptées avec leur multiplicité*, et la somme des multiplicités est alors égale au degré. Le polynôme X^2+1 n'est pas scindé sur $\mathbb{R}$, mais il l'est sur $\mathbb{C}$: $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$.

13.4.4 Relations entre coefficients et racines

Pour $x_1, \ldots, x_n \in \mathbb{K}$ et $k \in [\![1, n]\!]$, on note

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k},$$

la somme de tous les produits de k des x_i d'indices distincts ; on l'appelle la k-ième **fonction symétrique élémentaire** des x_i. Ainsi $\sigma_1 = x_1 + \cdots + x_n$ et $\sigma_n = x_1 \cdots x_n$.

Théorème 4 : Relations entre coefficients et racines :
Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ un polynôme scindé de degré n, de racines $x_1, \ldots, x_n$ comptées avec leur multiplicité. Alors, pour tout $k \in [\![1, n]\!]$,

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, \quad \text{en particulier} \quad x_1 + \cdots + x_n = -\frac{a_{n-1}}{a_n}, \quad x_1 \cdots x_n = (-1)^n \frac{a_0}{a_n}.$$

∘ Démonstration : On montre par récurrence sur n que $(X-x_1)\cdots(X-x_n) = \sum_{k=0}^{n} (-1)^k \sigma_k X^{n-k}$, avec $\sigma_0 = 1$. C'est clair pour $n=1$. Si c'est vrai pour n, on note σ'_k les fonctions symétriques de $x_1, \ldots, x_{n+1}$: un produit de k d'entre eux contient x_{n+1} ou non, d'où $\sigma'_k = \sigma_k + x_{n+1}\sigma_{k-1}$, avec $\sigma_{n+1} = 0$. En multipliant par $X - x_{n+1}$, le coefficient de X^{n+1-k} vaut

$$(-1)^k \sigma_k - x_{n+1}(-1)^{k-1}\sigma_{k-1} = (-1)^k \sigma'_k.$$

Il reste à comparer avec $P = a_n(X-x_1)\cdots(X-x_n)$: le coefficient de X^{n-k} vaut $a_{n-k} = a_n(-1)^k\sigma_k$. □

Exemples :

- Pour $n=2$, on retrouve le théorème 4 du chapitre 4 : les racines de aX^2+bX+c ont pour somme $-\frac{b}{a}$ et pour produit $\frac{c}{a}$.
- On cherche les racines de $P = X^3 - 6X^2 + 11X - 6$, sachant qu'elles sont en progression arithmétique : $x_1 = r-d$, $x_2 = r$, $x_3 = r+d$. La somme vaut $3r = 6$, donc $r = 2$ est racine, ce que l'on vérifie : $P(2) = 8 - 24 + 22 - 6 = 0$. La division par $X-2$ donne $X^2 - 4X + 3$, de racines 1 et 3 : $P = (X-1)(X-2)(X-3)$. Une relation entre les racines, jointe à une seule des formules, a suffi.
- Si x_1, x_2, x_3 sont les racines complexes de $X^3 + pX + q$, alors $\sigma_1 = 0$ et $\sigma_2 = p$, donc $x_1^2 + x_2^2 + x_3^2 = \sigma_1^2 - 2\sigma_2 = -2p$, sans qu'il soit besoin de connaître les racines. Pour $p > 0$, cette somme est strictement négative : les trois racines ne sont pas toutes réelles.

Remarque : Les relations ne servent pas à calculer les racines : pour $n = 3$, elles forment un système de trois équations aussi difficile que l'équation elle-même. Elles servent à calculer des expressions symétriques des racines, comme la somme des carrés, ou à exploiter une information supplémentaire, comme dans le deuxième exemple. Le troisième exemple suppose que $X^3 + pX + q$ est scindé sur $\mathbb{C}$; c'est le théorème de d'Alembert-Gauss, énoncé à la section 13.7.

13.5 Dérivation

13.5.1 Polynôme dérivé

Définition : Le **polynôme dérivé** de $P = \sum_{k=0}^{n} a_k X^k$ est $P' = \sum_{k=1}^{n} k\, a_k X^{k-1}$. On définit par récurrence les dérivées successives : $P^{(0)} = P$ et $P^{(k+1)} = \left(P^{(k)}\right)'$.

Cette définition est purement algébrique : aucune limite n'intervient. Pour $\mathbb{K} = \mathbb{R}$, elle coïncide avec la dérivée du chapitre 5 : la fonction polynomiale associée à P' est la dérivée de $\widetilde{P}$, puisque la dérivée de $x \mapsto x^k$ est $x \mapsto kx^{k-1}$.

Proposition 11 : Pour tous polynômes P et Q et tous scalaires λ et μ :

(i) $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$ et $(PQ)' = P'Q + PQ'$;

(ii) $(P \circ Q)' = Q' \times (P' \circ Q)$;

(iii) si $\deg P \geqslant 1$, alors $\deg P' = \deg P - 1$; et $P' = 0$ si et seulement si P est constant.

∘ Démonstration :

▷ *(i)* La linéarité se lit sur les coefficients. Pour le produit, les deux membres sont linéaires en P et en Q séparément ; il suffit donc de vérifier l'égalité pour $P = X^i$ et $Q = X^j$, ce qui donne $(i+j)X^{i+j-1}$ de part et d'autre.

▷ *(ii)* Par récurrence avec (i), $(Q^k)' = kQ'Q^{k-1}$ pour tout $k \geqslant 1$; par linéarité,

$$(P \circ Q)' = \sum_{k \geqslant 1} a_k\, kQ'Q^{k-1} = Q' \times (P' \circ Q).$$

▷ *(iii)* Si P est de degré $n \geqslant 1$ et de coefficient dominant a_n, le coefficient de X^{n-1} dans P' est $na_n \neq 0$, puisque $n \neq 0$ dans $\mathbb{K}$. Un polynôme constant a une dérivée nulle, et un polynôme non constant une dérivée non nulle, de degré $\deg P - 1 \geqslant 0$. □

Théorème 5 : Formule de Leibniz :
Pour tous polynômes P et Q et tout $n \in \mathbb{N}$,

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

∘ Démonstration : C'est la démonstration du théorème 9 du chapitre 9, qui n'utilise que la linéarité de la dérivation et la règle du produit, établies ici par la proposition 11. Par récurrence sur n : si la formule est vraie au rang n, on dérive chaque terme, puis on réindexe la somme des termes $P^{(k+1)}Q^{(n-k)}$, et la formule de Pascal $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ (chapitre 3) donne le rang $n+1$. □

13.5.2 Formule de Taylor

Théorème 6 : Formule de Taylor pour les polynômes :
Soit P un polynôme de degré au plus n, et $a \in \mathbb{K}$. Alors

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X - a)^k.$$

∘ Démonstration :

▷ *Écriture selon les puissances de $X-a$.* On écrit $X=(X-a)+a$, et l'on développe chaque puissance $X^j=\big((X-a)+a\big)^j$ par la formule du binôme (chapitre 11, théorème 3). En regroupant, on obtient des scalaires $b_0,\dots,b_n$ tels que

$$P=\sum_{k=0}^{n} b_k(X-a)^k.$$

▷ *Identification des b_k.* Par récurrence, la dérivée j-ième de $(X-a)^k$ vaut $\frac{k!}{(k-j)!}(X-a)^{k-j}$ si $j\leqslant k$, et 0 si $j>k$. Elle s'annule donc en a, sauf si $j=k$, où elle vaut $k!$. En dérivant j fois l'écriture précédente et en évaluant en a, on obtient $P^{(j)}(a)=j!\,b_j$. □

Remarque : Le chapitre 10 a établi la formule de Taylor-Young pour les fonctions de classe $\mathcal{C}^n$: $f(x)=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(x-a)^k+o\big((x-a)^n\big)$. Pour un polynôme de degré au plus n, le reste est exactement nul : la partie régulière de son développement limité à l'ordre n en a est le polynôme lui-même.

