Chapitre 19

Arithmétique des polynômes et fractions rationnelles

Dans ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

I Polynômes irréductibles

Rappel. On dit que deux polynômes $A, B \in \mathbb{K}[X]$ sont associés si $A \mid B$ et $B \mid A$, *i.e.* il existe $\lambda \in \mathbb{K}^\star$ tel que $A = \lambda B$.

Définition - Polynôme irréductible

On dit qu'un polynôme *non constant* $P \in \mathbb{K}[X]$ est *irréductible* si ses seuls diviseurs sont associés à 1 ou à P.

Remarque. Lorsqu'il y a ambiguïté, on précise sur quel corps on entend la propriété. Par exemple, $X^2 + 1$ est irréductible *sur* $\mathbb{R}$, mais pas sur $\mathbb{C}$ (il a $X - \mathrm{i}$ pour diviseur).

Exemple.
- Tout polynôme de degré 1 de $\mathbb{K}[X]$ est irréductible.
- Tout polynôme de degré 2 de $\mathbb{R}[X]$ n'ayant pas de racine réelle est irréductible.

Théorème - Polynômes irréductibles de $\mathbb{C}[X]$, de $\mathbb{R}[X]$

i. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

ii. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et les polynômes de degré 2 à discriminant strictement négatif.

Démonstration.

i. Soit $P \in \mathbb{C}[X]$. Si $\deg P = 1$, alors P est irréductible. Si $\deg P > 2$, on sait que P a une racine $\alpha \in \mathbb{C}$, donc $X - \alpha \mid P$, et P n'est pas irréductible.

ii. Soit $P \in \mathbb{R}[X]$, de discriminant Δ. Si $\deg P = 1$ ou si $\deg P = 2$ et $\Delta < 0$, on a vu que P est irréductible. Si $\deg P = 2$ et $\Delta \geqslant 0$, on sait que P n'est pas irréductible. Supposons maintenant $\deg P > 2$.
- Si P possède une racine réelle α, alors $X - \alpha$ divise P, et P n'est pas irréductible.
- Si P n'a pas de racine réelle, alors il possède une racine $z \in \mathbb{C}\backslash\mathbb{R}$, et on sait que $\bar{z}$ est également une racine de P, distincte de z. Ainsi, $(X-z)(X-\bar{z}) = X^2 - 2\,\mathfrak{Re}\, z + |z|^2 \in \mathbb{R}[X]$ divise P, et P n'est pas irréductible. □

Théorème - Factorisation irréductible

Tout polynôme non constant de $P \in \mathbb{K}[X]$ s'écrit de manière unique (à ordre des facteurs près) sous la forme $P = \lambda P_1^{m_1} \dots P_k^{m_k}$, où les polynômes $P_1, \dots, P_k$ sont irréductibles unitaires, et $m_1, \dots, m_k \in \mathbb{N}^\star$.

- **Cas complexe.** Si $P \in \mathbb{C}[X]$, alors la factorisation première de P est de la forme :

$$P = \prod_{i=1}^{k} (X - \alpha_i)^{m_i}.$$

- **Cas réel.** Si $P \in \mathbb{R}[X]$, alors la factorisation première de P est de la forme :

$$P = \prod_{i=1}^{k} (X - \alpha_i)^{m_i} \prod_{j=1}^{l} (X^2 + \beta_j X + \gamma_j)^{n_j},$$

où les polynômes $X^2 + \beta_j X + \gamma_j$ sont de discriminant strictement négatif.

Démonstration. L'existence de la factorisation première se prouve par récurrence forte sur le degré du polynôme P, de manière en tout point analogue à cette de la factorisation première d'un entier.

L'écriture des factorisations premières se déduit du théorème précédent. L'unicité provient de l'unicité à ordre des facteurs près de la forme scindée d'un polynôme de $\mathbb{C}[X]$. □

Exemple. Le polynôme $X^3 - 1$ a pour factorisation irréductible :

- $P = (X-1)(X-\mathrm{j})(X-\mathrm{j}^2)$ dans $\mathbb{C}[X]$,
- $P = (X-1)(X^2+X+1)$ dans $\mathbb{R}[X]$.

