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 trop fort à celles du chapitre « Arithmétique des entiers relatifs » seront souvent omises.

On rappelle que deux polynômes $P, Q \in \mathbb{K}[X]$ sont dits *associés* (*sur* $\mathbb{K}$) s'ils se divisent mutuellement, i.e. si $P = \lambda Q$ pour un certain $Q \in \mathbb{K}^*$.

1 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 ! **L'irréductibilité dépend de $\mathbb{K}$.** 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 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 $A \in \mathbb{K}[X]$ pour lesquels $P = AD$. 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 $D = \frac{1}{a}P$.

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 nul de $\mathbb{K}[X]$ est le produit d'un élément de $\mathbb{K}^*$ et d'un ensemble fini — éventuellement vide — de polynômes irréductibles **unitaires** sur $\mathbb{K}$. Une telle écriture est appelé une *factorisation irréductible de P sur $\mathbb{K}$*.

Démonstration Par récurrence forte sur le degré.

- **Initialisation :** Les polynômes constants non nuls sont le produit d'eux-mêmes avec... rien.
- **Hérédité :** Soit $n \in \mathbb{N}^*$. Faisons l'hypothèse que tout polynôme non nul de $\mathbb{K}[X]$ de degré strictement inférieur à n est le produit d'un élément de $\mathbb{K}^*$ et d'un ensemble fini de polynômes irréductibles unitaires 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, on obtient la décomposition voulue en factorisant simplement par le coefficient dominant. Dans le cas contraire $P = AB$ pour certains $A, B \in \mathbb{K}[X]$ non nuls de degrés strictement inférieurs à n. Or par hypothèse de récurrence, A et B sont chacun le produit d'un élément de $\mathbb{K}^*$ et d'un ensemble fini de polynômes irréductibles unitaires, donc P aussi par produit.

Il nous reste bien sûr à déterminer tous les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Déjà, les polynômes de degré 1 le sont. Il se trouve que la réciproque est vraie dans $\mathbb{C}[X]$ — 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) La factorisation irréductible d'un polynôme non constant de $\mathbb{C}[X]$ coïncide avec sa forme scindée — en particulier, elle est unique.

Démonstration Pour l'assertion (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. Ainsi, $X-\lambda$ divise P, donc par irréductibilité de P sur $\mathbb{C}$, P et $X-\lambda$ sont associés, donc P est de degré 1. La réciproque a été traitée à l'instant comme un exemple.

Que dire à présent des irréductibles de $\mathbb{R}[X]$? La situation reste assez simple, mais 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 $A \in \mathbb{R}[X]$ pour lesquels $P = AD$. Cette fois, 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 :

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

avec :
— A pour coefficient dominant,
— $\lambda_1,\dots,\lambda_r$ pour racines réelles distinctes de multiplicités respectives $m_1,\dots,m_r$,
— des polynômes $X^2+b_jX+c_j$ 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 λ est réel, $X-\lambda$ 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 λ n'est pas réel, alors $\overline{\lambda} \neq \lambda$, donc $P=(X-\lambda)\big(X-\overline{\lambda}\big)Q$ pour un certain $Q \in \mathbb{C}[X]$. Or après développement : $P=\big(X^2-2\,\mathrm{Re}(\lambda)\,X+|\lambda|^2\big)Q$ et $X^2-2\,\mathrm{Re}(\lambda)\,X+|\lambda|^2$ est à coefficients réels, donc Q aussi 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, donc P est de degré 2, 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.

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 $\mathbb{C}$ s'écrit $X^4+16=\Big(X-2\,e^{-\frac{i\pi}{4}}\Big)\Big(X-2\,e^{\frac{i\pi}{4}}\Big)\Big(X-2\,e^{-\frac{3i\pi}{4}}\Big)\Big(X-2\,e^{\frac{3i\pi}{4}}\Big)$.

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 $r \in \mathbb{C}$:

$$r^4+16=0 \quad\Longleftrightarrow\quad r^4=-16=\Big(2\,e^{\frac{i\pi}{4}}\Big)^4 \quad\Longleftrightarrow\quad \exists\, k \in [\![0,3]\!],\quad r=2\,e^{\frac{i\pi}{4}+\frac{2ik\pi}{4}}.$$

La factorisation irréductible de X^4+16 sur $\mathbb{C}$ en découle — avec ici des racines simples.

