ARITHMÉTIQUE DES POLYNÔMES ET FRACTIONS RATIONNELLES

Dans tout ce chapitre, $\mathbb{K}$ est l'un des corps $\mathbb{R}$ ou $\mathbb{C}$. Les preuves qui ressemblent très fort à celles du chapitre « Arithmétique des entiers relatifs » seront souvent omises.

1 FACTORISATION IRRÉDUCTIBLE SUR $\mathbb{R}$ OU $\mathbb{C}$

1.1 LE THÉORÈME DE D'ALEMBERT-GAUSS

Tout polynôme possède-t-il une racine ? Question essentielle s'il en est, mais à laquelle nous n'avons encore jamais répondu. La réponse affirmative suivante est un théorème majeur des mathématiques.

Théorème **(Théorème de d'Alembert-Gauss)**
Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine **COMPLEXE**.

Démonstration Hors programme, mais les curieux trouveront une preuve en fin de chapitre. ■

✖ **ATTENTION !** ✖ Le théorème est faux dans $\mathbb{R}[X]$. Le polynôme X^2+1, par exemple, n'a pas de racine **RÉELLE**.

1.2 POLYNÔMES IRRÉDUCTIBLES ET FACTORISATION IRRÉDUCTIBLE SUR $\mathbb{R}$ OU $\mathbb{C}$

Définition **(Polynôme irréductible)** Soit $P \in \mathbb{K}[X]$. On dit que P est *irréductible* (*sur* $\mathbb{K}$) si P n'est **PAS CONSTANT** et si ses seuls diviseurs sont 1 et P à constante multiplicative non nulle près.

✖ **ATTENTION !** ✖ La précision « irréductible **SUR** $\mathbb{K}$ » n'est pas superflue. Le polynôme X^2+1 n'est pas irréductible sur $\mathbb{C}$ car : $X^2+1=(X+\mathrm{i})(X-\mathrm{i})$, mais nous allons voir dans un instant qu'il l'est sur $\mathbb{R}$.

Exemple Tout polynôme de degré 1 est irréductible.

Démonstration Soit $P \in \mathbb{K}[X]$ de degré 1. Soient D un diviseur de P et $A \in \mathbb{K}[X]$ tel que : $P=AD$. Comme A est non nul : $\deg(A) \geqslant 0$, donc : $\deg(D) \leqslant \deg(P)$. Ainsi D est de degré 0 ou 1.

— Si : $\deg(D)=0$, D est constant non nul.

— Si : $\deg(D)=1$, alors : $\deg(A)=0$, i.e. A est constant non nul a. Aussitôt D s'écrit : $D=\dfrac{1}{a}P$.

Comme voulu, P est irréductible sur $\mathbb{K}$.

Le résultat suivant est un théorème d'**EXISTENCE** facile à démontrer. Il montre que les polynômes irréductibles sont l'analogue polynomial des nombres premiers dans $\mathbb{Z}$ et des particules élémentaires en physique. Tout polynôme peut être cassé en petits morceaux que l'on ne peut pas casser davantage. Nous aurons plus tard un théorème d'**UNICITÉ**.

Théorème **(Existence de la factorisation irréductible)** Tout polynôme non constant de $\mathbb{K}[X]$ est un produit de polynômes irréductibles sur $\mathbb{K}$.

✌ **Explication** ✌ Dans cet énoncé lapidaire, on considère les polynômes constants non nuls comme le produit de 0 polynôme irréductible et tout polynôme irréductible comme le produit d'1 polynôme irréductible — soi-même.

Démonstration Par récurrence forte sur le degré.

- **Initialisation :** Les polynômes de degré 1 sont irréductibles, tout simplement.
- **Hérédité :** Soit $n \geqslant 2$. Faisons l'hypothèse que tout polynôme non nul de $\mathbb{K}[X]$ de degré strictement inférieur à n est un produit de polynômes irréductibles sur $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ non nul de degré n. Deux cas possibles — soit P est irréductible, soit il ne l'est pas. Si P est irréductible, c'est terminé, il est produit de polynômes irréductibles. Dans le cas contraire : $P = AB$ pour certains $A, B \in \mathbb{K}[X]$ non constants — donc de degrés strictement inférieurs à n. Par hypothèse de récurrence, A et B sont des produits de polynômes irréductibles sur $\mathbb{K}$, donc P aussi par produit. ■

Il nous reste bien sûr à comprendre ce que sont concrètement les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Nous avons vu que les polynômes de degré 1 le sont de toute façon. Ce qui est plus étonnant, c'est que la réciproque est vraie pour $\mathbb{K} = \mathbb{C}$ — autre manière d'énoncer le théorème de d'Alembert-Gauss.

Théorème (Polynômes irréductibles de $\mathbb{C}[X]$ et unicité de la factorisation irréductible sur $\mathbb{C}$)

(i) Les irréductibles de $\mathbb{C}[X]$ sont exactement ses polynômes de degré 1.

(ii) Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$. La factorisation irréductible d'un polynôme non constant de $\mathbb{C}[X]$ coïncide donc avec sa forme scindée — elle est unique en particulier.

Démonstration

(i) Soit $P \in \mathbb{C}[X]$ irréductible. Non constant, P possède une racine $\lambda \in \mathbb{C}$ d'après le théorème de d'Alembert-Gauss, donc $X - \lambda$ divise P. L'irréductibilité de P sur $\mathbb{C}$ montre alors que P et $X - \lambda$ sont associés, donc que P est de degré 1. La réciproque a été traitée à l'instant comme un exemple.

(ii) découle de (i) et de la seule existence d'une factorisation irréductible. ■

Que dire à présent des irréductibles de $\mathbb{R}[X]$? La situation reste assez simple, mais elle l'est moins que sur $\mathbb{C}$.

Exemple Tout polynôme de $\mathbb{R}[X]$ de degré 2 SANS RACINE RÉELLE est irréductible sur $\mathbb{R}$ — par exemple $X^2 + 1$.

Démonstration Soit $P \in \mathbb{R}[X]$ de degré 2 sans racine réelle. Soient D un diviseur de P et $A \in \mathbb{R}[X]$ tel que : $P = AD$. Comme A est non nul : $\deg(A) \geqslant 0$, donc : $\deg(D) \leqslant \deg(P)$. Ainsi D est de degré 0, 1 ou 2.

— Si : $\deg(D) = 0$, D est constant non nul.

— Si : $\deg(D) = 2$, alors : $\deg(A) = 0$, i.e. A est constant non nul a. Aussitôt D s'écrit : $D = \dfrac{1}{a} P$.

— Enfin, D peut-il être de degré 1 ? Si c'était le cas, D serait de la forme $aX + b$ pour certains $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, donc $-\dfrac{b}{a}$ serait racine de P mais c'est contraire à nos hypothèses.

Comme voulu, P est irréductible sur $\mathbb{R}$.

Théorème (Polynômes irréductibles de $\mathbb{R}[X]$ et unicité de la factorisation irréductible sur $\mathbb{R}$)

(i) Les irréductibles de $\mathbb{R}[X]$ sont exactement ses polynômes de degré 1 et ses polynômes de degré 2 à discriminant strictement négatif, i.e. sans racine réelle.

(ii) La factorisation irréductible d'un polynôme non constant de $\mathbb{R}[X]$ est unique. Elle est précisément de la forme :

$$A \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \times \prod_{j=1}^{s} \left(X^2 + b_j X + c_j\right)^{n_j}$$

avec :
— A pour coefficient dominant,
— $\lambda_1, \dots, \lambda_r$ pour racines réelles distinctes de multiplicités respectives $m_1, \dots, m_r$,
— des polynômes $X^2 + b_j X + c_j$ distincts et irréductibles sur $\mathbb{R}$ pour tout $j \in [\![1, s]\!]$, et $n_j \in \mathbb{N}^*$.

Démonstration

(i) Soit $P \in \mathbb{R}[X]$ irréductible. Non constant, P possède une racine λ COMPLEXE d'après le théorème de d'Alembert-Gauss et nous savons alors, P étant à coefficients réels, que $\overline{\lambda}$ aussi est racine de P.

- Si : $\lambda \in \mathbb{R}$, $X - \lambda$ divise P dans $\mathbb{R}[X]$, or P est irréductible sur $\mathbb{R}$, donc P et $X - \lambda$ sont associés et P est de degré 1.