Remarque. Ainsi, qui $P, Q \in \mathbb{C}[X]$, alors $P \mid Q$ si et seulement si pour toute racine α de P, on a $m_\alpha(P) \leqslant m_\alpha(Q)$.

II PGCD, PPCM

1. PGCD

Dans toute la suite, pour $A \in \mathbb{K}[X]$, on note $\mathscr{D}_A$ l'ensemble des polynômes $P \in \mathbb{K}[X]$ qui divisent le polynôme A, c'est-à-dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = AQ$.

Remarque. On a $\mathscr{D}_0 = \mathbb{K}[X]$.

Définition-théorème - PGCD de deux polynômes

Si $A, B \in \mathbb{K}[X]$ ne sont pas tous les deux nuls, il existe des polynômes divisant A et B de degré maximal, on les appelle *plus grands diviseurs communs* (PGCD) de A et B.

Démonstration. Il suffit de remarquer que l'ensemble D des degrés des polynômes divisant à la fois A et B est une partie non vide de $\mathbb{N}$. En effet, on a $1 \mid A$ et $1 \mid B$, donc $0 \in D$. Par ailleurs, le polynôme nul ne peut pas diviser A et B car ils sont non tous deux nuls, donc $D \subset \mathbb{N}$. Par conséquent, D admet bien un plus grand élément. □

Remarques.

– Pour tout $A \in \mathbb{K}[X]$, on a $\mathscr{D}_A \cap \mathscr{D}_0 = \mathscr{D}_A$, donc les PGCD de A et 0 sont tous les diviseurs de A de degré maximal, c'est-à-dire les polynômes de la forme λA avec $\lambda \in \mathbb{K}^\star$.

Théorème

Soient $A, B, R \in \mathbb{K}[X]$. S'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + R$, alors $\mathscr{D}_A \cap \mathscr{D}_B = \mathscr{D}_B \cap \mathscr{D}_R$. Par conséquent, les PGCD de A et B sont exactement les PGCD de B et R.

Démonstration. Si $D \in K[X]$ divise B et R, alors D divise $A = BQ + R$, ce qui donne $\mathscr{D}_B \cap \mathscr{D}_R \subset \mathscr{D}_A \cap \mathscr{D}_B$. L'autre inclusion est obtenue de la même manière : si D divise A et B, alors D divise $R = A - BQ$. □

Algorithme d'Euclide pour l'obtention de PGCD de deux polynômes.

Si $A, B \in \mathbb{K}[X]$, on note $R_0 = A$ et $R_1 = B$, et on effectue la procédure suivante.

Pour $k \in \mathbb{N}^\star$:

– Si $R_k \neq 0$: on effectue la division euclidienne de R_{k-1} par R_k : $R_{k-1} = Q_{k+1}R_k + R_{k+1}$. Alors, on a $\mathscr{D}_{R_{k-1}} \cap \mathscr{D}_{R_k} = \mathscr{D}_{R_k} \cap \mathscr{D}_{R_{k+1}}$, et $\deg R_{k+1} < \deg R_k$.
– Si $R_k = 0$, la procédure s'arrête, et les PCGD de A et B sont les multiples de R_{k-1}.

Ainsi, les PGCD de A et B sont les multiples du *dernier reste non nul* de la famille des restes successifs de l'algorithme d'Euclide.

Remarques.

– La propriété $\deg R_{k+1} < \deg R_k$ si $R_k \neq 0$ assure l'existence d'un entier k_0 tel que $R_{k_0} = 0$. En d'autres termes, l'algorithme s'arrête.

– Par récurrence immédiate, on a $\mathscr{D}_{R_{k-1}} \cap \mathscr{D}_{R_k} = \mathscr{D}_{R_0} \cap \mathscr{D}_{R_1} = \mathscr{D}_A \cap \mathscr{D}_B$. Ainsi,

$$\mathscr{D}_A \cap \mathscr{D}_B = \mathscr{D}_{R_{k_0-1}} \cap \mathscr{D}_{R_{k_0}} = \mathscr{D}_{R_{k_0-1}},$$

car $R_{k_0} = 0$. Ainsi, les PGCD de A et B sont les multiples de R_{k_0-1}.