- **Factorisation irréductible sur $\mathbb{R}$:** Il nous reste à regrouper les racines par paires de conjuguées.
$$\left(X-2\,\mathrm{e}^{-\frac{i\pi}{4}}\right)\left(X-2\,\mathrm{e}^{\frac{i\pi}{4}}\right)=X^2-2\left(\mathrm{e}^{-\frac{i\pi}{4}}+\mathrm{e}^{\frac{i\pi}{4}}\right)X+4=X^2-4\cos\frac{\pi}{4}\times X+4=X^2-2\sqrt{2}X+4$$
et $\left(X-2\,\mathrm{e}^{-\frac{3i\pi}{4}}\right)\left(X-2\,\mathrm{e}^{\frac{3i\pi}{4}}\right)=X^2-2\left(\mathrm{e}^{-\frac{3i\pi}{4}}+\mathrm{e}^{\frac{3i\pi}{4}}\right)X+4=X^2-4\cos\frac{3\pi}{4}\times X+4=X^2+2\sqrt{2}X+4.$

2 PGCD, PPCM

Pour tout $P\in\mathbb{K}[X]$, on notera $\mathrm{div}(P)$ l'ensemble des diviseurs de P — sous-entendu dans $\mathbb{K}[X]$ — mais il ne s'agit pas d'une notation universelle. L'ensemble des multiples de P est quant à lui l'ensemble $P\mathbb{K}[X]$.

Définition-théorème (PGCD, PPCM) Soient $A_1,\dots,A_r\in\mathbb{K}[X]$.

- **PGCD :** On appelle *plus grand commun diviseur* (ou *PGCD*) *de* $A_1,\dots,A_r$ tout polynôme $D\in\mathbb{K}[X]$ pour lequel :
$$\mathrm{div}(A_1)\cap\ldots\cap\mathrm{div}(A_r)=\mathrm{div}(D)$$
Les PGCD de $A_1,\dots,A_r$, s'il en existe, sont associés et un seul d'entre eux est unitaire ou nul, qu'on appelle LE *PGCD de* $A_1,\dots,A_r$ et noté $A_1\wedge\ldots\wedge A_r$.
- **PPCM :** On appelle *plus petit commun multiple* (ou *PPCM*) *de* $A_1,\dots,A_r$ tout polynôme $M\in\mathbb{K}[X]$ pour lequel :
$$A_1\mathbb{K}[X]\cap\ldots\cap A_r\mathbb{K}[X]=M\mathbb{K}[X].$$
Les PPCM de $A_1,\dots,A_r$, s'il en existe, sont associés et un seul d'entre eux est unitaire ou nul, qu'on appelle LE *PPCM de* $A_1,\dots,A_r$ et noté $A_1\vee\ldots\vee A_r$.

Démonstration Soient $D,\widetilde{D}$ deux PGCD de $A_1,\dots,A_r$. En particulier $\mathrm{div}(D)=\mathrm{div}\big(\widetilde{D}\big)$, donc D et $\widetilde{D}$ se divisent mutuellement, donc sont associés. Même chose avec les PPCM.

2.1 Existence et calcul du PGCD

L'existence du PGCD de deux polynômes repose sur ce que j'appelle l'*idée fondamentale de l'algorithme d'Euclide*. Soient $A,B,P\in\mathbb{K}[X]$. Montrons que $\mathrm{div}(A)\cap\mathrm{div}(AP+B)=\mathrm{div}(A)\cap\mathrm{div}(B)$. Or tout simplement, tout diviseur commun de A et B divise aussi A et $AP+B$, et inversement, tout diviseur commun de A et $AP+B$ divise aussi A et $(AP+B)-AP=B$.

En particulier, pour tous $A,B\in\mathbb{K}[X]$ avec B non nul : $\mathrm{div}(A)\cap\mathrm{div}(B)=\mathrm{div}(B)\cap\mathrm{div}(R)$ si on note R le reste de la division euclidienne de A par B.

Théorème (Existence du PGCD) Toute collection finie de polynômes possède un PGCD.

Plus précisément, pour deux polynômes $A,B\in\mathbb{K}[X]$ dont l'un au moins est non nul, $A\wedge B$ est l'unique diviseur commun unitaire de degré maximal de A et B. En outre : $0\wedge 0=0$.