13.5.3 Multiplicité et dérivées

Proposition 12 : Soit $P\neq 0$, $a\in\mathbb{K}$ et $m\in\mathbb{N}$. Alors a est racine de P de multiplicité m si et seulement si

$$P(a)=P'(a)=\cdots=P^{(m-1)}(a)=0 \qquad \text{et} \qquad P^{(m)}(a)\neq 0.$$

∘ Démonstration : Avec $n=\deg P$ et $c_k=\frac{P^{(k)}(a)}{k!}$, la formule de Taylor s'écrit

$$P=\sum_{k=0}^{m-1}c_k(X-a)^k+(X-a)^m\sum_{k=m}^{n}c_k(X-a)^{k-m}.$$

La première somme est de degré strictement inférieur à m : c'est le reste de la division de P par $(X-a)^m$, par unicité dans le théorème 2. Donc $(X-a)^m$ divise P si et seulement si $c_0=\cdots=c_{m-1}=0$. Dans ce cas, $P=(X-a)^mQ$ avec $Q(a)=c_m$, et la proposition 9 conclut. □

Exemples :

- Pour $P=X^5-5X+4$, on a $P(1)=0$, $P'=5X^4-5$ et $P'(1)=0$, puis $P''=20X^3$ et $P''(1)=20\neq 0$: 1 est racine double. La division donne $P=(X-1)^2(X^3+2X^2+3X+4)$.
- Pour le polynôme $P=(X+1)(X-1)^2(X-2)$ de l'introduction, 1 est racine de P et de P', mais pas de P''. Pour $\mathbb{K}=\mathbb{R}$, cela signifie que la courbe est tangente à l'axe des abscisses au point d'abscisse 1, ce que montrait la figure.

Remarque : L'erreur la plus répandue est d'oublier la condition $P^{(m)}(a)\neq 0$: les égalités $P(a)=\cdots=P^{(m-1)}(a)=0$ disent seulement que la multiplicité est *au moins* m. Pour X^3 en 0, on a $P(0)=P'(0)=0$, et pourtant 0 est racine triple, non double.

13.6 Arithmétique dans $\mathbb{K}[X]$

L'arithmétique de $\mathbb{K}[X]$ suit pas à pas celle de $\mathbb{Z}$: la division euclidienne y existe, le degré y remplace la valeur absolue, et les constantes non nulles y jouent le rôle de ± 1. Les démonstrations sont celles du chapitre 12 ; on les rappelle brièvement, en signalant ce qui change.

13.6.1 PGCD et PPCM

Au chapitre 12, le PGCD a été obtenu à partir des sous-groupes de $\mathbb{Z}$. Le rôle de ces sous-groupes est tenu ici par les parties de $\mathbb{K}[X]$ stables par somme et par multiplication par un polynôme quelconque ; on les appelle des *idéaux*, notion qui sera étudiée en deuxième année.

Proposition 13 : Soit I une partie de $\mathbb{K}[X]$ non réduite à $\{0\}$, telle que $P+Q \in I$ et $UP \in I$ pour tous P, Q de I et tout U de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire D tel que I soit l'ensemble $D\,\mathbb{K}[X]$ des multiples de D.

∘ Démonstration :

▷ *Existence.* L'ensemble des degrés des éléments non nuls de I est une partie non vide de $\mathbb{N}$: elle a un plus petit élément. Soit $D_0 \in I$ non nul de degré minimal, et D l'unitaire associé, qui est dans I puisque $D = \lambda D_0$. Tout multiple de D est dans I. Réciproquement, si $P \in I$, la division euclidienne $P = DQ + R$ donne $R = P - QD \in I$, avec $\deg R < \deg D$: par minimalité, $R = 0$.

▷ *Unicité.* Si $D\,\mathbb{K}[X] = D'\,\mathbb{K}[X]$, alors D et D' se divisent mutuellement : ils sont associés (proposition 5), et unitaires, donc égaux. □

Pour deux polynômes A et B, l'ensemble $A\,\mathbb{K}[X] + B\,\mathbb{K}[X] = \{AU + BV \mid U, V \in \mathbb{K}[X]\}$ et l'intersection $A\,\mathbb{K}[X] \cap B\,\mathbb{K}[X]$ vérifient les hypothèses de la proposition 13, dès qu'ils ne sont pas réduits à $\{0\}$.

Définition : Soit A et B deux polynômes.

- Si A et B ne sont pas tous deux nuls, le **PGCD** de A et B est l'unique polynôme unitaire D tel que $A\,\mathbb{K}[X] + B\,\mathbb{K}[X] = D\,\mathbb{K}[X]$. On le note $A \wedge B$.
- Si A et B sont non nuls, le **PPCM** de A et B est l'unique polynôme unitaire M tel que $A\,\mathbb{K}[X] \cap B\,\mathbb{K}[X] = M\,\mathbb{K}[X]$. On le note $A \vee B$. Si A ou B est nul, on pose $A \vee B = 0$.

Proposition 14 : Soit A et B deux polynômes non tous deux nuls.

(i) Les diviseurs communs à A et B sont exactement les diviseurs de $A \wedge B$; en particulier, $A \wedge B$ est un diviseur commun de degré maximal.

(ii) Les multiples communs à A et B sont exactement les multiples de $A \vee B$.

(iii) Si $B \neq 0$ et si R est le reste de la division euclidienne de A par B, alors $A \wedge B = B \wedge R$.

∘ Démonstration :

▷ *(i)* Comme $A = A \times 1 + B \times 0$, le polynôme A est multiple de $D = A \wedge B$, et de même B. Un diviseur de D divise donc A et B. Réciproquement, D s'écrit $AU + BV$, et un diviseur commun de A et B divise $AU + BV$. Un diviseur commun divise D, donc a un degré au plus égal à celui de D.

▷ *(ii)* C'est la définition de $A \vee B$, lorsque A et B sont non nuls ; sinon, le seul multiple commun est 0.

▷ *(iii)* Les ensembles $A\,\mathbb{K}[X] + B\,\mathbb{K}[X]$ et $B\,\mathbb{K}[X] + R\,\mathbb{K}[X]$ sont égaux, puisque $R = A - BQ$ et $A = BQ + R$, comme dans la proposition 4 du chapitre 12. □

Remarque : Le point (i) dit que l'on aurait pu définir le PGCD comme l'unique diviseur commun unitaire de degré maximal. L'unitarité est indispensable à l'unicité : $X+1$, $2X+2$ et $-X-1$ sont trois diviseurs communs de degré maximal de X^2-1 et X^2+X, et seul le premier est leur PGCD.