On a obtenu le résultat suivant, qui permet de définir *le* PGCD de deux polynôme, comme l'unique polynôme unitaire multiple de R_{k_0-1}.

Théorème et définition - Le PGCD de deux polynômes

Si $A, B \in \mathbb{K}[X]$ sont des polynômes non tous deux nuls, les PGCD de A et B sont associés. De plus, il existe un unique PGCD unitaire de A et B, on l'appelle *le* PGCD de A et B, et on le note $A \wedge B$. On a par ailleurs

$$\mathscr{D}_A \cap \mathscr{D}_B = \mathscr{D}_{A \wedge B}.$$

On convient par ailleurs que $0 \wedge 0 = 0$.

Remarque. On retiendra que si $D \mid A$ et $D \mid B$, alors $D \mid A \wedge B$.

Théorème - PGCD et racines

Si $A, B \in \mathbb{K}[X]$, alors les racines communes de A et B sont les racines de $A \wedge B$.

Démonstration. On note $D = A \wedge B$. Si $\alpha \in \mathbb{K}$. Comme $\mathscr{D}_A \cap \mathscr{D}_B = \mathscr{D}_{A \wedge B}$, on a

$$D(\alpha) = 0 \iff X - \alpha \mid D \iff X - \alpha \mid A \text{ et } X - \alpha \mid B \iff A(\alpha) = B(\alpha) = 0. \qquad \square$$

Théorème - Relation de Bézout pour deux polynômes

Soient $A, B \in \mathbb{K}[X]$. Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$. Une telle relation est appelée *relation de Bézout*.

Remarque. Comme pour les entiers, une relation de Bézout n'est pas unique !

Démonstration. On reprend les notations de l'algorithme d'Euclide : $R_0 = A$, $R_1 = B$, et pour tout $k \in \mathbb{N}^\star$ tel que $R_k \neq 0$, on écrit $R_{k-1} = Q_{k+1}R_k + R_{k+1}$, division euclidienne de R_{k-1} par R_k. On montre ensuite par récurrence double que pour tout $k \in \mathbb{N}$, il existe $U_k, V_k \in \mathbb{Z}$ tels que $R_k = U_k A + V_k B$.

– *Initialisation* : en posant $U_0 = 1$, $V_0 = 0$, $U_1 = 0$ et $V_1 = 1$, on a bien $R_0 = u_0 A + V_0 B$ et $R_1 = U_1 A + V_1 B$.
– *Hérédité* : soit $k \in \mathbb{N}^\star$, on suppose qu'il existe $U_{k-1}, V_{k-1}, U_k, V_k \in \mathbb{Z}$ tels que $R_{k-1} = U_{k-1}A + V_{k-1}B$ et $R_k = U_k A + V_k B$. Ainsi,

$$R_{k+1} = R_{k-1} - Q_{k+1}R_k = (U_{k-1} - Q_{k+1}U_k)\,A + (V_{k-1} - Q_{k+1}V_k)\,B.$$

On obtient le résultat en posant $U_{k+1} = U_{k-1} - Q_{k+1}U_k$ et $V_{k+1} = V_{k-1} - Q_{k+1}V_k$.

Comme on sait qu'il existe un entier k_0 tel que $R_{k_0} = 0$ et $A \wedge B = R_{k_0-1}$, on a donc $A \wedge B = U_{k_0-1}A + V_{k_0-1}B$. $\square$

Remarque. Comme dans le cas des entiers, la preuve ci-dessus fournit des relations de récurrence permettant de calculer U_k et V_k à chaque étape. On obtient l'algorithme d'Euclide étendu pour les polynômes.

Algorithme d'Euclide étendu.

On peut synthétiser la réalisation de l'algorithme d'Euclide étendu dans un tableau contenant les restes successifs, les quotients, ainsi que les polynômes U_k et V_k.

On commence par écrire R_0, R_1 et les premières valeurs U_0, V_0, U_1, V_1, puis on utilise les relations de récurrence.