Démonstration

- **Cas de deux polynômes (algorithme d'Euclide) :** Soient $A,B\in\mathbb{K}[X]$ avec $\deg(B)\leqslant\deg(A)$ sans perte de généralité. On définit dans ce cas une famille de polynômes $R_0,R_1,R_2\dots$ 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}, ce qui implique en particulier que $\deg(R_{k+2})<\deg(R_{k+1})$.

  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 $N\in\mathbb{N}^*$, autrement dit $R_N=0$ — bref, l'algorithme se termine. Or grâce à l'idée fondamentale de l'algorithme d'Euclide :
$$\begin{aligned}\mathrm{div}(A)\cap\mathrm{div}(B)&=\mathrm{div}(R_0)\cap\mathrm{div}(R_1)=\mathrm{div}(R_1)\cap\mathrm{div}(R_2)=\ldots=\mathrm{div}(R_{N-1})\cap\mathrm{div}(R_N)\\&=\mathrm{div}(R_{N-1})\cap\mathrm{div}(0)=\mathrm{div}(R_{N-1})\cap\mathbb{K}[X]=\mathrm{div}(R_{N-1}),\end{aligned}$$
  donc A et B possèdent un PGCD, en l'occurrence R_{N-1}.
- **Cas général :** Par récurrence. **Initialisation :** Faite à l'instant pour deux polynômes.

  Hérédité : Soit $r\geqslant 2$. On suppose que toute collection de r polynômes possède un PGCD. Pour tous $A_1,\dots,A_{r+1}\in\mathbb{K}[X]$:
$$\begin{aligned}\mathrm{div}(A_1)\cap\ldots\cap\mathrm{div}(A_{r+1})&=\big(\mathrm{div}(A_1)\cap\ldots\cap\mathrm{div}(A_r)\big)\cap\mathrm{div}(A_{r+1})\\&\overset{\text{HDR}}{=}\mathrm{div}(A_1\wedge\ldots\wedge A_r)\cap\mathrm{div}(A_{r+1})=\mathrm{div}\big((A_1\wedge\ldots\wedge A_r)\wedge A_{r+1}\big),\end{aligned}$$
  donc $A_1,\dots,A_{r+1}$ possèdent un PGCD.

L'*algorithme d'Euclide* calcule rapidement le PGCD de deux polynômes A et B pour lesquels $0 \leqslant \deg(B) \leqslant \deg(A)$. D'après ce qui précède :

$A \wedge B$ est le **DERNIER RESTE NON NUL**, rendu **UNITAIRE** si besoin, 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 : $\left(2X^4 + 9X^3 + 12X^2 + 10X + 3\right) \wedge \left(2X^4 + X^3 - 2X^2 + 3X + 2\right) = X + \dfrac{1}{2}$.

Théorème (Factorisation d'un PGCD) Pour tous $A_1, \ldots, A_r, P \in \mathbb{K}[X]$ avec P **UNITAIRE** :

$$(A_1 P) \wedge \ldots \wedge (A_r P) = (A_1 \wedge \ldots \wedge A_r) P.$$

Démonstration Contentons-nous du cas $r = 2$ pour simplifier. Il nous suffit de montrer que les polynômes **UNITAIRES OU NULS** $(A_1 P) \wedge (A_2 P)$ et $(A_1 \wedge A_2) P$ se divisent mutuellement.

- Pour commencer, $(A_1 \wedge A_2) P$ divise $A_1 P$ et $A_2 P$, donc aussi $(A_1 P) \wedge (A_2 P)$ par définition du PGCD.
- Inversement, P divise $A_1 P$ et $A_2 P$, donc aussi $(A_1 P) \wedge (A_2 P)$ par définition du PGCD, donc $(A_1 P) \wedge (A_2 P) = DP$ pour un certain $D \in \mathbb{K}[X]$. Dans ces conditions, DP divise $A_1 P$ et $A_2 P$ avec $P \neq 0$, donc D divise A_1 et A_2, donc aussi $A_1 \wedge A_2$. En retour, $(A_1 P) \wedge (A_2 P) = DP$ divise $(A_1 \wedge A_2) P$.

2.2 RELATIONS DE BÉZOUT

Définition-théorème (Relations de Bézout) 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*.