13.6.2 Relation de Bézout et algorithme d'Euclide

Théorème 7 : Relation de Bézout :
Soit A et B deux polynômes non tous deux nuls. Il existe des polynômes U et V tels que

$$AU + BV = A \wedge B.$$

∘ Démonstration : Par définition, $A \wedge B$ appartient à $A\,\mathbb{K}[X] + B\,\mathbb{K}[X]$. □

Comme pour les entiers, le point (iii) de la proposition 14 fournit un algorithme : on divise A par B, puis B par le reste, et ainsi de suite. Les degrés des restes décroissent strictement, donc l'un d'eux est nul ; le PGCD est l'unitaire associé au dernier reste non nul, et l'on obtient U et V en remontant les calculs, comme à la section 12.3.

♡ **Méthode : Pour calculer $A \wedge B$ et une relation de Bézout :**

- On effectue les divisions euclidiennes successives, en numérotant les lignes (L_1), (L_2), etc., jusqu'à un reste nul.
- On divise le dernier reste non nul par son coefficient dominant : c'est $A \wedge B$.
- On isole ce dernier reste dans l'avant-dernière ligne, puis on remonte en remplaçant à chaque étape le reste de plus petit degré par son expression tirée de la ligne au-dessus.

Exemple : Pour $A = X^4 - 1$ et $B = X^3 + 2X^2 + 2X + 1$, les divisions successives donnent

$$A = (X-2)B + \underbrace{(2X^2 + 3X + 1)}_{R_1} \quad (L_1), \qquad B = \Big(\frac{X}{2} + \frac{1}{4}\Big)R_1 + \underbrace{\frac{3}{4}(X+1)}_{R_2} \quad (L_2),$$

puis $R_1 = (2X+1)(X+1)$ est un multiple de R_2. Donc $A \wedge B = X + 1$. La remontée donne

$$R_2 = B - \Big(\frac{X}{2} + \frac{1}{4}\Big)(A - (X-2)B) = -\frac{2X+1}{4}\,A + \frac{2X^2 - 3X + 2}{4}\,B,$$

et, en multipliant par $\frac{4}{3}$, $X + 1 = -\frac{2X+1}{3}\,A + \frac{2X^2-3X+2}{3}\,B$. On le vérifie en développant. Des fractions apparaissent alors que A et B sont à coefficients entiers : c'est la division par les coefficients dominants qui les introduit, et c'est pourquoi on travaille sur un corps.

13.6.3 Polynômes premiers entre eux

Définition : Deux polynômes A et B non tous deux nuls sont **premiers entre eux** si $A \wedge B = 1$, c'est-à-dire si leurs seuls diviseurs communs sont les constantes non nulles.

Théorème 8 : Théorème de Bézout :
Les polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que

$$AU + BV = 1.$$

∘ Démonstration : Si $A \wedge B = 1$, c'est le théorème 7. Réciproquement, si $AU + BV = 1$, alors $1 \in A\,\mathbb{K}[X] + B\,\mathbb{K}[X] = (A \wedge B)\,\mathbb{K}[X]$, donc $A \wedge B$ divise 1 : c'est une constante, unitaire, donc égale à 1. □

Théorème 9 : Lemme de Gauss :
Soit A, B, C trois polynômes. Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$.

∘ Démonstration : On écrit $AU + BV = 1$, et l'on multiplie par C : $C = ACU + BCV$. Or A divise ACU et BC, donc C. □

Proposition 15 : Soit A, B, N des polynômes.

(i) Si $A \mid N$, $B \mid N$ et $A \wedge B = 1$, alors $AB \mid N$.

(ii) Si $A \wedge N = 1$ et $B \wedge N = 1$, alors $AB \wedge N = 1$.

(iii) Si A et B sont unitaires, alors $(A \wedge B)(A \vee B) = AB$.

∘ Démonstration :

▷ *(i)* On écrit $N = AK$; comme $B \mid AK$ et $B \wedge A = 1$, le lemme de Gauss donne $B \mid K$.

▷ *(ii)* On multiplie les relations $AU + NV = 1$ et $BU' + NV' = 1$: on obtient $AB(UU') + N(\cdots) = 1$.

▷ *(iii)* On reprend la démonstration de la proposition 7 du chapitre 12 : avec $D = A \wedge B$, $A = DA'$ et $B = DB'$, on a $A' \wedge B' = 1$, en divisant une relation de Bézout par D, et $M = DA'B'$ est unitaire. C'est un multiple commun de A et de B, et si N est un multiple commun, alors $N = AK = DA'K$ et $B' \mid A'K$, donc $B' \mid K$ par le lemme de Gauss, et $M \mid N$. Ainsi $M = A \vee B$, et $DM = D^2A'B' = AB$. □

Remarque : Les définitions s'étendent à une famille finie $(A_1, \dots, A_n)$ de polynômes non tous nuls : son PGCD est l'unique polynôme unitaire D tel que $\sum_i A_i\,\mathbb{K}[X] = D\,\mathbb{K}[X]$, et la relation de Bézout s'écrit $A_1U_1 + \cdots + A_nU_n = D$. On distingue, comme à la section 12.4, les polynômes premiers entre eux *dans leur ensemble* ($D = 1$) et *deux à deux* : $X(X-1)$, $X(X-2)$ et $(X-1)(X-2)$ sont premiers entre eux dans leur ensemble, sans l'être deux à deux.

13.7 Polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$

Remarque : Comme $\mathbb{R} \subset \mathbb{C}$, un polynôme à coefficients réels est aussi un polynôme à coefficients complexes : $\mathbb{R}[X] \subset \mathbb{C}[X]$, et l'on peut évaluer un polynôme réel en tout nombre complexe. Les opérations, le degré et la dérivation ne dépendent pas du corps dans lequel on les calcule. Il en va de même de la division euclidienne : si A et B sont réels, leur division dans $\mathbb{R}[X]$ fournit un quotient et un reste qui conviennent aussi dans $\mathbb{C}[X]$, et ce sont donc, par unicité, ceux de la division dans $\mathbb{C}[X]$. Par l'algorithme d'Euclide, le PGCD de deux polynômes réels est le même dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$. Seule la notion d'irréductibilité change, comme on va le voir.

13.7.1 Décomposition en facteurs irréductibles

Les nombres premiers sont les entiers $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p. Leur analogue dans $\mathbb{K}[X]$ est le suivant.

Définition : Un polynôme $P \in \mathbb{K}[X]$ est **irréductible** s'il n'est pas constant et si ses seuls diviseurs sont les constantes non nulles et les polynômes associés à P.

Les polynômes de degré 1 sont irréductibles : un diviseur d'un polynôme de degré 1 est de degré 0 ou 1. Si I est irréductible et ne divise pas A, alors $I \wedge A = 1$, puisque $I \wedge A$ est un diviseur unitaire de I qui n'est pas associé à I. Le lemme de Gauss donne donc le *lemme d'Euclide* : si un irréductible divise un produit AB, il divise A ou B.

Théorème 10 : Décomposition en facteurs irréductibles :
Tout polynôme non constant $P \in \mathbb{K}[X]$ s'écrit

$$P = \lambda\, P_1^{\alpha_1} \cdots P_r^{\alpha_r},$$

où λ est le coefficient dominant de P, les P_i des polynômes irréductibles unitaires deux à deux distincts, et les α_i des entiers naturels non nuls. Cette écriture est unique à l'ordre des facteurs près.

∘ Démonstration :

▷ *Existence.* Par récurrence forte sur le degré. Si P est irréductible, $P = \lambda \times \frac{P}{\lambda}$ convient. Sinon, P a un diviseur A qui n'est ni constant ni associé à P : $P = AB$ avec $1 \leqslant \deg A, \deg B < \deg P$, et l'on applique l'hypothèse de récurrence à A et B.