- Si : $\lambda \notin \mathbb{R}$, alors : $\overline{\lambda} \neq \lambda$, donc : $P = (X-\lambda)\big(X-\overline{\lambda}\big)Q$ pour un certain $Q \in \mathbb{C}[X]$, mais si on développe : $P = \Big(\underbrace{X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2}_{\in \mathbb{R}[X]}\Big)Q$, donc en réalité Q est à coefficients **RÉELS** par unicité de la division euclidienne dans $\mathbb{C}[X]$. De là, P étant irréductible sur $\mathbb{R}$, P et $X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$ sont associés et P est de degré 2. En outre, enfin, P est bien sans racine réelle.

(ii) Soit $P \in \mathbb{R}[X]$ non constant. Nous savons que P est scindé **SUR** $\mathbb{C}$, mais aussi, parce qu'il est à coefficients **RÉELS**, que ses racines non réelles peuvent être regroupées par paires de conjuguées de mêmes multiplicités. Comme en (i), le regroupement de termes $X-\lambda$ et $X-\overline{\lambda}$ donne un terme $X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$ irréductible. Pour finir, cette factorisation irréductible sur $\mathbb{R}$ est unique, car si elle ne l'était pas, P aurait plusieurs formes scindées sur $\mathbb{C}$ — ce que nous savons être faux. ■

✎ **En pratique** ✎ La factorisation irréductible sur $\mathbb{R}$ se calcule à partir de la factorisation irréductible sur $\mathbb{C}$ par regroupement des racines non réelles par paires de conjuguées.

Exemple La factorisation irréductible de X^4+16 sur $\mathbb{C}$ est : $X^4 + 16 = \big(X - 2\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}\big)\big(X - 2\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}\big)\big(X - 2\mathrm{e}^{-\frac{3\mathrm{i}\pi}{4}}\big)\big(X - 2\mathrm{e}^{\frac{3\mathrm{i}\pi}{4}}\big)$.
Quant à sa factorisation irréductible sur $\mathbb{R}$: $X^4 + 16 = \big(X^2 - 2\sqrt{2}X + 4\big)\big(X^2 + 2\sqrt{2}X + 4\big)$.

Démonstration

- **Factorisation irréductible sur $\mathbb{C}$:** Qui sont les racines complexes de X^4+16 ? Pour tout $r \in \mathbb{C}$:
$$r^4 + 16 = 0 \iff r^4 = -16 = \Big(2\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}\Big)^4 \iff \exists\, k \in [\![0,3]\!],\quad r = 2\mathrm{e}^{\frac{\mathrm{i}\pi}{4} + \frac{2\mathrm{i}k\pi}{4}}.$$
Les racines de X^4+16 sont donc : $2\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}$ $(k=0)$, $2\mathrm{e}^{\frac{3\mathrm{i}\pi}{4}}$ $(k=1)$, $2\mathrm{e}^{-\frac{3\mathrm{i}\pi}{4}}$ $(k=2)$ et $2\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}$ $(k=3)$. La factorisation irréductible de X^4+16 sur $\mathbb{C}$ en découle — avec ici que des racines simples.
- **Factorisation irréductible sur $\mathbb{R}$:** Il nous reste à regrouper les racines par paires de conjuguées.
$$\big(X - 2\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}\big)\big(X - 2\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}\big) = X^2 - 2\Big(\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}} + \mathrm{e}^{\frac{\mathrm{i}\pi}{4}}\Big)X + 4 = X^2 - 4\cos\frac{\pi}{4} \times X + 4 = X^2 - 2\sqrt{2}X + 4$$
et $$\big(X - 2\mathrm{e}^{-\frac{3\mathrm{i}\pi}{4}}\big)\big(X - 2\mathrm{e}^{\frac{3\mathrm{i}\pi}{4}}\big) = X^2 - 2\Big(\mathrm{e}^{-\frac{3\mathrm{i}\pi}{4}} + \mathrm{e}^{\frac{3\mathrm{i}\pi}{4}}\Big)X + 4 = X^2 - 4\cos\frac{3\pi}{4} \times X + 4 = X^2 + 2\sqrt{2}X + 4.$$

2 PGCD, PPCM

Définition (Diviseur/multiple commun) Soient $A_1, \dots, A_r \in \mathbb{K}[X]$.

- On appelle *diviseur commun de* $A_1, \dots, A_r$ tout polynôme de $\mathbb{K}[X]$ qui divise à la fois $A_1, \dots, A_r$.
- On appelle *multiple commun de* $A_1, \dots, A_r$ tout polynôme de $\mathbb{K}[X]$ divisible à la fois par $A_1, \dots, A_r$.

2.1 PGCD DE DEUX POLYNÔMES

Définition-théorème (PGCD de deux polynômes)

- Soient $A, B \in \mathbb{K}[X]$ avec : $A \neq 0$ ou $B \neq 0$. On appelle *plus grand commun diviseur* (ou *PGCD*) *de A et B* tout diviseur commun de A et B de degré maximal.
- On convient que 0 est le seul PGCD de 0 et 0.

Démonstration Pour justifier l'existence d'un PGCD dans le cas où : $A \neq 0$, remarquons simplement que l'ensemble des **DEGRÉS** des diviseurs communs non nuls de A et B contient 0 — car A et B sont divisibles par 1 — et qu'il est majoré par $\deg(A)$. Cet ensemble est donc une partie non vide majorée de $\mathbb{N}$, donc possède un plus grand élément. ■

Exemple Pour tout $A \in \mathbb{K}[X]$, les PGCD de A et 0 sont exactement les associés de A.

Démonstration Si : $A \neq 0$, les diviseurs communs de A et 0 sont exactement les diviseurs de A et les diviseurs de A de degré maximal sont exactement ses associés.

Théorème (Idée fondamentale de l'algorithme d'Euclide) Pour tous $A, B, K \in \mathbb{K}[X]$, $A+BK$ et B ont les mêmes diviseurs communs que A et B, et donc aussi les mêmes PGCD.

Explication En particulier, pour tous $A, B \in \mathbb{K}[X]$ avec : $B \neq 0$, en notant R le reste de la division euclidienne de A par B, B et R ont les mêmes diviseurs communs que A et B.

Démonstration Tout diviseur commun de A et B divise aussi $A+BK$ et B, et inversement, tout diviseur commun de $A+BK$ et B divise aussi $A = (A+BK)-BK$ et B. ■

Théorème (« Unicité » du PGCD de deux polynômes, diviseurs communs et diviseurs du PGCD) Soient $A, B \in \mathbb{K}[X]$.

- Les PGCD de A et B sont associés. Un seul d'entre eux est donc unitaire — ou nul si : $A = B = 0$ — on l'appelle LE *PGCD de A et B* et on le note $A \wedge B$.
- Les diviseurs communs de A et B sont exactement les diviseurs de $A \wedge B$.

Démonstration Nous allons mettre en œuvre dans cette preuve un algorithme de calcul du PGCD qu'on appelle l'*algorithme d'Euclide*. Soient $A, B \in \mathbb{K}[X]$. On peut supposer que : $\deg(B) \leqslant \deg(A)$ sans perte de généralité. On définit une suite de polynômes $R_0, R_1, R_2 \ldots$ de la manière suivante.

— Au départ, on pose : $R_0 = A$ et $R_1 = B$.

— Ensuite, pour $k \in \mathbb{N}$, TANT QUE : $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} — en particulier : $\deg(R_{k+2}) < \deg(R_{k+1})$.

À l'issue de cette construction : $\deg(R_0) \geqslant \deg(R_1) > \deg(R_2) > \ldots$, et comme il n'existe qu'un nombre FINI d'entiers naturels entre 0 et $\deg(R_0)$, on obtient forcément : $\deg(R_N) = -\infty$ pour un certain $N \in \mathbb{N}^*$, i.e. : $R_N = 0$ — l'algorithme se termine. Or, en vertu de l'idée fondamentale de l'algorithme d'Euclide, $A = R_0$ et $B = R_1$ ont les mêmes diviseurs communs et les mêmes PGCD que R_1 et R_2, puis que R_2 et $R_3 \ldots$ et enfin que R_{N-1} et $R_N = 0$. Les PGCD de R_{N-1} et 0 étant exactement les associés de R_{N-1}, les diviseurs communs de A et B sont ainsi exactement les diviseurs de R_{N-1} et leurs PGCD sont exactement les associés de R_{N-1}. En particulier, les PGCD de A et B sont associés. ■

En pratique **(Algorithme d'Euclide)** Comme on vient de le voir, l'*algorithme d'Euclide* est un algorithme de calcul du PGCD de deux polynômes. Il a été montré en particulier que : $A \wedge B = R_{N-1}$ où R_{N-1} est le dernier polynôme non nul de la liste $R_0, R_1, R_2 \ldots$ On retiendra ceci :

À une constante multiplicative près, $A \wedge B$ est le DERNIER RESTE NON NUL de la suite des restes successifs $R_0, R_1, R_2 \ldots$

Exemple On peut vérifier grâce à l'algorithme d'Euclide que : $(X+1)^3 \wedge (X+1)^2(X+2) = (X+1)^2$.