R_k	Q_k	U_k	V_k
A		1	0
B		0	1
⋮	⋮	⋮	⋮

On étend la définition de PGCD pour deux polynômes à un nombre fini de polynômes.

Définition-théorème - PGCD d'un nombre fini de polynômes

Si $A_1, \dots, A_n$ sont des polynômes non tous nuls, il existe un unique polynôme unitaire diviseur commun à $A_1, \dots, A_n$ de degré maximal, on l'appelle PGCD de $A_1, \dots, A_n$ et on le note $A_1 \wedge \dots \wedge A_n$.

Théorème - Relation de Bézout, cas d'un nombre fini de polynômes

Si $A_1, \dots, A_n \in \mathbb{K}[X]$ sont non tous nuls, il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que $U_1A_1 + \dots + U_nA_n = A_1 \wedge \dots \wedge A_n$.

2. PPCM

Définition - PPCM de deux polynômes

Soient $A, B \in \mathbb{K}[X]$ non nuls. On appelle PPCM de A et B un polynôme multiple de A et B de degré minimal.

Remarque. L'existence est assurée car l'ensemble $\mathcal{D}$ des degrés des polynômes multiples communs de A et B est une partie non vide de $\mathbb{N}$ (comme AB est multiple commun de A et B, $\deg A \deg B \in \mathcal{D}$).

Théorème

Soient $A, B \in \mathbb{K}[X]$ non nuls et M un PPCM de A et B. Les multiples communs de A et B sont exactement les multiples de M.

Démonstration. La démonstration est la même que dans le cas de $\mathbb{Z}[X]$. □

Remarque. On retiendra que pour tout $P \in \mathbb{K}[X]$, si $A \mid P$ et $B \mid P$, alors $M \mid P$.

Définition-théorème - Le PPCM de deux polynômes

Si $A, B \in \mathbb{K}[X]$ non nuls, alors les PPCM de A et B sont associés. En particulier, il existe un unique PPCM de A et B unitaire. On l'appelle PPCM de A et B, et on le note $A \vee B$.

Démonstration. Si M, M' sont deux PPCM de A et B, alors d'après le résultat précédent, on a $M \mid M'$ du fait que M' est multiple commun de A et B. De même $M' \mid M$. □

Exemple. Si $A = (X-2)^2(X+\mathrm{i})(X-\mathrm{i})^2$ et $B = (X-2)^3(X+\mathrm{j})(X-\mathrm{i})$, alors

$$A \wedge B = (X-2)^2(X-\mathrm{i}) \quad \text{et} \quad A \vee B = (X-2)^3(X+\mathrm{i})(X+\mathrm{j})(X-\mathrm{i})^2.$$

Comme pour les entiers, on obtient le résultat suivant (par exemple à l'aide de la factorisation irréductible).

Théorème - PGCD et PPCM

Soient $A, B \in \mathbb{K}[X]$ non nuls. Les polynômes $(A \wedge B)(A \vee B)$ et AB sont associés.

III Polynômes premiers entre eux

Définition - Polynômes premiers entre eux

On dit que deux polynômes $A, B \in \mathbb{K}[X]$ sont premiers entre eux si leur seul diviseur commun unitaire est 1, autrement dit $A \wedge B = 1$.

Remarque. Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racines communes.

En effet, les racines communes de A et B étant les racines de $A \wedge B$, on en déduit qu'ils n'ont pas de racine commune si et seulement si $A \wedge B$ n'a pas de racine dans C, c'est-à-dire qu'il est de degré 0.

Théorème - Théorème de Bézout

Si $A, B \in \mathbb{K}[X]$, alors $A \wedge B = 1$ si et seulement s'il existe $U, V \in \mathbb{K}[X]$, $AU + BV = 1$.

Démonstration. Même preuve que dans $\mathbb{Z}$. □

Remarque. Comme pour les entiers, on introduit, pour un nombre fini de polynômes, la notion de polynômes *premiers entre deux à deux*, et de polynômes *premiers entre eux dans leur ensemble*. Le théorème de Bézout s'applique à des polynômes premiers entre eux dans leur ensembles.