▷ *Unicité.* Comme pour le théorème 6 du chapitre 12, par récurrence forte sur le degré. Le coefficient dominant est imposé. Si $P_1 \cdots P_k = Q_1 \cdots Q_\ell$ sont deux produits d'irréductibles unitaires, le lemme d'Euclide montre que P_1 divise l'un des Q_j, donc lui est égal, puisque deux irréductibles unitaires qui se divisent sont associés et unitaires. On simplifie par P_1, ce qui est permis dans l'anneau intègre $\mathbb{K}[X]$, et l'on conclut par l'hypothèse de récurrence. □

Tout dépend donc de la liste des irréductibles, qui dépend du corps : $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, puisqu'un diviseur de degré 1 fournirait une racine réelle, mais il ne l'est pas dans $\mathbb{C}[X]$. Pour $\mathbb{K} = \mathbb{C}$, la réponse repose sur le théorème suivant, annoncé aux chapitres 4 et 8.

Théorème 11 : Théorème de d'Alembert-Gauss (admis) :
Tout polynôme non constant à coefficients complexes possède au moins une **racine complexe**.

Démonstration admise. Toutes les démonstrations connues utilisent un argument d'analyse. La plus courante montre d'abord que $z \mapsto |P(z)|$ atteint un minimum sur $\mathbb{C}$, ce qui demande la notion de partie compacte du plan, étudiée en deuxième année ; elle montre ensuite, grâce aux racines k-ièmes du chapitre 4, qu'en un point z_0 où $P(z_0) \neq 0$, on peut toujours trouver un point voisin où $|P|$ est plus petit.

13.7.2 Polynômes de $\mathbb{C}[X]$

Proposition 16 : Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Tout polynôme non constant de $\mathbb{C}[X]$ est scindé :

$$P = \lambda\,(X-a_1)^{m_1}\cdots(X-a_r)^{m_r},$$

où $a_1,\dots,a_r$ sont les racines distinctes de P et $m_1,\dots,m_r$ leurs multiplicités, de somme $\deg P$. Pour A et B non nuls dans $\mathbb{C}[X]$:

(i) A divise B si et seulement si toute racine de A est racine de B, avec une multiplicité au moins égale ;

(ii) A et B sont premiers entre eux si et seulement s'ils n'ont **aucune racine commune**.

∘ Démonstration : Si P est de degré au moins 2, il a une racine a par le théorème 11, et $X-a$ est un diviseur non trivial : P n'est pas irréductible. Le théorème 10 donne alors la factorisation. Pour le point (i), si $B=AC$ et si a est racine de A de multiplicité m, alors $(X-a)^m$ divise A, donc B. Réciproquement, si chaque racine a_i de A, de multiplicité m_i, est racine de B de multiplicité au moins m_i, la proposition 10 montre que $\prod_i (X-a_i)^{m_i}$ divise B ; or ce produit est associé à A. Pour le point (ii), une racine commune a donne le diviseur commun $X-a$; réciproquement, si $A\wedge B\neq 1$, ce polynôme non constant a une racine, qui est commune à A et à B. □

Proposition 17 : Pour tout $n\in\mathbb{N}^*$, avec $\omega=\mathrm{e}^{2\mathrm{i}\pi/n}$,

$$X^n-1=\prod_{k=0}^{n-1}(X-\omega^k).$$

∘ Démonstration : Les n racines n-ièmes de l'unité ω^k, $0\leqslant k\leqslant n-1$, sont distinctes (chapitre 4, proposition 21) et sont racines de X^n-1. Par la proposition 8, leur produit divise X^n-1 ; les deux polynômes sont unitaires et de degré n, ils sont donc égaux. □

En comparant les coefficients de X^{n-1}, le théorème 4 redonne, pour $n\geqslant 2$, la somme $\sum_{k=0}^{n-1}\omega^k=0$ du chapitre 4.

13.7.3 Polynômes de $\mathbb{R}[X]$

Proposition 18 : Soit $P\in\mathbb{R}[X]$ et $z\in\mathbb{C}$. Si z est racine de P de multiplicité m, alors $\overline{z}$ est racine de P de même multiplicité m.

∘ Démonstration : Les coefficients de P étant réels, la conjugaison donne $\overline{P(w)}=P(\overline{w})$ pour tout $w\in\mathbb{C}$, et de même pour les dérivées $P^{(k)}$, qui sont encore à coefficients réels. La caractérisation de la proposition 12 est donc vérifiée en $\overline{z}$ dès qu'elle l'est en z. □

Théorème 12 : Irréductibles de $\mathbb{R}[X]$:
Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de **discriminant strictement négatif**. Tout polynôme non constant $P\in\mathbb{R}[X]$ s'écrit donc

$$P=\lambda\prod_{i=1}^{r}(X-a_i)^{m_i}\prod_{j=1}^{s}(X^2+p_jX+q_j)^{n_j},\qquad p_j^2-4q_j<0.$$

∘ Démonstration : Un polynôme de degré 2 sans racine réelle est irréductible dans $\mathbb{R}[X]$, puisqu'un diviseur de degré 1 fournirait une racine réelle ; c'est le cas lorsque le discriminant est négatif. Réciproquement, soit $P\in\mathbb{R}[X]$ irréductible, de degré au moins 2. Il n'a pas de racine réelle, sinon $X-a$ le diviserait. Par le théorème 11, il a une racine $z\in\mathbb{C}\setminus\mathbb{R}$, et $\overline{z}\neq z$ est aussi racine. Le polynôme

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

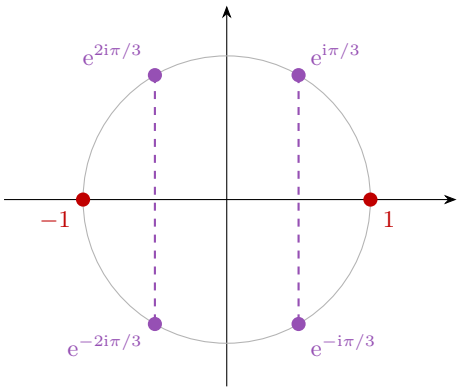
est à coefficients réels, et divise P dans $\mathbb{C}[X]$ par la proposition 8. Le quotient est à coefficients réels, puisque la division dans $\mathbb{R}[X]$ donne le même quotient, d'après la remarque du début de cette section. Comme P est irréductible, il est associé à $X^2 - 2\,\mathrm{Re}(z)X + |z|^2$, de discriminant $-4\,\mathrm{Im}(z)^2 < 0$. La factorisation découle du théorème 10. □

♡ **Méthode : Pour factoriser un polynôme $P \in \mathbb{R}[X]$ en irréductibles :**

- On factorise P dans $\mathbb{C}[X]$: $P = \lambda \prod (X - z_k)^{m_k}$, où λ est le coefficient dominant et m_k la multiplicité de la racine z_k.
- Chaque racine réelle α, de multiplicité m, fournit le facteur $(X - \alpha)^m$.
- Les racines non réelles vont par paires de conjuguées de même multiplicité (proposition 18). On choisit *une seule* racine z dans chaque paire, par exemple celle de partie imaginaire strictement positive ; si elle est de multiplicité m, elle fournit le facteur $(X - z)^m (X - \overline{z})^m = \left(X^2 - 2\,\mathrm{Re}(z)\,X + |z|^2\right)^m$.
- On contrôle que la somme des degrés des facteurs, multiplicités comprises, est égale à $\deg P$.