Si vous aimez les calculs : $\left(2X^4+9X^3+12X^2+10X+3\right) \wedge \left(2X^4+X^3-2X^2+3X+2\right) = X + \frac{1}{2}$.

Théorème (Relations de Bézout pour deux polynômes) Soient $A, B \in \mathbb{K}[X]$. Il existe des polynômes $U, V \in \mathbb{K}[X]$ pour lesquels : $A \wedge B = AU + BV$. Une telle relation est appelée UNE *relation de Bézout de A et B*.

ATTENTION ! Les polynômes U et V ne sont pas du tout uniques.

Démonstration On l'a vu précédemment, on peut toujours se ramener au cas où : $\deg(B) \leqslant \deg(A)$. On reprend dans cette preuve les restes successifs de l'algorithme d'Euclide en posant : $R_0 = A$ et $R_1 = B$ et en notant pour tout $k \in \mathbb{N}$, tant que : $R_{k+1} \neq 0$, R_{k+2} le reste de la division euclidienne de R_k par R_{k+1}. Le quotient de cette division euclidienne sera quant à lui noté Q_{k+2} : $R_{k+2} = R_k - Q_{k+2}R_{k+1}$. La suite ainsi construite est finie de rang final N pour lequel : $R_N = 0$.

On définit deux nouvelles suites $(U_k)_{0\leqslant k\leqslant N}$ et $(V_k)_{0\leqslant k\leqslant N}$ par : $(U_0,V_0)=(1,0)$, $(U_1,V_1)=(0,1)$ et pour tout $k\in[\![0,N-1]\!]$: $\big(U_{k+1},V_{k+1}\big)=\big(U_k-Q_{k+2}U_{k+1},V_k-Q_{k+2}V_{k+1}\big)$. Il n'est alors pas dur de voir par récurrence double que pour tout $k\in[\![0,N]\!]$: $R_k=AU_k+BV_k$. En particulier : $A\wedge B=R_{N-1}=AU_{N-1}+BV_{N-1}$. ■

✎ **En pratique** ✎ **(Algorithme d'Euclide étendu)** Le principe de l'algorithme est le même qu'au chapitre « Arithmétique des entiers relatifs » et je ne re-détaillerai pas ici. Cherchons par exemple le PGCD de : $A=6X^4+8X^3-7X^2-5X-2$ et $B=6X^3-4X^2-X-1$ ainsi qu'une relation de Bézout associée.

k	R_k	Q_k	U_k	V_k
0	$6X^4+8X^3-7X^2-5X-2$		1	0
1	$6X^3-4X^2-X-1$		0	1
2	$2X^2-2X$	$X+2$	1	$-X-2$
3	$X-1$	$3X+1$	$-3X-1$	$3X^2+7X+3$

Relation de Bézout :

$$\begin{aligned}A\wedge B&=X-1\\&=-(3X+1)\times A+\big(3X^2+7X+3\big)\times B.\end{aligned}$$

Théorème **(Propriétés du PGCD de deux polynômes)** Soient $A,B,C,K\in\mathbb{K}[X]$.

(i) **Associativité :** $(A\wedge B)\wedge C=A\wedge(B\wedge C)$.

(ii) **Factorisation par un diviseur commun :** $(AK)\wedge(BK)$ et $K(A\wedge B)$ sont associés.

✎ **En pratique** ✎ Quand on connaît la factorisation irréductible de deux polynômes A et B, on peut déterminer $A\wedge B$ sans utiliser l'algorithme de Bézout. Le principe est le même que dans $\mathbb{Z}$.

Exemple $\big(2X(X+1)^2(X+2)^3\big)\wedge\big(X(X+2)^4\big(X^2+1\big)\big)=X(X+2)^3$.

2.2 PGCD d'une famille finie de polynômes

Définition-théorème **(PGCD d'une famille finie de polynômes)**

- Soient $A_1,\dots,A_r\in\mathbb{K}[X]$ des polynômes dont l'un au moins est non nul. On appelle *plus grand commun diviseur* (ou *PGCD*) *de* $A_1,\dots,A_r$ tout diviseur commun de $A_1,\dots,A_r$ de degré maximal.

  On peut montrer que les PGCD de $A_1,\dots,A_r$ sont associés. Un seul d'entre eux est donc unitaire — ou nul si : $A_1=\dots=A_r=0$ — on l'appelle LE *PGCD de* $A_1,\dots,A_r$ et on le note $A_1\wedge\dots\wedge A_r$.
- On pose enfin pour tout $r\geqslant 2$: $\underbrace{0\wedge\dots\wedge 0}_{r\text{ fois}}=0$.

✎ **En pratique** ✎ Comme dans le cas des entiers, le calcul du PGCD d'une famille finie de polynômes peut être ramené à des calculs de PGCD de deux polynômes. Par exemple :

$$\big(X^3+4X^2+5X+2\big)\wedge\big(X^3+4X^2+4X\big)\wedge\big(X^2-4\big)=(X+2)\wedge\big(X^2-4\big)=X+2.$$

Théorème **(Reprise des résultats précédents dans le cas d'une famille finie de polynômes)** Soient $A_1,\dots,A_r\in\mathbb{K}[X]$.

- Les diviseurs communs de $A_1,\dots,A_r$ sont exactement les diviseurs de $A_1\wedge\dots\wedge A_r$.
- Pour tout $K\in\mathbb{K}[X]$: $(A_1K)\wedge\dots(A_rK)$ et $K(A_1\wedge\dots\wedge A_r)$ sont associés.
- Il existe des polynômes $U_1,\dots,U_r\in\mathbb{K}[X]$ pour lesquels : $A_1\wedge\dots\wedge A_r=A_1U_1+\dots+A_rU_r$. Une telle relation est appelée UNE *relation de Bézout de* $A_1,\dots,A_r$.

2.3 Polynômes premiers entre eux

Définition **(Polynômes premiers entre eux, cas de deux polynômes)** Soient $A,B\in\mathbb{K}[X]$. On dit que A et B sont *premiers entre eux* si 1 est leur seul diviseur commun unitaire, i.e. si : $A\wedge B=1$.

Définition **(Polynômes premiers entre eux dans leur ensemble/deux à deux)** Soient $A_1,\dots,A_r\in\mathbb{K}[X]$.

- On dit que $A_1,\dots,A_r$ sont *premiers entre eux dans leur ensemble* si 1 est leur seul diviseur commun unitaire, i.e. si : $A_1\wedge\dots\wedge A_r=1$.
- On dit que $A_1,\dots,A_r$ sont *premiers entre eux deux à deux* si A_i et A_j sont premiers entre eux pour tous $i,j\in[\![1,r]\!]$ distincts.

✖ **Attention !** ✖ Premiers entre eux **deux à deux** $\Longrightarrow$ Premiers entre eux **dans leur ensemble** mais **la réciproque est fausse !** Par exemple, $X(X+1)$, $X(X+2)$ et $(X+1)(X+2)$ sont premiers entre eux dans leur ensemble **mais :** $X(X+1)\wedge X(X+2)=X\neq 1$, $X(X+2)\wedge(X+1)(X+2)=X+2\neq 1$ et $(X+1)(X+2)\wedge X(X+1)=X+1\neq 1$.

Théorème **(Théorème de Bézout)** Soient $A,B\in\mathbb{K}[X]$. Les assertions suivantes sont équivalentes :

(i) $A\wedge B=1$. (ii) Il existe deux polynômes $U,V\in\mathbb{K}[X]$ tels que $AU+BV=1$.