Théorème - Lemme de Gauss

Soient $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $A \wedge B = 1$ alors $A \mid C$.

Démonstration. Même preuve que dans $\mathbb{Z}$. □

Théorème - Produit de polynômes

Soient $A, B, P \in \mathbb{K}[X]$.

- Si $A \wedge P = 1$ et $B \wedge P = 1$, alors $AB \wedge P = 1$.
- Si A et B divisent P et $A \wedge B = 1$, alors $AB \mid P$.

Démonstration. Même preuve que dans $\mathbb{Z}$. □

IV Fractions rationnelles

1. Le corps $\mathbb{K}(X)$

Définition - Fraction rationnelle

On introduit un ensemble $\mathbb{K}(X)$ dont les éléments sont notés $\frac{P}{Q}$, où $P, Q \in \mathbb{K}[X]$ et Q est non nul, et tel que si $\frac{P}{Q}, \frac{R}{S} \in \mathbb{K}(X)$, alors

$$\frac{P}{Q} = \frac{R}{S} \quad \Leftrightarrow \quad PS = QR.$$

On appelle les éléments de $\mathbb{K}(X)$ des *fractions rationnelles* à coefficients dans $\mathbb{K}$.

Remarque. On peut construire un tel ensemble comme l'ensemble des classes d'équivalence de la relation $\sim$ définie sur $\mathbb{K}[X] \times \mathbb{K}[X]^\star$ par : $(P, Q) \sim (R, S) \quad \Leftrightarrow \quad PS = QR$. Cette construction est admise ici.

Définition-théorème - Forme irréductible

Si $F \in \mathbb{K}(X)$, alors F s'écrit de manière unique sous la forme $\frac{P}{Q}$ où $P, Q \in \mathbb{K}[X]$, Q est unitaire et $P \wedge Q = 1$. On appelle cette écriture la *forme irréductible* de F.

Démonstration.

- *Existence* : si $F = \frac{A}{B} \in \mathbb{K}(X)$ et D est un PGCD de A et B, alors on peut écrire $A = DP$ et $B = DQ$ avec $P \wedge Q = 1$. On a $\frac{A}{B} = PQ$, et quitte à diviser par $\mathfrak{c}_{\text{dom}}[Q]$, on peut supposer Q unitaire.
- *Unicité* : si $\frac{P}{Q}$ et $\frac{\widetilde{P}}{\widetilde{Q}}$ sont deux formes irréductibles de F, alors $P\widetilde{Q} = Q\widetilde{P}$. Comme $P \wedge Q = 1$ et $\widetilde{P} \wedge \widetilde{Q} = 1$, le lemme de Gauss entraîne que $Q \mid \widetilde{Q}$ et $\widetilde{Q} \mid Q$. Comme les polynômes sont unitaires, on a $Q = \widetilde{Q}$, puis $P = \widetilde{P}$. □

Exemple. La fraction rationnelle $\dfrac{(X-2)^2(X+1)}{X(X-3)^2}$ est sous forme irréductible.

Définition-théorème - Opérations sur $\mathbb{K}(X)$

On munit $\mathbb{K}(X)$ des lois de composition internes $+$ et $\times$ en posant pour $F, G \in \mathbb{K}(X)$ avec $F = \frac{P}{Q}$ et $G = \frac{R}{S}$:

$$F + G = \frac{PS + QR}{QS}, \qquad FG = \frac{PR}{QS}.$$

Muni de ces deux lois, $\mathbb{K}(X)$ est un corps.

Remarques.

- Il convient de remarquer que les opérations définies ci-dessus sont bien définies sur $\mathbb{K}(X)$, c'est-à-dire qu'elles ne dépendent pas du choix des écritures $\frac{P}{Q}$, $\frac{R}{S}$.
- Nous ne vérifions pas ici que les lois ci-dessus confèrent à $\mathbb{K}(X)$ une structure de corps, mais chacune des propriétés se vérifie aisément.