Plus généralement, soient $A_1, \ldots, A_r \in \mathbb{K}[X]$. Il existe des polynômes $U_1, \ldots, U_r \in \mathbb{K}[X]$ pour lesquels $A_1 \wedge \ldots \wedge A_r = A_1 U_1 + \ldots + A_r U_r$. Une telle relation est appelée **UNE** *relation de Bézout de $A_1, \ldots, A_r$*.

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

Démonstration Contentons-nous du cas de deux polynômes A et B avec $\deg(B) \leqslant \deg(A)$ sans perte de généralité. 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 $(U_0, V_0) = (1, 0)$ et $(U_1, V_1) = (0, 1)$, puis pour tout $k \in [\![0, N-2]\!]$: $\left(U_{k+2}, V_{k+2}\right) = \left(U_k - Q_{k+2} U_{k+1}, V_k - Q_{k+2} V_{k+1}\right)$. Il n'est pas dur de montrer par récurrence double que pour tout $k \in [\![0, N]\!]$: $R_k = AU_k + BV_k$. En particulier $A \wedge B = R_{N-1} = AU_{N-1} + BV_{N-1}$.

Le procédé de construction des polynômes U et V de la démonstration qui précède s'appelle l'*algorithme d'Euclide étendu*. En résumé, alors que l'algorithme d'Euclide ne s'intéresse qu'aux restes des divisions euclidiennes successives effectuées, l'algorithme d'Euclide étendu va plus loin en tenant compte aussi des quotients successifs obtenus.

Exemple Pour $A = 6X^4 + 8X^3 - 7X^2 - 5X - 2$ et $B = 6X^3 - 4X^2 - X - 1$: $A \wedge B = X - 1 = -(3X+1) \times A + \left(3X^2 + 7X + 3\right) \times B$.

Démonstration On calcule d'abord les restes successifs associés à A et B :

$$\underline{A} = (X+2) \times \underline{B} + \underline{2X^2 - 2X}, \qquad \underline{B} = (3X+1) \times \left(\underline{2X^2 - 2X}\right) + \underline{X-1}, \qquad \underline{2X^2 - 2X} = 2 \times (\underline{X-1}) + \underline{0}.$$

Le dernier reste non nul vaut $X - 1$ et il est **UNITAIRE**, c'est notre PGCD. Pour calculer un jeu de coefficients de Bézout associé, on remonte la chaîne des divisions euclidiennes successives en partant du PGCD $X - 1$:

$$\begin{aligned} \underline{X-1} &= \underline{B} - (3X+1) \times \left(\underline{2X^2 - 2X}\right) && \text{(On a éliminé } \underline{X-1}.\text{)} \\ &= \underline{B} - (3X+1) \times \left(\underline{A} - (X+2) \times \underline{B}\right) = -(3X+1) \times \underline{A} + \left(3X^2 + 7X + 3\right) \times \underline{B}. && \text{(On a éliminé } \underline{2X^2 - 2X}.\text{)} \end{aligned}$$

Pour finir, 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 $2X(X+1)^2(X+2)^3 \wedge X(X+2)^4\left(X^2+1\right) = X(X+2)^3$.

2.3 Polynômes premiers entre eux

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

- **Cas de deux polynômes :** On dit que A et B sont *premiers entre eux* si 1 est leur seul diviseur commun unitaire, i.e. si $A \wedge B = 1$.
- **Dans leur ensemble :** On dit que $A_1, \ldots, A_r$ sont *premiers entre eux dans leur ensemble* si 1 est leur seul diviseur commun unitaire, i.e. si $A_1 \wedge \ldots \wedge A_r = 1$.
- **Deux à deux :** On dit que $A_1, \ldots, A_r$ 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 :

$$X(X+1) \wedge X(X+2) = X \neq 1, \quad X(X+2) \wedge (X+1)(X+2) = X+2 \neq 1 \quad \text{et} \quad (X+1)(X+2) \wedge X(X+1) = X+1 \neq 1.$$

Théorème (Théorèmes de Bézout et Gauss, conséquences) Soient $A, B, C, P, A_1, \ldots, A_r \in \mathbb{K}[X]$.