Théorème **(Théorème de Gauss)** Soient $A,B,C\in\mathbb{K}[X]$. Si : $A|BC$ et si : $A\wedge B=1$, alors : $A|C$.

Théorème **(Polynômes premiers entre eux et produit de polynômes)** Soient $P,A_1,\dots,A_r\in\mathbb{K}[X]$.

(i) Si chacun des polynômes $A_1,\dots,A_r$ est premier avec P, leur produit $A_1\dots A_r$ l'est aussi.

(ii) Si $A_1,\dots,A_r$ divisent P et sont premiers entre eux **deux à deux**, leur produit $A_1\dots A_r$ divise P.

2.4 PPCM de deux polynômes

Définition **(PPCM de deux polynômes)** Soient $A,B\in\mathbb{K}[X]$. On appelle *plus petit commun multiple* (ou *PPCM*) *de A et B* tout polynôme $M\in\mathbb{K}[X]$ satisfaisant les deux assertions :

— M est un multiple commun de A et B, — M divise tout multiple commun de A et B.

Théorème **(Existence du PPCM et lien avec le PGCD)** Soient $A,B\in\mathbb{K}[X]$.

- **Existence et « unicité » :** Les polynômes A et B possèdent un unique PPCM **unitaire ou nul** appelé **le** PPCM de A et B et noté $A\vee B$, et leurs autres PPCM sont les associés de $A\vee B$, i.e. les polynômes $\lambda(A\vee B)$, λ décrivant $\mathbb{K}^*$.
- **Lien avec le PGCD :** Les polynômes AB et $(A\wedge B)(A\vee B)$ sont associés.

✎ **En pratique** ✎ Quand on connaît la factorisation irréductible de deux polynômes A et B, on peut déterminer $A\vee B$ sans utiliser l'algorithme de Bézout. Le principe est le même que dans $\mathbb{Z}$.

Exemple $\left(3X^2(X+1)\right)\vee\left(X^4(X+2)^2\right)=X^4(X+1)(X+2)^2$.

3 Fractions rationnelles

Nous avons déjà parlé informellement des fractions rationnelles en début d'année au chapitre « Introduction à la décomposition en éléments simples », mais nous ne connaissions alors pas la notion de polynôme formel et tous nos résultats étaient admis. Nous sommes à présent en mesure de les fonder proprement.

3.1 Construction des fractions rationnelles

Définition (Ensemble $\mathbb{K}(X)$) On construit dans la preuve ci-dessous un ensemble $\mathbb{K}(X)$ satisfaisant les trois assertions suivantes :

— À tout couple $(A,B)\in\mathbb{K}[X]^2$ tel que $B\neq 0$, on peut associer un unique élément de $\mathbb{K}(X)$ noté $\dfrac{A}{B}$.

— Tout élément de $\mathbb{K}(X)$ peut être écrit sous la forme $\dfrac{A}{B}$ pour certains $A,B\in\mathbb{K}[X]$ avec : $B\neq 0$.

— Pour tous $(A,B),(C,D)\in\mathbb{K}[X]^2$, si : $B\neq 0$ et $D\neq 0$, alors : $\dfrac{A}{B}=\dfrac{C}{D}\iff AD=BC$.

Les éléments de $\mathbb{K}(X)$ sont appelés les *fractions rationnelles à coefficients dans* $\mathbb{K}$.

Démonstration Notons $\mathscr{F}$ l'ensemble $\mathbb{K}[X]\times\big(\mathbb{K}[X]\setminus\{0\}\big)$. On définit sur $\mathscr{F}$ une relation binaire $\sim$ de la manière suivante — pour tous $(A,B),(C,D)\in\mathscr{F}$: $(A,B)\sim(C,D)\iff AD=BC$. Il se trouve alors que cette relation $\sim$ est une relation d'équivalence.

- **Réflexivité :** Pour tout $(A,B)\in\mathscr{F}$: $AB=AB$ donc : $(A,B)\sim(A,B)$.
- **Transitivité :** Soient $(A,B),(C,D),(E,F)\in\mathscr{F}$ pour lesquels : $(A,B)\sim(C,D)$ et $(C,D)\sim(E,F)$. Aussitôt : $AD=BC$ et $CF=DE$, donc : $ADF=BCF=BDE$. Or $\mathbb{K}[X]$ est intègre et : $D\neq 0$, donc : $AF=BE$, i.e. : $(A,B)\sim(E,F)$.
- **Symétrie :** Pour tous $(A,B),(C,D)\in\mathscr{F}$, si : $(A,B)\sim(C,D)$, alors : $AD=BC$, donc aussi : $CB=DA$, i.e. : $(C,D)\sim(A,B)$.

Notons à présent $\mathbb{K}(X)$ l'ensemble quotient de $\mathscr{F}$ par $\sim$ et, pour tout $(A,B)\in\mathscr{F}$, $\dfrac{A}{B}$ la classe d'équivalence de (A,B) associée. L'ensemble ainsi construit satisfait par définition toutes les propriétés désirées. Remarquez bien pour finir que la notation « fraction » n'est qu'une NOTATION pour désigner une classe d'équivalence ! — mais à vrai dire, c'est une remarque que vous pouvez oublier. ■

Exemple Dans $\mathbb{R}(X)$, les fractions $\dfrac{1}{X}$ et $\dfrac{X+1}{X(X+1)}$ sont égales car : $1\times X(X+1)=X\times(X+1)$.

Définition (Structure de corps sur $\mathbb{K}(X)$) On munit $\mathbb{K}(X)$ de deux lois internes $+$ et $\times$ qui en font un corps en posant, pour tous $(A,B),(C,D)\in\mathbb{K}[X]^2$, si : $B\neq 0$ et $D\neq 0$, alors :

$$\frac{A}{B}+\frac{C}{D}=\frac{AD+BC}{BD}\qquad\text{et}\qquad\frac{A}{B}\times\frac{C}{D}=\frac{AC}{BD},$$

définitions possibles car les fractions $\dfrac{AD+BC}{BD}$ et $\dfrac{AC}{BD}$ dépendent de $\dfrac{A}{B}$ et $\dfrac{C}{D}$ sans dépendre du choix de (A,B) et (C,D).

Démonstration Soient $A,B,C,D,E,F\in\mathbb{K}[X]$, si : $B\neq 0$, $D\neq 0$ et $F\neq 0$, alors :

- **Bonne définition de $+$ et $\times$:** Pourquoi d'abord y a-t-il un problème de définition ? Les fractions $\dfrac{A}{B}$ et $\dfrac{C}{D}$ sont définies à l'aide de quatre polynômes précis A,B,C,D, mais une fraction a plein d'écritures possibles, disons : $\dfrac{A}{B}=\dfrac{\widetilde{A}}{\widetilde{B}}$ et $\dfrac{C}{D}=\dfrac{\widetilde{C}}{\widetilde{D}}$ avec $\widetilde{A},\widetilde{B},\widetilde{C},\widetilde{D}\in\mathbb{K}[X]$ et : $\widetilde{B}\neq 0$ et $\widetilde{D}\neq 0$. Si nous voulons

que les définitions de $+$ et $\times$ aient un sens, nous devons nous assurer que les deux égalités suivantes sont vraies : $\dfrac{AD+BC}{BD}=\dfrac{\widetilde{A}\widetilde{D}+\widetilde{B}\widetilde{C}}{\widetilde{B}\widetilde{D}}$ et $\dfrac{AC}{BD}=\dfrac{\widetilde{A}\widetilde{C}}{\widetilde{B}\widetilde{D}}$. Or par définition de $\sim$:

$$AC\times\widetilde{B}\widetilde{D}=A\widetilde{B}\times C\widetilde{D}=B\widetilde{A}\times D\widetilde{C}=BD\times\widetilde{A}\widetilde{C}$$

et : $(AD+BC)\times\widetilde{B}\widetilde{D}=A\widetilde{B}\times D\widetilde{D}+B\widetilde{B}\times C\widetilde{D}=B\widetilde{A}\times D\widetilde{D}+B\widetilde{B}\times D\widetilde{C}=BD\times\left(\widetilde{A}\widetilde{D}+\widetilde{B}\widetilde{C}\right)$.