Remarque : Le passage par $\mathbb{C}$ est toujours possible, mais il n'est pas toujours le plus court. On peut souvent chercher d'abord une racine réelle évidente et diviser, ou faire apparaître une différence de deux carrés, comme pour $X^4 + 1$ à la fin de cette section. Pour $X^n - 1$ ou $X^n + 1$, on part directement des racines n-ièmes du chapitre 4. L'erreur la plus répandue est de garder les deux racines d'une même paire : on écrit alors deux fois le même trinôme, et le degré obtenu est trop grand, ce que le contrôle final détecte.

La figure applique la méthode à $X^6 - 1$, dont les six racines sont les racines sixièmes de l'unité : les deux racines réelles ± 1 donnent deux facteurs de degré 1, et les deux paires de racines conjuguées donnent deux trinômes.



$(X - e^{i\pi/3})(X - e^{-i\pi/3}) = X^2 - X + 1$
$(X - e^{2i\pi/3})(X - e^{-2i\pi/3}) = X^2 + X + 1$

racines réelles : $X - 1$ et $X + 1$

Chaque segment violet relie deux racines conjuguées ; leur produit est un trinôme réel de discriminant -3. On obtient

$$X^6 - 1 = (X - 1)(X + 1)(X^2 - X + 1)(X^2 + X + 1) \quad \text{dans } \mathbb{R}[X].$$

Remarque : L'erreur la plus répandue est de croire qu'un polynôme réel sans racine réelle est irréductible dans $\mathbb{R}[X]$. C'est vrai en degré 2 et 3, mais faux au-delà : $X^4 + 1$ n'a pas de racine réelle, et pourtant $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$. Le théorème 12 dit que les seuls irréductibles réels sont de degré au plus 2.

13.8 Interpolation de Lagrange

Le théorème 3 dit qu'un polynôme de degré au plus $n - 1$ est déterminé par ses valeurs en n points distincts. On peut le reconstituer explicitement à partir de ces valeurs.

Théorème 13 : Interpolation de Lagrange :
Soit $x_1, \ldots, x_n$ des éléments deux à deux distincts de $\mathbb{K}$, et $y_1, \ldots, y_n$ des éléments de $\mathbb{K}$. Il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que $P(x_i) = y_i$ pour tout i :

$$P = \sum_{i=1}^{n} y_i L_i, \qquad \text{où} \qquad L_i = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}.$$

∘ Démonstration :

▷ *Existence.* Le polynôme L_i est de degré $n-1$, s'annule en chaque x_j avec $j \neq i$, et vaut 1 en x_i. Donc $P(x_k) = \sum_i y_i L_i(x_k) = y_k$, et $P \in \mathbb{K}_{n-1}[X]$.

▷ *Unicité.* Deux tels polynômes prennent les mêmes valeurs en n points distincts et sont de degré au plus $n-1$: ils sont égaux par le théorème 3. □

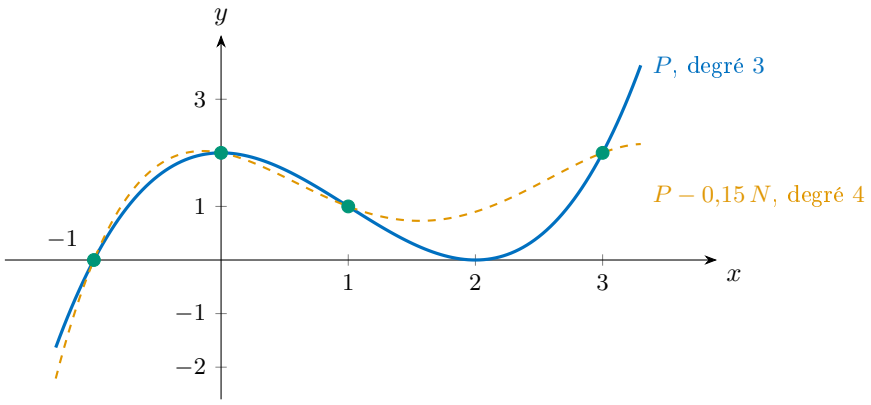
Proposition 19 : Avec les notations du théorème 13, et $N = (X-x_1)\cdots(X-x_n)$, les polynômes Q tels que $Q(x_i) = y_i$ pour tout i sont exactement les $Q = P + AN$, où A parcourt $\mathbb{K}[X]$.

∘ Démonstration : Ces polynômes conviennent, puisque N s'annule en chaque x_i. Réciproquement, si Q convient, $Q - P$ admet les n racines distinctes x_i, donc est divisible par N (proposition 8). □

Exemple : On cherche le polynôme de degré au plus 3 qui vaut 0, 2, 1, 2 en -1, 0, 1, 3. Le calcul des quatre L_i donne

$$P = \frac{1}{2}X^3 - \frac{3}{2}X^2 + 2 = \frac{1}{2}(X+1)(X-2)^2.$$

On vérifie que $P(0) = 2$, $P(1) = 1$ et $P(3) = 2$. Le polynôme n'est que de degré 3, mais la factorisation révèle une racine double en 2, qu'aucune des données ne laissait prévoir.



Les deux courbes passent par les quatre points verts : le polynôme de Lagrange P est le seul de degré au plus 3, et l'on obtient tous les autres en lui ajoutant un multiple de $N = (X+1)X(X-1)(X-3)$, comme le dit la proposition 19.

Remarque : Le chapitre 14 donnera à ce résultat sa forme naturelle : les polynômes $L_1, \ldots, L_n$ forment une base de l'espace vectoriel $\mathbb{K}_{n-1}[X]$, et les y_i sont les coordonnées de P dans cette base.

13.9 Fractions rationnelles

13.9.1 Le corps $\mathbb{K}(X)$

On construit les fractions de polynômes comme on construit les rationnels à partir des entiers : un rationnel est une fraction $\frac{p}{q}$, et deux écritures $\frac{p}{q}$ et $\frac{p'}{q'}$ désignent le même nombre si $pq' = p'q$.

Définition : Sur l'ensemble des couples (P, Q) de polynômes avec $Q \neq 0$, on pose $(P, Q) \sim (P', Q')$ si $PQ' = P'Q$. Une **fraction rationnelle** est une classe d'équivalence pour cette relation ; la classe de (P, Q) est notée $\frac{P}{Q}$. L'ensemble des fractions rationnelles est noté $\mathbb{K}(X)$.

Proposition 20 : La relation $\sim$ est une relation d'équivalence. Les opérations

$$\frac{P}{Q} + \frac{P'}{Q'} = \frac{PQ' + P'Q}{QQ'} \qquad \text{et} \qquad \frac{P}{Q} \times \frac{P'}{Q'} = \frac{PP'}{QQ'}$$

ne dépendent pas des couples choisis, et font de $\mathbb{K}(X)$ un corps commutatif. L'application $P \mapsto \frac{P}{1}$ est un morphisme d'anneaux injectif de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$.

∘ Démonstration :

▷ *Équivalence.* La réflexivité et la symétrie sont claires. Si $PQ' = P'Q$ et $P'Q'' = P''Q'$, alors

$$Q'(PQ'') = (P'Q)Q'' = Q(P''Q') = Q'(P''Q),$$

et l'on simplifie par $Q' \neq 0$, puisque $\mathbb{K}[X]$ est intègre : $PQ'' = P''Q$. Les dénominateurs QQ' sont non nuls pour la même raison.