- **Théorème de Bézout :** Les assertions suivantes sont équivalentes :

  (i) A et B sont premiers entre eux. (ii) Il existe deux polynômes $U, V \in \mathbb{K}[X]$ pour lesquels $AU + BV = 1$.
- **Théorème de Gauss :** Si $A \mid BC$ avec $A \wedge B = 1$, alors $A \mid C$.
- **Lemme d'Euclide :** Pour tout $P \in \mathbb{K}[X]$ IRRÉDUCTIBLE : $P \mid AB \iff P \mid A$ ou $P \mid B$.
- **Produits de polynômes :**
  - — Si chacun des polynômes $A_1, \ldots, A_r$ est premier avec P, leur produit $A_1 \ldots A_r$ l'est aussi.
  - — Si $A_1, \ldots, A_r$ divisent P et sont premiers entre eux DEUX À DEUX, leur produit $A_1 \ldots A_r$ divise P.

2.4 Existence et calcul du PPCM

Définition-théorème (PPCM de deux polynômes, lien avec le PGCD) Toute collection finie de polynômes possède un PPCM.

Plus précisément, pour deux polynômes $A, B \in \mathbb{K}[X]$ non nuls, $A \vee B$ est l'unique multiple commun unitaire de degré minimal de A et B.

Lien avec le PGCD : Les polynômes AB et $(A \wedge B)(A \vee B)$ sont associés.

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

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 maintenant en mesure de les fonder proprement.

3.1 Construction des fractions rationnelles

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

— À tout couple $(A,B) \in \mathbb{K}[X]^2$ avec B non nul, 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 non nul.

— Pour tous $(A,B),(C,D) \in \mathbb{K}[X]^2$ avec B et D non nuls : $\quad \dfrac{A}{B} = \dfrac{C}{D} \iff AD = BC$.

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

Démonstration On pose $\mathscr{F} = \mathbb{K}[X] \times \left(\mathbb{K}[X] \setminus \{0\}\right)$. Pour tous $(A,B),(C,D) \in \mathscr{F}$, on dit que $(A,B) \sim (C,D)$ si $AD = BC$. La relation $\sim$ ainsi définie est une relation d'équivalence sur $\mathscr{F}$.

- **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 $CB = DA$, autrement dit $(C,D) \sim (A,B)$.

On note finalement $\mathbb{K}(X)$ l'ensemble quotient $\mathscr{F}/\sim$ 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. Notez bien en passant que la notation fractionnaire n'est au départ qu'une **NOTATION** pour désigner une classe d'équivalence.

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 $(A,B),(C,D) \in \mathbb{K}[X]^2$ avec B et D non nuls :

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

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 $A,B,C,D,E,F \in \mathbb{K}[X]$ avec B, D et F non nuls.

- **Bonne définition de $+$ et $\times$:** Mais où est le problème ? 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 $\widetilde{B}$ et $\widetilde{D}$ non nuls. Pour 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 $\sim$: $\quad AC \times \widetilde{B}\widetilde{D} = A\widetilde{B} \times C\widetilde{D} = B\widetilde{A} \times D\widetilde{C} = BD \times \widetilde{A}\widetilde{C} \quad$ 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 $+$:** $\quad \dfrac{A}{B} + \dfrac{C}{D} = \dfrac{AD+BC}{BD} = \dfrac{CB+DA}{DB} = \dfrac{C}{D} + \dfrac{A}{B}$.
- **Associativité de $+$:**
$$\left(\frac{A}{B} + \frac{C}{D}\right) + \frac{E}{F} = \frac{AD+BC}{BD} + \frac{E}{F} = \frac{(AD+BC)F + (BD)E}{(BD)F} = \frac{A(DF) + B(CF+DE)}{B(DF)} = \frac{A}{B} + \frac{CF+DE}{DF} = \frac{A}{B} + \left(\frac{C}{D} + \frac{E}{F}\right).$$
- **Neutralité de $\dfrac{0}{1}$ pour $+$:** $\quad \dfrac{A}{B} + \dfrac{0}{1} = \dfrac{A \times 1 + B \times 0}{B \times 1} = \dfrac{A}{B} \quad$ et de même $\dfrac{0}{1} + \dfrac{A}{B} = \dfrac{A}{B}$.
- **Inverses pour $+$:** $\quad \dfrac{A}{B} + \dfrac{-A}{B} = \dfrac{AB + B(-A)}{B^2} = \dfrac{0}{B^2} = \dfrac{0}{1} \quad$ et de même $\dfrac{-A}{B} + \dfrac{A}{B} = \dfrac{0}{1}$.