- **Commutativité de $+$:** $\dfrac{A}{B}+\dfrac{C}{D}=\dfrac{AD+BC}{BD}=\dfrac{CB+DA}{DB}=\dfrac{C}{D}+\dfrac{A}{B}$.
- **Associativité de $+$:** $\left(\dfrac{A}{B}+\dfrac{C}{D}\right)+\dfrac{E}{F}=\dfrac{AD+BC}{BD}+\dfrac{E}{F}=\dfrac{(AD+BC)F+(BD)E}{(BD)F}$

$$=\frac{A(DF)+B(CF+DE)}{B(DF)}=\frac{A}{B}+\frac{CF+DE}{DF}=\frac{A}{B}+\left(\frac{C}{D}+\frac{E}{F}\right).$$

- **Neutralité de $\dfrac{0}{1}$ pour $+$:** $\dfrac{A}{B}+\dfrac{0}{1}=\dfrac{A\times1+B\times0}{B\times1}=\dfrac{A}{B}$ et de même $\dfrac{0}{1}+\dfrac{A}{B}=\dfrac{A}{B}$.
- **Inverses pour $+$:** $\dfrac{A}{B}+\dfrac{-A}{B}=\dfrac{AB+B(-A)}{B^2}=\dfrac{0}{B^2}=\dfrac{0}{1}$ et de même $\dfrac{-A}{B}+\dfrac{A}{B}=\dfrac{0}{1}$.
- À ce stade, $\left(\mathbb{K}(X),+\right)$ est un groupe commutatif d'élément neutre $\dfrac{0}{1}$. Pour montrer que $\left(\mathbb{K}(X),+,\times\right)$ est un anneau, on peut montrer de même que $\left(\mathbb{K}(X),\times\right)$ est un magma associatif d'élément neutre $\dfrac{1}{1}$ et que $\times$ est distributive sur $+$. Enfin, pour montrer que $\left(\mathbb{K}(X),+,\times\right)$ est un corps, on peut montrer que $\times$ est commutative et que toute fraction non nulle $\dfrac{A}{B}$ admet un inverse, en l'occurrence $\dfrac{B}{A}$. ■

Théorème (Les polynômes sont des fractions rationnelles) On identifie tout polynôme $P\in\mathbb{K}[X]$ à la fraction rationnelle $\dfrac{P}{1}$. Cette identification fait de $\mathbb{K}[X]$ un sous-anneau de $\mathbb{K}(X)$.

Démonstration

- **Pseudo-inclusion :** L'application $P\longmapsto\dfrac{P}{1}$ est injective de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$ car pour tous $P,Q\in\mathbb{K}[X]$, si : $\dfrac{P}{1}=\dfrac{Q}{1}$, alors : $P=P\times1=1\times Q=Q$. On peut donc voir $\mathbb{K}[X]$ comme une partie de $\mathbb{K}(X)$.
- **Cohérence des notations $+$ et $\times$:** Soient $P,Q\in\mathbb{K}[X]$. C'est bien beau de vouloir voir P et Q comme des fractions, le problème c'est que $P+Q$ et $P\times Q$ désignent alors à la fois des objets dans $\mathbb{K}[X]$ et des objets dans $\mathbb{K}(X)$ — peut-être différents. Tout se passe pour le mieux heureusement, car :

$$\frac{P}{1}+\frac{Q}{1}=\frac{P\times1+1\times Q}{1\times1}=\frac{P+Q}{1}\qquad\text{et}\qquad\frac{P}{1}\times\frac{Q}{1}=\frac{PQ}{1\times1}=\frac{P\times Q}{1}.$$

- **Sous-anneau :** Avec notre identification : $\mathbb{K}[X]=\left\{\dfrac{P}{1}\right\}_{P\in\mathbb{K}[X]}$. En particulier : $\dfrac{1}{1}=1\in\mathbb{K}[X]$. Ensuite, $\mathbb{K}[X]$ est stable par différence et produit car pour tous $P,Q\in\mathbb{K}[X]$: $\dfrac{P}{1}-\dfrac{Q}{1}=\dfrac{P-Q}{1}\in\mathbb{K}[X]$ et $\dfrac{P}{1}\times\dfrac{Q}{1}=\dfrac{PQ}{1}\in\mathbb{K}[X]$. ■

Théorème (Structure d'espace vectoriel de $\mathbb{K}(X)$) Parce que tout élément de $\mathbb{K}$ peut être identifié à un polynôme et donc à une fraction rationnelle, on sait multiplier toute fraction rationnelle de $\mathbb{K}(X)$ par un scalaire. Cette identification fait de $\mathbb{K}(X)$ un $\mathbb{K}$-espace vectoriel.

Dans tout ce qui suit, quand nous écrirons sans préciser : $R=\dfrac{A}{B}$, il sera sous-entendu que : $(A,B)\in\mathbb{K}[X]^2$ et $B\neq0$. Les résultats qui suivent seront admis par souci d'efficacité.

Définition **(Forme irréductible d'une fraction rationnelle)** Soit $R \in \mathbb{K}(X)$. On appelle *forme irréductible de R* toute écriture de R de la forme : $R = \dfrac{A}{B}$ avec A et B premiers entre eux. Une telle écriture est toujours possible, et unique à multiplication près par des scalaires non nuls.

Exemple La fraction $\dfrac{(X^2+1)(X+1)^2}{X(X+1)}$ n'est pas irréductible, mais la fraction $\dfrac{(X^2+1)(X+1)}{X}$ l'est.

Définition **(Dérivée d'une fraction rationnelle)**

- Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$. La fraction rationnelle $\dfrac{A'B - AB'}{B^2}$ dépend de R sans dépendre du choix de (A,B). On l'appelle la *dérivée de R* et on la note R'.
- Pour tous $R, S \in \mathbb{K}(X)$: $(R+S)' = R' + S'$, $(RS)' = R'S + RS'$ et si $S \neq 0$: $\left(\dfrac{R}{S}\right)' = \dfrac{R'S - RS'}{S^2}$.
  En outre, la dérivée d'un polynôme coïncide avec sa dérivée comme fraction rationnelle.

Exemple $\displaystyle\sum_{k=0}^{+\infty} \frac{k}{7^k} = \frac{7}{36}$.

Démonstration Dérivons pour tout $n \in \mathbb{N}$ la relation : $\displaystyle\sum_{k=0}^{n} X^k = \frac{1-X^{n+1}}{1-X}$ dans $\mathbb{K}(X)$.

Cela donne : $\displaystyle\sum_{k=0}^{n} kX^{k-1} = \frac{-(n+1)X^n(1-X) + \left(1-X^{n+1}\right)}{(1-X)^2} = \frac{1 + nX^{n+1} - (n+1)X^n}{(1-X)^2}$, puis multiplions par X : $\displaystyle\sum_{k=0}^{n} kX^k = \frac{X}{(1-X)^2}\left(1 + nX^{n+1} - (n+1)X^n\right)$. Évaluons enfin en $\dfrac{1}{7}$: $\displaystyle\sum_{k=0}^{n} \frac{k}{7^k} = \frac{7}{36}\left(1 + \frac{n}{7^{n+1}} - \frac{n+1}{7^n}\right)$.
Il ne reste plus qu'à passer à la limite.

Définition **(Degré d'une fraction rationnelle)**

- Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$. La quantité $\deg(A) - \deg(B)$ dépend de R sans dépendre du choix de (A,B). On l'appelle le *degré de R* et on la note $\deg(R)$. Le degré d'une fraction rationnelle est ainsi soit un entier RELATIF, soit $-\infty$.
- Pour tous $R, S \in \mathbb{K}(X)$: $\deg(R+S) \leqslant \max\left\{\deg(R), \deg(S)\right\}$ et $\deg(RS) = \deg(R) + \deg(S)$,
  et si $\deg(R) \neq 0$: $\deg(R') = \deg(R) - 1$. En outre, le degré d'un polynôme coïncide avec son degré comme fraction rationnelle.

✖ **ATTENTION !** ✖ Seule la fraction rationnelle 0 est de degré $-\infty$, mais une fraction rationnelle peut être de degré positif sans être un polynôme. Par exemple, la fraction rationnelle $\dfrac{X^4 + X^3 + 1}{X^2 + 3}$ est de degré $4-2 = 2$ sans être un polynôme.

Définition **(Fonction rationnelle)** Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$ IRRÉDUCTIBLE. La fonction $x \longmapsto \dfrac{A(x)}{B(x)}$ définie sur $\mathbb{K}$ privé des racines de B est appelée la *fonction rationnelle associée à R* et encore notée R — définition possible car cette fonction dépend de R sans dépendre du choix de (A,B).