  En particulier, si $F \in \mathbb{K}(X)$ est non nulle, alors $F = \frac{P}{Q}$ admet pour inverse $\frac{Q}{P}$, notée $\frac{1}{F}$.
- On remarque qu'à tout polynôme $P \in \mathbb{K}[X]$ on peut associer la fraction rationnelle $\frac{P}{1}$, et l'application $P \mapsto \frac{P}{1}$ définit même un morphisme injectif d'anneaux de $\mathbb{K}[X]$ sur $\mathbb{K}(X)$.

  En identifiant $P \in \mathbb{K}[X]$ à $\frac{P}{1}$, on peut considérer que $\mathbb{K}[X] \subset \mathbb{K}(X)$, de sorte que $\mathbb{K}[X]$ est un sous-anneau de $\mathbb{K}(X)$.

Définition - Fraction rationnelle dérivée

Si $F = \frac{P}{Q} \in \mathbb{K}(X)$, on introduit la fraction rationnelle F' appelée *fraction rationnelle dérivée* de F définie par

$$F' = \frac{P'Q - PQ'}{Q^2}.$$

Remarques.

- Ici à nouveau, l'opération est bien définie sur $\mathbb{K}(X)$: elle ne dépend pas du choix de l'écriture $\frac{P}{Q}$ de F.
- On peut montrer que la dérivation ainsi définie vérifie les propriétés habituelles : si $F, G \in \mathbb{K}(X)$, alors

$$(F+G)' = F' + G', \qquad (FG)' = F'G + FG', \qquad \left(\frac{F}{G}\right)' = \frac{FG' - F'G}{G^2}.$$

  Par ailleurs, si $P \in \mathbb{K}[X]$, alors $\left(\frac{P}{1}\right)' = \frac{P'}{1}$: la dérivée de P dans $\mathbb{K}(X)$ est la même que sa dérivée dans $\mathbb{K}[X]$.

2. Zéros, pôles, fonctions rationnelles

Définition - Zéros, pôles

Soit $F \in \mathbb{K}(X)$ ayant pour forme irréductible $\frac{P}{Q}$.

- On dit que $\alpha \in \mathbb{K}$ est un *zéro* de F si α est une racine de P.
- On dit que $\alpha \in \mathbb{K}$ est un *pôle* de F si α est une racine de Q.

On appelle multiplicité d'un zéro (*resp.* d'un pôle) de F sa multiplicité comme racine de P (*resp.* de Q).

Exemple. Dans $\mathbb{C}(X)$, la fraction rationnelle $\dfrac{(X-2)(X-3)^2}{(X^2+1)(X+1)}$ a pour zéros 2 et 3, de multiplicités respectives 1 et 2, et pour pôles $-\mathrm{i}, \mathrm{i}, -1$.

Définition - Fonction rationnelle

Soient $F \in \mathbb{K}(X)$ ayant pour forme irréductible $\frac{P}{Q}$ et $\mathcal{D}_F = \{\alpha \in \mathbb{K},,\ Q(\alpha) \neq 0\}$. On appelle *fonction rationnelle* associée à F la fonction

$$\begin{array}{rccc} \widetilde{F} : & \mathcal{D}_F & \to & \mathbb{K} \\ & x & \mapsto & \frac{\widetilde{P}(x)}{\widetilde{Q}(x)} \end{array}$$

On note souvent F au lieu de $\widetilde{F}$.

Remarque. Il est important de bien vérifier que la fraction rationnelle est écrite sous sa forme irréductible pour introduire la fonction rationnelle associée, de manière à ne pas introduire de pôle "artificiels".

3. Degré d'une fraction rationnelle

Définition - Degré d'une fraction rationnelle

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$. On appelle *degré* de F l'entier

$$\deg F = \deg P - \deg Q.$$

Remarques.

- Ici encore, le degré d'une fraction rationnelle est bien défini : il ne dépend pas du choix de l'écriture $\frac{P}{Q}$ de F.
- Le degré d'un polynôme vu comme fraction rationnelle coïncide avec son degré en tant que polynôme.
- Si $F \in \mathbb{K}(X)$, alors $\deg F \in \mathbb{Z} \cup \{-\infty\}$.

Théorème - Degré et opérations

Soient $F, G \in \mathbb{K}(X)$.