- À ce stade, $\big(\mathbb{K}(X),+\big)$ est un groupe commutatif d'élément neutre $\dfrac{0}{1}$. Pour montrer que $\big(\mathbb{K}(X),+,\times\big)$ est un anneau, on peut montrer de même que $\big(\mathbb{K}(X),\times\big)$ est un magma associatif d'élément neutre $\dfrac{1}{1}$ et que $\times$ est distributive sur $+$. Enfin, pour montrer que $\big(\mathbb{K}(X),+,\times\big)$ 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) L'application $P \longmapsto \dfrac{P}{1}$ est un morphisme injectif d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$. Grâce à cette injection, on identifiera désormais 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 L'application $P \overset{\varphi}{\longmapsto} \dfrac{P}{1}$ est un morphisme d'anneaux car $\varphi(1) = \dfrac{1}{1}$ et pour tous $P,Q \in \mathbb{K}[X]$:

$$\varphi(P)+\varphi(Q) = \frac{P}{1}+\frac{Q}{1} = \frac{P+Q}{1} = \varphi(P+Q) \qquad \text{et} \qquad \varphi(P)\,\varphi(Q) = \frac{P}{1}\times\frac{Q}{1} = \frac{PQ}{1} = \varphi(PQ).$$

Montrons ensuite que φ est injective, i.e. que $\operatorname{Ker}\varphi \subset \big\{0\big\}$. Pour tout $P \in \operatorname{Ker}\varphi$: $\dfrac{P}{1} = \varphi(P) = \dfrac{0}{1}$, donc $P = 0$.

Pour finir, l'image de $\mathbb{K}[X]$ par φ est un sous-anneau de $\mathbb{K}(X)$ car l'image d'un sous-anneau par un morphisme d'anneaux est toujours un sous-anneau.

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 $B \neq 0$. 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 L'écriture $\dfrac{\big(X^2+1\big)(X+1)^2}{X(X+1)}$ n'est pas irréductible, mais l'écriture $\dfrac{\big(X^2+1\big)(X+1)}{X}$ l'est.

Définition (Dérivée d'une fraction rationnelle) Pour tout $R = \dfrac{A}{B} \in \mathbb{K}(X)$, 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 $R,S \in \mathbb{K}(X)$: $\quad (R+S)' = R'+S', \quad (RS)' = R'S+RS' \quad$ et si S est non nulle : $\left(\dfrac{R}{S}\right)' = \dfrac{R'S-RS'}{S^2}$.

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 $\mathbb{R}(X)$. Cela donne :

$$\sum_{k=0}^{n} kX^{k-1} = \frac{-(n+1)X^n(1-X)+\big(1-X^{n+1}\big)}{(1-X)^2} = \frac{1+nX^{n+1}-(n+1)X^n}{(1-X)^2},$$

puis : $\displaystyle\sum_{k=0}^{n} kX^k = \frac{X}{(1-X)^2}\big(1+nX^{n+1}-(n+1)X^n\big)$. Évaluons 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) Pour tout $R = \frac{A}{B} \in \mathbb{K}(X)$, 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 $R, S \in \mathbb{K}(X)$: $\quad \deg(R+S) \leqslant \max\left\{\deg(R), \deg(S)\right\} \quad$ et $\quad \deg(RS) = \deg(R) + \deg(S)$.

En outre, le degré d'un polynôme coïncide avec son degré comme fraction rationnelle.

Attention ! Une fraction rationnelle peut être de degré positif sans être un polynôme. C'est le cas de la fraction rationnelle $\frac{X^4 + X^3 + 1}{X^2 + 3}$, de degré $4 - 2 = 2$.

Définition (Fonction rationnelle) Soit $R = \frac{A}{B} \in \mathbb{K}(X)$ **IRRÉDUCTIBLE**. La fonction $x \longmapsto \frac{A(x)}{B(x)}$ 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).

On impose ici à l'écriture $R = \frac{A}{B}$ 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 $x \longmapsto \frac{x^3 + x + 1}{x - 1}$ est définie sur $\mathbb{R} \setminus \left\{1\right\}$ mais la fonction $x \longmapsto \frac{x\left(x^3 + x + 1\right)}{x(x-1)}$ l'est seulement sur $\mathbb{R} \setminus \left\{0, 1\right\}$.

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

- **Zéros :** 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.
- **Pôles :** 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*).

On impose ici à l'écriture $R = \frac{A}{B}$ 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 $\frac{\left(X^2+1\right)(X-2)^3(X+1)X}{(X-1)^2\left(X^2+X+1\right)}$ 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 $R = \frac{A}{B} \in \mathbb{K}(X)$. 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.