✌ **Explication** ✌ On impose ici à l'écriture : $R = \dfrac{A}{B}$ d'être irréductible pour que le dénominateur de R ait le moins de racines possible, et donc pour que R, comme fonction, soit définie sur le plus grand ensemble possible. Par exemple, la fonction $x \longmapsto \dfrac{x^3 + x + 1}{x - 1}$ est définie sur $\mathbb{R} \setminus \{1\}$ mais la fonction $x \longmapsto \dfrac{x\left(x^3 + x + 1\right)}{x(x-1)}$ l'est seulement sur $\mathbb{R} \setminus \{0, 1\}$.

Définition **(Zéro et pôle d'une fraction rationnelle, multiplicité)** Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$ IRRÉDUCTIBLE.

- Soit $\lambda \in \mathbb{K}$. On dit que λ est un *zéro de* R si λ est une racine de A. La multiplicité de λ dans A est alors appelée la *multiplicité de* λ *dans* R.
- Soit $\mu \in \mathbb{K}$. On dit que μ est un *pôle de* R si μ est une racine de B. La multiplicité de μ dans B est alors appelée la *multiplicité de* μ *dans* R. Un pôle de multiplicité 1 (resp. 2) est aussi appelé un pôle *simple* (resp. *double*).

Explication On impose ici à l'écriture : $R = \dfrac{A}{B}$ d'être irréductible pour qu'il ne soit pas possible de confondre les zéros et les pôles de R. Quand A et B sont premiers entre eux, il est certain en effet qu'ils n'ont pas de racine commune.

Exemple Dans $\mathbb{R}(X)$, la fraction $\dfrac{(X^2+1)(X-2)^3(X+1)X}{(X-1)^2(X^2+X+1)}$ a pour zéros les réels -1, 0 et 2 et pour pôle le seul réel 1. La multiplicité de 2 est égale à 3, celle de 1 est 2, etc.

Théorème **(Partie entière)** Soit $R = \dfrac{A}{B} \in \mathbb{K}(X)$. Il existe un unique polynôme $E \in \mathbb{K}[X]$ et une unique fraction rationnelle $Q \in \mathbb{K}(X)$ pour lesquels : $R = E + Q$ et $\deg(Q) < 0$. Le polynôme E est appelé la *partie entière de* R et n'est autre que le quotient de la division euclidienne de A par B.

Explication En particulier, la partie entière de R est nulle si : $\deg(R) < 0$.

Démonstration

- **Existence :** Notons E le quotient de la division euclidienne de A par B et F son reste, et posons : $Q = \dfrac{F}{B}$.
  Alors d'une part : $\deg(Q) = \deg(F) - \deg(B) < 0$, mais d'autre part : $R = \dfrac{A}{B} = \dfrac{EB+F}{B} = E + Q$.
- **Unicité :** Soient : $R = E + Q$ et $R = \widetilde{E} + \widetilde{Q}$ deux décompositions de R. Le POLYNÔME $E - \widetilde{E}$ est de degré : $\deg(\widetilde{Q} - Q) \leqslant \max\left\{\deg(\widetilde{Q}), \deg(Q)\right\} < 0$, donc est nul, donc : $E = \widetilde{E}$, puis : $Q = \widetilde{Q}$. ■

Exemple La partie entière de la fraction $\dfrac{X^4 - 3X^3 + 5X^2 - 1}{X^2 - 3X + 1}$ est $X^2 + 4$.

Démonstration Simple division euclidienne : $X^4 - 3X^3 + 5X^2 - 1 = (X^2 - 3X + 1)(X^2 + 4) + 12X - 5$.

3.2 DÉCOMPOSITION EN ÉLÉMENTS SIMPLES SUR $\mathbb{R}$ OU $\mathbb{C}$

Théorème **(Décomposition en éléments simples sur $\mathbb{C}$)** Soit $R \in \mathbb{C}(X)$ de partie entière E et de pôles distincts $\lambda_1, \dots, \lambda_r$ de multiplicités respectives $m_1, \dots, m_r$. Il existe une et une seule famille $(a_{ik})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant k \leqslant m_i}}$ de nombres complexes telle que :

$$R = E + \sum_{i=1}^{r} \underbrace{\sum_{k=1}^{m_i} \frac{a_{ik}}{(X-\lambda_i)^k}}_{\text{Partie polaire associée au pôle } \lambda_i}.$$

On n'oublie pas la partie entière !

Cette décomposition de R est appelée sa décomposition en éléments simples sur $\mathbb{C}$.

Démonstration Démonstration hors programme, mais il n'est pas inintéressant de comprendre l'EXISTENCE de la décomposition. Écrivons pour cela : $R = \dfrac{A}{B}$ avec $A \in \mathbb{C}[X]$ et : $B = (X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$.

- Les polynômes $\dfrac{B}{(X-\lambda_1)^{m_1}}, \dots, \dfrac{B}{(X-\lambda_r)^{m_r}}$ sont premiers entre eux dans leur ensemble, donc pour certains $U_1, \dots, U_r \in \mathbb{C}[X]$: $1 = \displaystyle\sum_{i=1}^{r} \frac{BU_i}{(X-\lambda_i)^{m_i}}$ — relation de Bézout.

- Multiplions par R : $R = \dfrac{A}{B} = \displaystyle\sum_{i=1}^{r} \frac{AU_i}{(X-\lambda_i)^{m_i}}$.
- Pour tout $i \in [\![1,r]\!]$, la division euclidienne de AU_i par $(X-\lambda_i)^{m_i}$ s'écrit : $AU_i = (X-\lambda_i)^{m_i} E_i + R_i$ pour certains $E_i \in \mathbb{C}[X]$ et $R_i \in \mathbb{C}_{m_i-1}[X]$.
- Pour tout $i \in [\![1,r]\!]$, décomposons R_i dans la base $\left((X-\lambda_i)^{m_i-k}\right)_{1\leqslant k\leqslant m_i}$ de $\mathbb{C}_{m_i-1}[X]$. Il existe des scalaires $a_{i1}, \dots, a_{im_i} \in \mathbb{C}$ pour lesquels : $R_i = \displaystyle\sum_{k=1}^{m_r} a_{ik}(X-\lambda_i)^{m_i-k}$. Il nous reste à conclure :

$$R = \frac{A}{B} = \sum_{i=1}^{r} \frac{AU_i}{(X-\lambda_i)^{m_i}} = \sum_{i=1}^{r} \frac{(X-\lambda_i)^{m_i}E_i + R_i}{(X-\lambda_i)^{m_i}} = \underbrace{\sum_{i=1}^{r} E_i}_{\text{Polynôme}} + \underbrace{\sum_{i=1}^{r} \frac{R_i}{(X-\lambda_i)^{m_i}}}_{\substack{\text{Fraction de degré} \\ \text{strictement négatif}}} = E + \sum_{i=1}^{r}\sum_{k=1}^{m_i} \frac{a_{ik}}{(X-\lambda_i)^k}. \quad \blacksquare$$

Exemple Dans les exemples suivants, on a pris soin de faire apparaître la partie entière même quand elle est nulle. Les fractions proposées étant en outre à coefficients RÉELS, elles sont égales à leur conjuguée, raison pour laquelle certains coefficients sont égaux à conjugaison près.

- Pour un certain $a \in \mathbb{C}$: $\dfrac{X^3+4}{X^2+1} = X + \dfrac{a}{X-\mathrm{i}} + \dfrac{\overline{a}}{X+\mathrm{i}}$.
- Pour certains $a,b,c,d,e \in \mathbb{C}$: $\dfrac{X^4+X+1}{X(X-5)^3(X^2+4)} = 0 + \dfrac{a}{X} + \dfrac{b}{(X-5)^3} + \dfrac{c}{(X-5)^2} + \dfrac{d}{X-5} + \dfrac{e}{X-2\mathrm{i}} + \dfrac{\overline{e}}{X+2\mathrm{i}}$.
- Pour certains $a,b,c \in \mathbb{C}$: $\dfrac{1}{X(X^2+X+1)^2} = 0 + \dfrac{a}{X} + \dfrac{b}{(X-\mathrm{j})^2} + \dfrac{c}{X-\mathrm{j}} + \dfrac{\overline{b}}{(X-\overline{\mathrm{j}})^2} + \dfrac{\overline{c}}{X-\overline{\mathrm{j}}}$.