▷ *Indépendance.* Si $(P, Q) \sim (P_1, Q_1)$, alors $(PP')Q_1Q' = (P_1Q)P'Q' = (P_1P')(QQ')$, ce qui traite le produit ; pour la somme, $(PQ' + P'Q)Q_1Q' = (P_1Q' + P'Q_1)QQ'$ se vérifie en développant, avec $PQ_1 = P_1Q$. On raisonne de même sur le second couple.

▷ *Axiomes de corps.* Les vérifications de l'associativité, de la commutativité et de la distributivité sont des calculs sur des couples, identiques à ceux que l'on fait pour les fractions d'entiers ; elles sont admises ici. Le neutre additif est $\frac{0}{1}$, le neutre multiplicatif $\frac{1}{1}$, et si $P \neq 0$, l'inverse de $\frac{P}{Q}$ est $\frac{Q}{P}$.

▷ *Plongement.* On a $\frac{P}{1} + \frac{P'}{1} = \frac{P+P'}{1}$ et $\frac{P}{1} \times \frac{P'}{1} = \frac{PP'}{1}$, et $\frac{P}{1} = \frac{P'}{1}$ si et seulement si $P = P'$. □

On identifie désormais P à $\frac{P}{1}$: $\mathbb{K}[X]$ devient un sous-anneau du corps $\mathbb{K}(X)$, de même que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.

Proposition 21 : *(Forme irréductible.)* Toute fraction rationnelle non nulle F s'écrit de façon unique $F = \frac{P}{Q}$ avec $P \wedge Q = 1$ et Q unitaire.

∘ Démonstration :

▷ *Existence.* Si $F = \frac{A}{B}$, on écrit $A = DP_0$ et $B = DQ_0$ avec $D = A \wedge B$, de sorte que $P_0 \wedge Q_0 = 1$, puis on divise P_0 et Q_0 par le coefficient dominant de Q_0.

▷ *Unicité.* Si $\frac{P}{Q} = \frac{P'}{Q'}$ sont deux telles écritures, alors $PQ' = P'Q$. Donc Q divise PQ', et comme $Q \wedge P = 1$, le lemme de Gauss donne $Q \mid Q'$. De même $Q' \mid Q$: ils sont associés et unitaires, donc égaux, puis $P = P'$. □

13.9.2 Degré, partie entière, zéros et pôles

Si $\frac{P}{Q} = \frac{P'}{Q'}$, l'égalité $PQ' = P'Q$ donne $\deg P - \deg Q = \deg P' - \deg Q'$. On peut donc poser $\deg \frac{P}{Q} = \deg P - \deg Q$, élément de $\mathbb{Z} \cup \{-\infty\}$. On vérifie, comme à la proposition 3, que

$$\deg(F + G) \leqslant \max(\deg F, \deg G) \qquad \text{et} \qquad \deg(FG) = \deg F + \deg G.$$

Proposition 22 : *(Partie entière.)* Toute fraction rationnelle F s'écrit de façon unique $F = E + G$, où E est un polynôme et G une fraction rationnelle de degré strictement négatif. Le polynôme E est la **partie entière** de F ; si $F = \frac{P}{Q}$, c'est le quotient de la division euclidienne de P par Q.

∘ Démonstration : La division euclidienne $P = QE + R$ donne $F = E + \frac{R}{Q}$, avec $\deg \frac{R}{Q} = \deg R - \deg Q < 0$. Si $E + G = E' + G'$, alors $E - E' = G' - G$ est un polynôme de degré strictement négatif, donc nul. □

Définition : Soit $F = \frac{P}{Q}$ une fraction sous forme irréductible. Les **zéros** de F sont les racines de P, et ses **pôles** les racines de Q ; la multiplicité d'un zéro ou d'un pôle est sa multiplicité comme racine de P ou de Q. La **fonction rationnelle** associée à F est l'application $x \mapsto \frac{P(x)}{Q(x)}$, définie sur $\mathbb{K}$ privé des pôles de F.

Un pôle et un zéro ne peuvent coïncider, puisque P et Q sont premiers entre eux : sur $\mathbb{C}$, ils n'ont pas de racine commune (proposition 16). C'est pourquoi on se place sous forme irréductible : la fraction $\frac{X^2-1}{X-1}$ est égale au polynôme $X + 1$, qui n'a aucun pôle, bien que $X - 1$ s'annule en 1.

13.10 Décomposition en éléments simples

13.10.1 Le théorème

Au chapitre 6, on a calculé une primitive de $\dfrac{1}{x^2-3x+2}$ en écrivant $\dfrac{1}{x^2-3x+2}=\dfrac{1}{x-2}-\dfrac{1}{x-1}$. Cette section montre que toute fraction rationnelle se décompose ainsi en une somme de fractions dont le dénominateur est une puissance d'un polynôme irréductible.

Théorème 14 : Décomposition en éléments simples :
Soit $F=\frac{P}{Q}$ une fraction rationnelle sous forme irréductible, de partie entière E.

- *Sur* $\mathbb{C}$. Si $Q=(X-a_1)^{m_1}\cdots(X-a_r)^{m_r}$ avec les a_i distincts, il existe des complexes $c_{i,k}$, uniques, tels que
$$F=E+\sum_{i=1}^{r}\sum_{k=1}^{m_i}\frac{c_{i,k}}{(X-a_i)^k}.$$
- *Sur* $\mathbb{R}$. Si $Q=\prod_i(X-a_i)^{m_i}\prod_j(X^2+p_jX+q_j)^{n_j}$ est la décomposition du théorème 12, il existe des réels $c_{i,k}$, $b_{j,k}$, $d_{j,k}$, uniques, tels que
$$F=E+\sum_{i}\sum_{k=1}^{m_i}\frac{c_{i,k}}{(X-a_i)^k}+\sum_{j}\sum_{k=1}^{n_j}\frac{b_{j,k}X+d_{j,k}}{(X^2+p_jX+q_j)^k}.$$

Les termes des sommes sont les **éléments simples**, de première espèce $\frac{c}{(X-a)^k}$ et de seconde espèce $\frac{bX+d}{(X^2+pX+q)^k}$; la somme des éléments simples relatifs au pôle a_i est la **partie polaire** de F en a_i.

Les deux cas se traitent ensemble : dans les deux, Q est un produit $B_1^{m_1}\cdots B_s^{m_s}$ de puissances de polynômes irréductibles unitaires deux à deux distincts, et un élément simple est une fraction $\frac{C}{B_i^k}$ avec $\deg C<\deg B_i$.

∘ Démonstration :

▷ *Séparation des facteurs.* Soit $\frac{A}{Q_1Q_2}$ avec $Q_1\wedge Q_2=1$ et $\deg A<\deg Q_1+\deg Q_2$. La relation de Bézout $Q_1U+Q_2V=1$ donne
$$\frac{A}{Q_1Q_2}=\frac{A(Q_1U+Q_2V)}{Q_1Q_2}=\frac{AV}{Q_1}+\frac{AU}{Q_2}.$$
On écrit $\frac{AV}{Q_1}=E_1+\frac{A_1}{Q_1}$ et $\frac{AU}{Q_2}=E_2+\frac{A_2}{Q_2}$ (proposition 22). Le membre de gauche étant de degré strictement négatif, l'unicité de la partie entière impose $E_1+E_2=0$. Ainsi $\frac{A}{Q_1Q_2}=\frac{A_1}{Q_1}+\frac{A_2}{Q_2}$, avec $\deg A_i<\deg Q_i$. Comme les $B_i^{m_i}$ sont premiers entre eux deux à deux (proposition 15 (ii)), une récurrence ramène $\frac{P}{Q}-E$ à une somme de fractions $\frac{A_i}{B_i^{m_i}}$ avec $\deg A_i<m_i\deg B_i$.