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 $Q = \frac{F}{B}$. Alors d'une part $R = \frac{A}{B} = \frac{EB + F}{B} = E + Q$, mais d'autre part $\deg(Q) = \deg(F) - \deg(B) < 0$.
- **Unicité :** Soient $R = E + Q$ et $R = \widetilde{E} + \widetilde{Q}$ deux décompositions de R. Le **POLYNÔME** $E - \widetilde{E}$ est de degré $\deg\left(\widetilde{Q} - Q\right) \leqslant \max\left\{\deg\left(\widetilde{Q}\right), \deg(Q)\right\} < 0$, donc est nul, donc $E = \widetilde{E}$, puis $Q = \widetilde{Q}$.

Exemple La partie entière de la fraction $\frac{X^4 - 3X^3 + 5X^2 - 1}{X^2 - 3X + 1}$ est $X^2 + 4$ par simple division euclidienne :

$$X^4 - 3X^3 + 5X^2 - 1 = \left(X^2 - 3X + 1\right)\left(X^2 + 4\right) + 12X - 5.$$

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 $\lambda_1, \ldots, \lambda_r$ de multiplicités respectives $m_1, \ldots, m_r$. Il existe une et une seule famille $(a_{ik})_{\substack{1\leqslant i\leqslant r\\1\leqslant k\leqslant m_i}}$ de nombres complexes pour laquelle :

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

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 $B = (X-\lambda_1)^{m_1} \ldots (X-\lambda_r)^{m_r}$. Les POLYNÔMES $\dfrac{B}{(X-\lambda_1)^{m_1}}, \ldots, \dfrac{B}{(X-\lambda_r)^{m_r}}$ sont premiers entre eux dans leur ensemble, d'où la relation de Bézout : $1 = \displaystyle\sum_{i=1}^{r} \frac{BU_i}{(X-\lambda_i)^{m_i}}$ pour certains $U_1, \ldots, U_r \in \mathbb{C}[X]$. Multiplions par R : $R = \displaystyle\sum_{i=1}^{r} \frac{AU_i}{(X-\lambda_i)^{m_i}}$.

À présent, pour tout $i \in [\![1,r]\!]$: $AU_i = (X-\lambda_i)^{m_i} E_i + R_i$ pour certains $E_i \in \mathbb{C}[X]$ et $R_i \in \mathbb{C}_{m_i-1}[X]$ par division euclidienne, et nous pouvons décomposer R_i dans la base $\left((X-\lambda_i)^{m_i-k}\right)_{1\leqslant k\leqslant m_i}$: $R_i = \displaystyle\sum_{k=1}^{m_i} a_{ik}(X-\lambda_i)^{m_i-k}$ pour certains $a_{i1}, \ldots, a_{im_i} \in \mathbb{C}$. Il n nous reste plus qu'à conclure :

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

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, par unicité de la décomposition en éléments simples certains coefficients sont égaux à conjugaison près tandis que d'autres sont réels.

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

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, avec des notations évidentes : $B = \beta \displaystyle\prod_{i=1}^{r} (X-\lambda_i)^{m_i} \prod_{j=1}^{s} \left(X^2+b_jX+c_j\right)^{n_j}$.

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 pour lesquelles :

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

On n'oublie pas la partie entière !

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

Démonstration Hors programme.

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

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

Pour le calcul pratique 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 $a,b,c \in \mathbb{R}$: $\quad \bigstar \quad \dfrac{X^2+3X+1}{(X-1)^2(X-2)} = \dfrac{a}{(X-1)^2} + \dfrac{b}{X-1} + \dfrac{c}{X-2}$.
- **Calcul de a :** On multiplie $\bigstar$ par $(X-1)^2$ puis on évalue en 1 : $\quad a=-5$.
- **Calcul de c :** On multiplie $\bigstar$ par $X-2$ puis on évalue en 2 : $\quad c=11$.
- **Calcul de b :** On multiplie $\bigstar$ par X puis on passe à la limite en $+\infty$: $\quad b+c=1, \quad$ donc $b=-10$.

Le théorème qui suit est spécifique aux **PÔLES SIMPLES** et pratique quand le dénominateur est écrit sous forme développée.