Théorème (Décomposition en éléments simples sur $\mathbb{R}$) Soit $R = \dfrac{A}{B} \in \mathbb{R}(X)$ IRRÉDUCTIBLE de partie entière E. On introduit la factorisation irréductible de B : $B = \beta \displaystyle\prod_{i=1}^{r} (X-\lambda_i)^{m_i} \prod_{j=1}^{s} \left(X^2+b_jX+c_j\right)^{n_j}$ (notations évidentes).
Il existe des familles uniques $(a_{ik})_{\substack{1\leqslant i\leqslant r \\ 1\leqslant k\leqslant m_i}}$, $(u_{jk})_{\substack{1\leqslant j\leqslant s \\ 1\leqslant k\leqslant n_j}}$ et $(v_{jk})_{\substack{1\leqslant j\leqslant s \\ 1\leqslant k\leqslant n_j}}$ de réels telles que :

$$R = E + \sum_{i=1}^{r}\sum_{k=1}^{m_i} \underbrace{\frac{a_{ik}}{(X-\lambda_i)^k}}_{\substack{\text{Partie polaire} \\ \text{associée au pôle } \lambda_i}} + \sum_{j=1}^{s}\sum_{k=1}^{n_j} \frac{u_{jk}X+v_{jk}}{\left(X^2+b_jX+c_j\right)^k}.$$

On n'oublie pas la partie entière !

Cette décomposition de R est appelée sa décomposition en éléments simples sur $\mathbb{R}$.

Démonstration Hors programme. $\blacksquare$

Exemple On reprend ci-dessous les exemples précédents, comparez !

- Pour certains $a',b' \in \mathbb{R}$: $\dfrac{X^3+4}{X^2+1} = X + \dfrac{a'X+b'}{X^2+1}$.
- Pour certains $a',b',c',d',e',f' \in \mathbb{R}$: $\dfrac{X^4+X+1}{X(X-5)^3(X^2+4)} = 0 + \dfrac{a'}{X} + \dfrac{b'}{(X-5)^3} + \dfrac{c'}{(X-5)^2} + \dfrac{d'}{X-5} + \dfrac{e'X+f'}{X^2+4}$.
- Pour certains $a',b',c',d',e' \in \mathbb{R}$: $\dfrac{1}{X(X^2+X+1)^2} = 0 + \dfrac{a'}{X} + \dfrac{b'X+c'}{(X^2+X+1)^2} + \dfrac{d'X+e'}{X^2+X+1}$.

✎ **En pratique** ✎ À présent, pour le calcul des coefficients, nous avions quatre techniques en début d'année :

— multiplier par $(X-\lambda)^m$ puis évaluer en λ,

— multiplier par X puis passer à la limite en $+\infty$,

— évaluer en un point,

— mettre au même dénominateur et identifier.

Exemple $\dfrac{X^2+3X+1}{(X-1)^2(X-2)} = -\dfrac{5}{(X-1)^2} - \dfrac{10}{X-1} + \dfrac{11}{X-2}$.

Démonstration

- **Forme de la décomposition en éléments simples sur $\mathbb{R}$:** La partie entière est nulle, donc pour certains $a,b,c \in \mathbb{R}$: ★ $\dfrac{X^2+3X+1}{(X-1)^2(X-2)} = \dfrac{a}{(X-1)^2} + \dfrac{b}{X-1} + \dfrac{c}{X-2}$.
- **Calcul de a :** On multiplie ★ par $(X-1)^2$ puis on évalue en 1 : $a = -5$.
- **Calcul de c :** On multiplie ★ par $X-2$ puis on évalue en 2 : $c = 11$.
- **Calcul de b :** On multiplie ★ par X puis on passe à la limite en $+\infty$: $b+c=1$, donc $b=-10$.

Le théorème qui suit est spécifique aux **PÔLES SIMPLES** et souvent pratique quand on connaît la forme développée du dénominateur.

Théorème (Partie polaire associée à un pôle simple) Soient $R = \dfrac{A}{B} \in \mathbb{C}(X)$ **IRRÉDUCTIBLE** et $\lambda \in \mathbb{C}$.
Si λ est un **PÔLE SIMPLE** de R de partie polaire associée $\dfrac{a}{X-\lambda}$ avec $a \in \mathbb{C}$, alors : $a = \dfrac{A(\lambda)}{B'(\lambda)}$.

Démonstration Comme λ est pôle simple de R : $B = (X-\lambda)C$ pour un certain $C \in \mathbb{K}[X]$ avec : $C(\lambda) \neq 0$ et la décomposition en éléments simples de R sur $\mathbb{C}$ s'écrit : $R = \dfrac{a}{X-\lambda} + Q$ pour une certaine fraction $Q \in \mathbb{C}(X)$ n'admettant pas λ pour pôle. Aussitôt : $\dfrac{A}{C} = (X-\lambda)R = a + (X-\lambda)Q$, donc en λ : $a = \dfrac{A(\lambda)}{C(\lambda)}$, mais par ailleurs : $B' = C + (X-\lambda)C'$ donc : $B'(\lambda) = C(\lambda)$, donc en effet : $a = \dfrac{A(\lambda)}{C(\lambda)} = \dfrac{A(\lambda)}{B'(\lambda)}$. ■

Exemple Pour tout $n \in \mathbb{N}^*$: $\dfrac{1}{X^n-1} = \dfrac{1}{n}\displaystyle\sum_{\omega\in\mathbb{U}_n} \dfrac{\omega}{X-\omega}$.

Démonstration Les pôles de $\dfrac{1}{X^n-1}$ sont les racines $n^{\text{èmes}}$ de l'unité et sont tous simples. La partie entière étant par ailleurs nulle : $\dfrac{1}{X^n-1} = \displaystyle\sum_{\omega\in\mathbb{U}_n} \dfrac{a_\omega}{X-\omega}$ pour une certaine famille $(a_\omega)_{\omega\in\mathbb{U}_n} \in \mathbb{C}^n$.
Soit $\omega \in \mathbb{U}_n$ fixé. La technique de multiplication/évaluation serait ici pénible à mettre en œuvre — essayez pour comprendre — nous allons nous en sortir grâce au théorème précédent. Comme : $\dfrac{1}{X^n-1} = \dfrac{A}{B}$ avec : $A=1$ et $B = X^n-1$ et comme ω est **PÔLE SIMPLE** : $a_\omega = \dfrac{A(\omega)}{B'(\omega)} = \dfrac{1}{n\omega^{n-1}} \overset{\omega^n=1}{=} \dfrac{1}{n\omega^{-1}} = \dfrac{\omega}{n}$.

✎ **En pratique** ✎ Quand les pôles **NON RÉELS** d'une fraction **RÉELLE** sont **SIMPLES**, on peut obtenir la décomposition en éléments simples sur $\mathbb{R}$ facilement à partir de la décomposition en éléments simples sur $\mathbb{C}$ par simple regroupement des parties polaires conjuguées.

Exemple $\displaystyle\int_0^{\frac{1}{2}} \frac{t^5\,\mathrm{d}t}{t^4-1} = \frac{1}{8} + \frac{1}{4}\ln\frac{3}{5}$.