▷ *Développement selon les puissances de* B. Soit B non constant et $\deg C<k\deg B$. Par récurrence sur k, la fraction $\frac{C}{B^k}$ est une somme $\sum_{j=1}^{k}\frac{C_j}{B^j}$ avec $\deg C_j<\deg B$: pour $k=1$, il n'y a rien à faire, et sinon la division $C=BS+C_k$ donne $\deg C_k<\deg B$, $\deg S<(k-1)\deg B$, et $\frac{C}{B^k}=\frac{S}{B^{k-1}}+\frac{C_k}{B^k}$. Pour $B=X-a$, les C_j sont des constantes ; pour $B=X^2+pX+q$, ils sont de degré au plus 1. L'existence est établie.

▷ *Unicité.* La partie entière est unique, puisqu'une somme d'éléments simples est de degré strictement négatif. Il suffit donc de montrer qu'une somme $\sum_{i,j}\frac{C_{i,j}}{B_i^j}$ d'éléments simples, avec $\deg C_{i,j}<\deg B_i$, ne peut être nulle que si tous les $C_{i,j}$ sont nuls. Sinon, on choisit i et le plus grand m tel que $C_{i,m}\neq 0$, et l'on multiplie par B_i^mT, où T est le produit des $B_\ell^{m_\ell}$ pour $\ell\neq i$. Tous les termes deviennent des polynômes multiples de B_i, sauf $C_{i,m}T$; donc B_i divise $C_{i,m}T$. Or B_i est irréductible et ne divise aucun B_ℓ pour $\ell\neq i$, donc il ne divise pas T, et le lemme d'Euclide donne $B_i\mid C_{i,m}$, ce qui est impossible puisque $0\leqslant\deg C_{i,m}<\deg B_i$. □

Remarque : Le théorème est l'analogue de l'écriture d'un rationnel comme somme de fractions dont les dénominateurs sont des puissances de nombres premiers, par exemple $\frac{7}{12} = \frac{1}{4} + \frac{1}{3}$, où $12 = 2^2 \times 3$. La démonstration en donne d'ailleurs un algorithme, mais on calcule plus vite les coefficients par les méthodes qui suivent.

13.10.2 Calcul des coefficients

Proposition 23 : *(Pôle simple.)* Soit $F = \frac{P}{Q}$ sous forme irréductible, et a un pôle simple : $Q = (X-a)Q_1$ avec $Q_1(a) \neq 0$. Le coefficient de $\frac{1}{X-a}$ dans la décomposition de F vaut

$$c = \frac{P(a)}{Q_1(a)} = \frac{P(a)}{Q'(a)}.$$

∘ Démonstration : On écrit $F = \frac{c}{X-a} + G$, où G regroupe la partie entière et les autres éléments simples, qui n'ont pas a pour pôle. En multipliant par $X-a$, on obtient l'égalité de fractions $\frac{P}{Q_1} = c + (X-a)G$, et l'on évalue en a, qui n'est pôle d'aucun des deux membres. Enfin, $Q' = Q_1 + (X-a)Q_1'$ donne $Q'(a) = Q_1(a)$. □

♡ **Méthode : Pour décomposer une fraction rationnelle en éléments simples** :

- ▶ On met F sous forme irréductible, on calcule sa partie entière par division euclidienne, et l'on factorise le dénominateur ; on écrit la forme de la décomposition avec des coefficients inconnus.
- ▶ Pour un pôle simple a, on applique la proposition 23. Pour un pôle a d'ordre m, on multiplie par $(X-a)^m$ et l'on évalue en a : on obtient le coefficient de $\frac{1}{(X-a)^m}$.
- ▶ Les coefficients restants s'obtiennent par la limite de $xF(x)$ en $+\infty$, qui donne la somme des coefficients des $\frac{1}{X-a_i}$ lorsque $\deg F < 0$, par l'évaluation en un point simple, ou par la parité.
- ▶ Sur $\mathbb{R}$, on peut décomposer sur $\mathbb{C}$, puis regrouper les termes associés à deux pôles conjugués.

Exemples :

- Pour $F = \frac{X^2+1}{(X-1)^2(X+2)}$, de degré -1, on cherche $F = \frac{\alpha}{(X-1)^2} + \frac{\beta}{X-1} + \frac{\gamma}{X+2}$. En multipliant par $(X-1)^2$ et en évaluant en 1 : $\alpha = \frac{2}{3}$. Par la proposition 23 en -2 : $\gamma = \frac{5}{9}$. La limite de $xF(x)$ en $+\infty$ vaut $1 = \beta + \gamma$, donc $\beta = \frac{4}{9}$:

$$\frac{X^2+1}{(X-1)^2(X+2)} = \frac{2}{3(X-1)^2} + \frac{4}{9(X-1)} + \frac{5}{9(X+2)}.$$

  On contrôle en 0 : $F(0) = \frac{1}{2}$ et $\frac{2}{3} - \frac{4}{9} + \frac{5}{18} = \frac{1}{2}$.

- Pour $F = \frac{1}{X^3-1}$, les pôles sont les racines cubiques de l'unité 1, j, $\overline{j}$, toutes simples. Pour chacune, $\frac{1}{Q'(\omega)} = \frac{1}{3\omega^2} = \frac{\omega}{3}$, puisque $\omega^3 = 1$. Sur $\mathbb{C}$:

$$\frac{1}{X^3-1} = \frac{1}{3}\Big(\frac{1}{X-1} + \frac{j}{X-j} + \frac{\overline{j}}{X-\overline{j}}\Big).$$

  On regroupe les deux derniers termes, avec $j + \overline{j} = -1$ et $j\overline{j} = 1$: $\frac{j(X-\overline{j})+\overline{j}(X-j)}{X^2+X+1} = \frac{-X-2}{X^2+X+1}$. Sur $\mathbb{R}$:

$$\frac{1}{X^3-1} = \frac{1}{3(X-1)} - \frac{X+2}{3(X^2+X+1)}.$$

Proposition 24 : *(Dérivée logarithmique.)* Si $P = \lambda(X-a_1)^{m_1}\cdots(X-a_r)^{m_r}$ est scindé, avec des a_i distincts, alors

$$\frac{P'}{P} = \sum_{i=1}^{r} \frac{m_i}{X-a_i}.$$

◦ Démonstration : Si A et B sont non nuls, la règle du produit (proposition 11) donne, dans $\mathbb{K}(X)$,

$$\frac{(AB)'}{AB} = \frac{A'B + AB'}{AB} = \frac{A'}{A} + \frac{B'}{B}.$$

Par récurrence, la dérivée logarithmique d'un produit est la somme des dérivées logarithmiques des facteurs. Celle d'une constante non nulle est nulle, et celle de $(X-a)^m$ vaut $\frac{m(X-a)^{m-1}}{(X-a)^m} = \frac{m}{X-a}$. □

Par exemple, $\dfrac{nX^{n-1}}{X^n-1} = \displaystyle\sum_{k=0}^{n-1} \frac{1}{X-\omega^k}$, d'après la proposition 17.