- $\deg(F+G) \leqslant \max(\deg F, \deg G)$, avec égalité si $\deg F \neq \deg G$.
- $\deg(FG) = \deg F + \deg G$.

4. Décomposition en éléments simples

Définition-théorème - Partie entière

Soit $F = \frac{A}{B} \in \mathbb{K}(X)$. Il existe un unique polynôme $E \in \mathbb{K}[X]$ et une unique fraction rationnelle $G \in \mathbb{K}(X)$ tels que

$$F = E + G \quad \text{et} \quad \deg G < 0.$$

Le polynôme E est appelé la *partie entière* de F, et est le quotient dans la division euclidienne de P par Q.

Démonstration. On note $A = BQ + R$ la division euclidienne de A par B. On a alors $F = \frac{BQ+R}{B} = Q + \frac{R}{B}$. On a $Q \in \mathbb{K}[X]$ et $\deg \frac{R}{B} = \deg R - \deg B < 0$, d'où l'existence.

Supposons maintenant que $F = E + G = \widehat{E} + \widehat{G}$, où $E, \widehat{E} \in \mathbb{K}[X]$ et $\deg G, \deg \widehat{G} < 0$. Alors $E - \widehat{E} = \widehat{G} - G$, et $\deg(E - \widehat{E}) = \deg(\widehat{G} - G) \leqslant \max(\deg G, \deg \widehat{G}) < 0$. Ainsi, $E - \widehat{E}$ est le polynôme nul, donc $E = \widehat{E}$ et $G = \widehat{G}$. □

Exemple. La fraction rationnelle $F = \dfrac{X^3 + X - 2}{X^2 + 2}$ s'écrit $F = X - \dfrac{X+2}{X^2+2}$, et a pour partie entière X.

Définition - Élément simple

On appelle *élément simple* de $\mathbb{K}(X)$ une fraction rationnelle de la forme $\frac{A}{B^n}$ où $n \in \mathbb{N}^\star$, B est un polynôme irréductible unitaire et $\deg A < \deg B$.

- Les éléments simples de $\mathbb{C}(X)$ sont les fractions rationnelles de la forme

$$\frac{a}{(X-\alpha)^n}, \quad \text{où } a, \alpha \in \mathbb{C},\ n \in \mathbb{N}^\star.$$

- Les éléments simples de $\mathbb{R}(X)$ sont les fractions rationnelles de la forme

$$\frac{a}{(X-\alpha)^n} \quad \text{ou} \quad \frac{cX+d}{(X^2+\beta X+\gamma)^n}, \quad \text{où } a, b, c, \alpha, \beta, \gamma \in \mathbb{R},\ n \in \mathbb{N}^\star, \text{ et } c^2 - 4d < 0.$$

Théorème - Décomposition en éléments simples dans $\mathbb{C}(X)$

Soient $F = \frac{P}{Q} \in \mathbb{K}(X)$ sous forme irréductible et la décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ de Q :

$$Q = \prod_{i=1}^{r} (X - \alpha_i)^{m_i}.$$

Il existe une unique famille $(a_{i,k})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant k \leqslant m_i}}$ de $\mathbb{C}$ telle que

$$F = E + \sum_{i=1}^{r} \sum_{k=1}^{m_i} \frac{a_{i,k}}{(X - \alpha_i)^k},$$

où E est la partie entière de F. Cette écriture est appelée *décomposition en éléments simples* dans $\mathbb{C}(X)$ de F.

Démonstration. Admise. □

Remarque. On dit que la somme $\sum_{k=1}^{m_i} \frac{a_{i,k}}{(X-\alpha_i)^k}$ est la *partie polaire* associée au pôle α_i de F.

Exemples.

– La fraction rationnelle $F = \dfrac{X^3 - 2X + 1}{(X-2)^2(X^2+1)}$ (de partie entière nulle) se décompose en éléments simples sous la forme :

$$F = \frac{a}{(X-2)^2} + \frac{b}{X-2} + \frac{c}{X-\mathrm{i}} + \frac{d}{X+\mathrm{i}}, \quad \text{avec } a, b, c, d \in \mathbb{C}.$$

On note que comme $\overline{F} = F$, l'unicité de la décomposition de F entraîne que, comme les deux dernières fractions sont conjuguées, on a $d = \bar{c}$.