Démonstration

- **Décomposition en éléments simples sur $\mathbb{C}$:** La partie entière est nulle, donc pour certains $a,b,c,d \in \mathbb{C}$:

$$\bigstar \quad \frac{X^5}{X^4-1} = \frac{X^5}{(X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i})} = X + \frac{a}{X-1} + \frac{b}{X+1} + \frac{c}{X-\mathrm{i}} + \frac{\overline{c}}{X+\mathrm{i}},$$

mais les pôles $1, -1$et i étant **SIMPLES** :

$$a = \frac{X^5}{\left(X^4-1\right)'}(1) = \frac{1}{4}, \qquad b = \frac{X^5}{\left(X^4-1\right)'}(-1) = \frac{1}{4} \qquad \text{et} \qquad c = \frac{X^5}{\left(X^4-1\right)'}(\mathrm{i}) = -\frac{1}{4}.$$

- **Décomposition en éléments simples sur $\mathbb{R}$:** On regroupe !
$$\frac{X^5}{X^4-1} = X + \frac{1}{4}\left(\frac{1}{X-1} + \frac{1}{X+1} - \frac{1}{X-\mathrm{i}} - \frac{1}{X+\mathrm{i}}\right) = X + \frac{1}{4}\left(\frac{1}{X-1} + \frac{1}{X+1} - \frac{2X}{X^2+1}\right).$$
- **Calcul de l'intégrale :**
$$\int_0^{\frac{1}{2}} \frac{t^5\,\mathrm{d}t}{t^4-1} = \left[\frac{t^2}{2} + \frac{1}{4}\Big(\ln(1-t) + \ln(t+1) - \ln\big(t^2+1\big)\Big)\right]_{t=0}^{t=\frac{1}{2}} = \left[\frac{t^2}{2} + \frac{1}{4}\,\ln\frac{1-t^2}{1+t^2}\right]_{t=0}^{t=\frac{1}{2}} = \frac{1}{8} + \frac{1}{4}\,\ln\frac{3}{5}.$$

Exemple Pour tout $n \in \mathbb{N}^*$, $\dfrac{1}{X^{2n}-1}$ a pour décomposition en éléments simples sur $\mathbb{R}$:
$$\frac{1}{X^{2n}-1} = \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{n}\sum_{k=1}^{n-1} \frac{X\cos\dfrac{k\pi}{n} - 1}{X^2 - 2X\cos\dfrac{k\pi}{n} + 1}.$$

Démonstration Nous avons déjà calculé la décomposition en éléments simples sur $\mathbb{C}$, elle admet -1 et 1 pour seuls pôles réels, les autres peuvent être regroupés par paires de conjugués.
$$\begin{aligned}
\frac{1}{X^{2n}-1} &= \frac{1}{2n}\sum_{k=0}^{2n-1} \frac{\mathrm{e}^{\frac{2\mathrm{i}k\pi}{2n}}}{X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{2n}}} = \frac{1}{2n}\sum_{k=0}^{2n-1} \frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}}{X - \mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}} = \frac{1}{2n}\left(\frac{1}{X-1} - \frac{1}{X+1} + \sum_{k=1}^{n-1}\left(\frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}}{X - \mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}} + \frac{\mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}}{X - \mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}}\right)\right) \\
&= \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{2n}\sum_{k=1}^{n-1} \frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\left(X - \mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\right) + \mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\left(X - \mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\right)}{\left(X - \mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\right)\left(X - \mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\right)} \\
&= \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{2n}\sum_{k=1}^{n-1} \frac{2X\cos\dfrac{k\pi}{n} - 2}{X^2 - 2X\cos\dfrac{k\pi}{n} + 1} = \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{n}\sum_{k=1}^{n-1} \frac{X\cos\dfrac{k\pi}{n} - 1}{X^2 - 2X\cos\dfrac{k\pi}{n} + 1}.
\end{aligned}$$

4 Preuve du théorème de d'Alembert-Gauss

Nous terminerons ce chapitre sur une preuve — hors programme — du théorème de d'Alembert-Gauss.

Démonstration Soit $P \in \mathbb{C}[X]$ non constant. Pour montrer que P possède une racine dans $\mathbb{C}$, nous allons nous intéresser à la fonction $|P|$, prouver d'abord qu'elle possède un minimum, puis prouver que ce minimum est forcément 0 — ce qui garantira bien l'existence d'une racine. Introduisons pour le moment les coefficients de P : $P = \sum_{k=0}^{d} a_k X^k$, avec : $d = \deg(P) \geqslant 1$ et $a_d \neq 0$.

- Montrons que $|P|$ possède un minimum dans $\mathbb{C}$. En tout cas, la fonction $|P|$ étant positive, la propriété de la borne inférieure justifie l'existence de : $m = \inf_{\mathbb{C}} |P|$. Mais avons-nous là un minimum ?

  1) Pour tous $r \geqslant 0$ et $z \in \mathbb{C}$ de module r : $\big|P(z)\big| \geqslant |a_d| \times |z|^d - \left|\sum_{k=0}^{d-1} a_k z^k\right| \geqslant |a_d| r^d - \sum_{k=0}^{d-1} |a_k| r^k$. Or : $\lim_{r\to+\infty}\left(|a_d| r^d - \sum_{k=0}^{d-1} |a_k| r^k\right) = +\infty$, donc : $|a_d| r^d - \sum_{k=0}^{d-1} |a_k| r^k > m+1$ pour tout r strictement supérieur à un certain $R > 0$. Finalement, pour tout $z \in \mathbb{C}$ tel que $|z| > R$: $\big|P(z)\big| > m+1$.

  2) Pour tout $n \in \mathbb{N}$, $m + \dfrac{1}{2^n}$ ne minore pas $|P|$, donc : $\big|P(z_n)\big| < m + \dfrac{1}{2^n}$ pour un certain $z_n \in \mathbb{C}$ — et même : $m \leqslant \big|P(z_n)\big| < m + \dfrac{1}{2^n}$. D'après le théorème d'encadrement : $\lim_{n\to+\infty} \big|P(z_n)\big| = m$.

3) Pour tout $n\in\mathbb{N}$: $\left|P(z_n)\right|<m+\dfrac{1}{2^n}\leqslant m+1$, donc d'après 1) : $|z_n|\leqslant R$. Bornée, la suite $(z_n)_{n\in\mathbb{N}}$ possède ainsi une suite extraite convergente $\left(z_{\varphi(n)}\right)_{n\in\mathbb{N}}$ d'après le théorème de Bolzano-Weierstrass, disons de limite ℓ. Dans ces conditions : $m\overset{2)}{=}\lim\limits_{n\to+\infty}\left|P\left(z_{\varphi(n)}\right)\right|=\left|P(\ell)\right|$. Conclusion : m est un minimum de $|P|$ — pas seulement une borne inférieure.

- Pour montrer que le minimum $m=\left|P(\ell)\right|$ de $|P|$ vaut forcément 0, supposons par l'absurde : $P(\ell)\neq 0$ et notons Q le polynôme $P(X+\ell)$ avec ses coefficients : $Q=b_0+b_qX^q+b_{q+1}X^{q+1}+\ldots+b_dX^d$, où b_q est le premier coefficient non nul après $b_0=Q(0)=P(\ell)\neq 0$. Notons en outre θ un argument de $-\dfrac{b_0}{b_q}$, de sorte que : $\dfrac{b_0}{b_q}=-\left|\dfrac{b_0}{b_q}\right|\mathrm{e}^{\mathrm{i}\theta}$. Fixons enfin $r\in\left]0,1\right]$ et posons : $z=r\mathrm{e}^{\frac{\mathrm{i}\theta}{q}}$.

$$\left|Q(z)\right|=\left|b_0+b_qz^q+b_{q+1}z^{q+1}+\ldots+b_dz^d\right|\leqslant\left|b_0+b_qz^q\right|+\sum_{k=q+1}^{d}|b_k|\times|z|^k=|b_0|\times\left|1+\frac{b_qr^q\mathrm{e}^{\mathrm{i}\theta}}{b_0}\right|+\sum_{k=q+1}^{d}|b_k|r^k$$
$$\overset{0<r\leqslant 1}{\leqslant}|b_0|\times\left|1-\left|\frac{b_q}{b_0}\right|r^q\right|+r^{q+1}\sum_{k=q+1}^{d}|b_k|=|b_0|\times\left|1-\left|\frac{b_q}{b_0}\right|r^q\right|+r^{q+1}T\qquad\text{si l'on pose } T=\sum_{k=q+1}^{d}|b_k|>0.$$

Choisissons a posteriori r inférieur à $\sqrt[q]{\left|\dfrac{b_0}{b_q}\right|}$ et $\dfrac{|b_q|}{2T}$. Alors : $1-\left|\dfrac{b_q}{b_0}\right|r^q\geqslant 0$ et $r^{q+1}T\leqslant\dfrac{|b_q|r^q}{2}$, donc : $\left|Q(z)\right|\leqslant|b_0|\times\left(1-\left|\dfrac{b_q}{b_0}\right|r^q\right)+\dfrac{|b_q|r^q}{2}=|b_0|-\dfrac{|b_q|r^q}{2}<|b_0|=\left|Q(0)\right|=\left|P(z_0)\right|=m$. Conclusion : $\left|P(z+\ell)\right|=\left|Q(z)\right|<m$ — alors que m minore $|P|$! Comme voulu : $P(\ell)=0$. ■