Théorème (Partie polaire associée à un pôle simple) Soient $R=\dfrac{A}{B} \in \mathbb{C}(X)$ et $\lambda \in \mathbb{C}$. Si λ est une **RACINE SIMPLE DE** B — donc un pôle simple de R — et si on note $\dfrac{a}{X-\lambda}$ la partie polaire de R associée à λ, alors $a=\dfrac{A(\lambda)}{B'(\lambda)}$.

Notre hypothèse selon laquelle λ est racine simple de B ne peut pas être remplacée par l'hypothèse selon laquelle λ est un pôle simple de R, qui n'empêche pas λ d'être racine de A et racine multiple de B, auquel cas $B'(\lambda)=0$.

Démonstration Comme λ est racine simple de B, $B=(X-\lambda)\,C$ 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. Ainsi $\dfrac{A}{C}=(X-\lambda)R=a+(X-\lambda)\,Q$, donc $\dfrac{A(\lambda)}{C(\lambda)}=a$ après évaluation en λ, or $B'=C+(X-\lambda)\,C'$, donc $B'(\lambda)=C(\lambda)$, et enfin $a=\dfrac{A(\lambda)}{C(\lambda)}=\dfrac{A(\lambda)}{B'(\lambda)}$.

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

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 : $\quad \dfrac{1}{X^n-1} = \displaystyle\sum_{\omega \in \mathbb{U}_n} \dfrac{a_\omega}{X-\omega} \quad$ 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. Écrivons $\dfrac{1}{X^n-1}=\dfrac{A}{B}$ avec $A=1$ et $B=X^n-1$. Comme ω est **PÔLE SIMPLE** : $\quad a_\omega = \dfrac{A(\omega)}{B'(\omega)} = \dfrac{1}{n\omega^{n-1}} \overset{\omega^n=1}{=} \dfrac{\omega}{n}$.

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 $\mathbb{C}$ en regroupant les parties polaires conjuguées.

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

Démonstration

- **Décomposition en éléments simples sur $\mathbb{C}$:** La partie entière vaut X, donc pour certains $a,b \in \mathbb{R}$ et $c \in \mathbb{C}$: $\quad \bigstar \quad \dfrac{X^5}{1-X^4} = \dfrac{-X^5}{(X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i})} = -X + \dfrac{a}{X-1} + \dfrac{b}{X+1} + \dfrac{c}{X-\mathrm{i}} + \dfrac{\overline{c}}{X+\mathrm{i}}$, et les pôles étant **SIMPLES** : $\quad a=\dfrac{X^5}{\left(1-X^4\right)'}(1)=-\dfrac{1}{4}, \quad b=\dfrac{X^5}{\left(1-X^4\right)'}(-1)=-\dfrac{1}{4} \quad$ et $\quad c=\dfrac{X^5}{\left(1-X^4\right)'}(\mathrm{i})=\dfrac{1}{4}$.

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

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.
$$\frac{1}{X^{2n}-1} = \frac{1}{2n}\sum_{k=0}^{2n-1} \frac{\mathrm{e}^{\frac{2\mathrm{i}k\pi}{2n}}}{X-\mathrm{e}^{\frac{2\mathrm{i}k\pi}{2n}}} = \frac{1}{2n}\sum_{k=0}^{2n-1} \frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}}{X-\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}} = \frac{1}{2n}\left(\frac{1}{X-1} - \frac{1}{X+1} + \sum_{k=1}^{n-1}\left(\frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}}{X-\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}} + \frac{\mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}}{X-\mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}}\right)\right)$$
$$= \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{2n}\sum_{k=1}^{n-1} \frac{\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\left(X-\mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\right) + \mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\left(X-\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\right)}{\left(X-\mathrm{e}^{\frac{\mathrm{i}k\pi}{n}}\right)\left(X-\mathrm{e}^{-\frac{\mathrm{i}k\pi}{n}}\right)}$$
$$= \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{2n}\sum_{k=1}^{n-1} \frac{2X\cos\dfrac{k\pi}{n} - 2}{X^2 - 2X\cos\dfrac{k\pi}{n} + 1} = \frac{1}{2n(X-1)} - \frac{1}{2n(X+1)} + \frac{1}{n}\sum_{k=1}^{n-1} \frac{X\cos\dfrac{k\pi}{n} - 1}{X^2 - 2X\cos\dfrac{k\pi}{n} + 1}.$$