13.10.3 Applications

Exemples :

- *Primitives.* La décomposition du premier exemple donne, sur un intervalle ne contenant ni 1 ni -2,

$$\int \frac{x^2+1}{(x-1)^2(x+2)}\,\mathrm{d}x = -\frac{2}{3(x-1)} + \frac{4}{9}\ln|x-1| + \frac{5}{9}\ln|x+2| + C.$$

  Les éléments de seconde espèce se traitent comme au chapitre 6, par un terme en $\frac{u'}{u}$ et un terme en Arctan : c'est la généralisation annoncée alors.

- *Dérivées successives.* Comme $\frac{1}{X^2-1} = \frac{1}{2}\Big(\frac{1}{X-1} - \frac{1}{X+1}\Big)$, on obtient, pour $x \neq \pm 1$ et tout $n \in \mathbb{N}$,

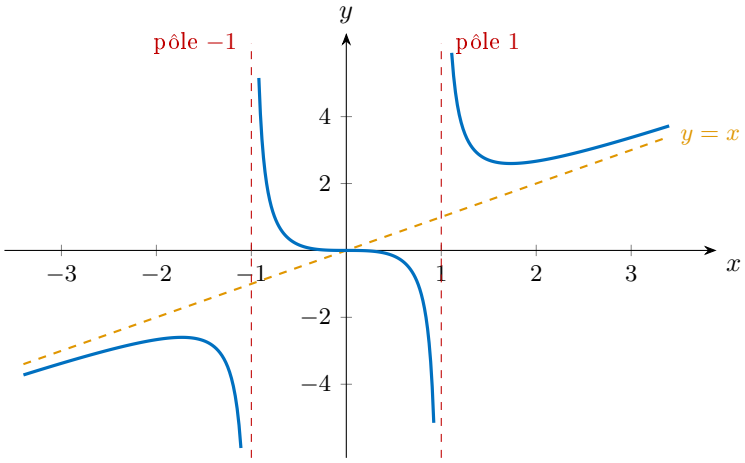
$$\Big(\frac{1}{x^2-1}\Big)^{(n)} = \frac{(-1)^n\, n!}{2}\Big(\frac{1}{(x-1)^{n+1}} - \frac{1}{(x+1)^{n+1}}\Big),$$

  alors que la formule de Leibniz conduirait à une somme de $n+1$ termes.

- *Sommes télescopiques.* On a $\frac{1}{X(X+1)(X+2)} = \frac{1}{2X} - \frac{1}{X+1} + \frac{1}{2(X+2)}$, ce que donne la proposition 23 pour les trois pôles simples. En regroupant $\frac{1}{2}\big(\frac{1}{k} - \frac{1}{k+1}\big) - \frac{1}{2}\big(\frac{1}{k+1} - \frac{1}{k+2}\big)$ et en télescopant, comme au chapitre 3 :

$$\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{1}{2(n+1)(n+2)},$$

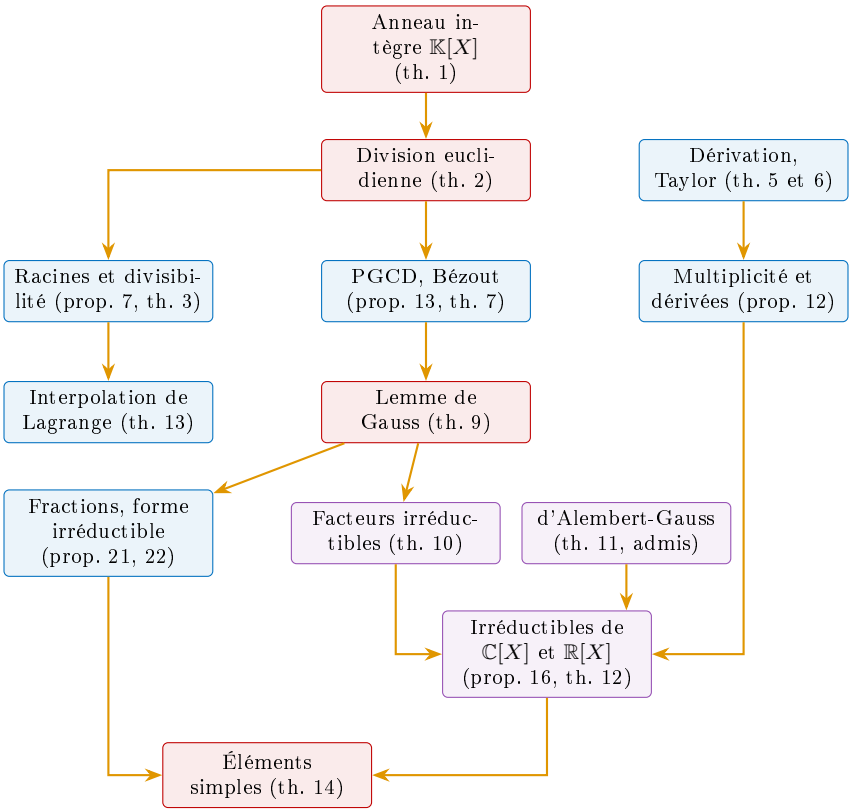
  qui tend vers $\frac{1}{4}$.



La fraction $\frac{X^3}{X^2-1} = X + \frac{1}{2(X-1)} + \frac{1}{2(X+1)}$ se lit sur sa courbe : la partie entière X donne l'asymptote oblique orange, et chaque partie polaire donne une asymptote verticale en un pôle, où la fonction change de signe parce que le pôle est simple.

13.11 Bilan

Tout le chapitre repose sur deux outils : la division euclidienne, qui fonde l'arithmétique, et l'évaluation, qui relie les racines à la divisibilité. Le schéma montre l'enchaînement des résultats ; une flèche signifie « sert à démontrer ».



Les boîtes rouges sont les résultats structurels, les boîtes violettes ceux qui dépendent du corps : seule la factorisation sur $\mathbb{R}$ et sur $\mathbb{C}$ fait appel au théorème de d'Alembert-Gauss, que l'on admet, et à la proposition 12, qui donne la même multiplicité à deux racines conjuguées. Le tableau compare l'arithmétique des entiers et celle des polynômes.

Notion	Dans $\mathbb{Z}$ (chapitre 12)	Dans $\mathbb{K}[X]$
taille	valeur absolue $\lvert b\rvert$	degré $\deg B$
division euclidienne	$0 \leqslant r < b$	$\deg R < \deg B$
inversibles	± 1	constantes non nulles
représentant normalisé	entier positif	polynôme unitaire
PGCD	$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$	$A\,\mathbb{K}[X] + B\,\mathbb{K}[X] = (A \wedge B)\,\mathbb{K}[X]$
éléments indécomposables	nombres premiers	polynômes irréductibles
décomposition	théorème 6 du chapitre 12	théorème 10
corps des fractions	$\mathbb{Q}$	$\mathbb{K}(X)$

Le chapitre 14 donnera à $\mathbb{K}_n[X]$ sa structure d'espace vectoriel, dont les polynômes de Lagrange formeront une base ; le chapitre 18 intégrera les fractions rationnelles sur un segment, grâce à leur décomposition en éléments simples.