– On a : $\dfrac{X}{(X^2+X+1)^2} = \dfrac{X}{((X-\mathrm{j})(X-\bar{\mathrm{j}}))^2} = \dfrac{a}{(X-\mathrm{j})^2} + \dfrac{b}{X-\mathrm{j}} + \dfrac{\bar{a}}{(X-\bar{\mathrm{j}})^2} + \dfrac{\bar{b}}{X-\bar{\mathrm{j}}}$, avec $a, b \in \mathbb{C}$.

Théorème - Décomposition en éléments simples dans $\mathbb{R}(X)$

Soient $F = \frac{P}{Q} \in \mathbb{K}(X)$ sous forme irréductible et la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ de Q :

$$Q = \prod_{i=1}^{r} (X - \alpha_i)^{m_i} \prod_{l=1}^{s} (X^2 + \beta_j X + \gamma_j)^{n_j}.$$

Il existe des familles $(a_{i,k})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant k \leqslant m_i}}$, $(b_{j,l})_{\substack{1 \leqslant j \leqslant s \\ 1 \leqslant l \leqslant n_j}}$, $(c_{j,l})_{\substack{1 \leqslant j \leqslant s \\ 1 \leqslant l \leqslant n_j}}$ de $\mathbb{R}$ uniques telle que

$$F = E + \sum_{i=1}^{r} \sum_{k=1}^{m_i} \frac{a_{i,k}}{(X - \alpha_i)^k} + \sum_{j=1}^{s} \sum_{l=1}^{n_j} \frac{b_{j,l} X + c_{j,l}}{(X^2 + \beta_j X + \gamma_j)^l},$$

où E est la partie entière de F. Cette écriture est appelée *décomposition en éléments simples* dans $\mathbb{R}(X)$ de F.

Démonstration. Admise. □

Exemples.

– On a : $\dfrac{X^3 - X + 1}{X^2 - 4} = X + \dfrac{a}{X-2} + \dfrac{b}{X+2}$, avec $a, b \in \mathbb{R}$.

– On a : $\dfrac{X^3 - 1}{(X^2+X+1)^2} = \dfrac{aX+b}{(X^2+X+1)^2} + \dfrac{cX+d}{X^2+X+1}$, avec $a, b, c, d \in \mathbb{R}$.

Calcul de la partie polaire

Pour calculer les coefficients de la partie polaire de F associée au pôle α, on peut penser aux procédés suivants :

– Si m est la multiplicité du pôle α, on peut multiplier F par $(X - \alpha)^m$ et faire une évaluation en α :

$$F = \frac{a_m}{(X-\alpha)^m} + \ldots + \frac{a_1}{X-\alpha} + G, \quad \text{donc} \quad (X-\alpha)^m F = a_m + G(X-\alpha)^m.$$

Comme α n'est pas un pôle de $(X-\alpha)^m F$ ni de G, on peut évaluer en α, et on obtient a_m.

- On peut multiplier $F \in \mathbb{R}(X)$ par X puis prendre la limite en $+\infty$ ou $-\infty$ de la fonction rationnelle associée.
- Si $F \in \mathbb{R}(X)$, on peut utiliser l'unicité de la décomposition pour établir des relations de conjugaison entre les coefficients associés à des pôles conjugués.
- On peut utiliser des évaluations de F.

Exemple. Cherchons la décomposition en éléments simples dans $\mathbb{R}(X)$ de $F = \dfrac{5X+3}{(X+1)^2(X-1)}$. On a

$$F = \frac{a}{(X+1)^2} + \frac{b}{X+1} + \frac{c}{X-1}, \quad \text{avec} \quad a, b, c \in \mathbb{R}.$$

- On évalue $(X+1)^2 F$ en -1, on obtient $a = 1$.
- On évalue $(X-1)F$ en 1, on obtient $c = 2$.
- On a $xF(x) \underset{x\to+\infty}{\longrightarrow} b + c$, donc $b + c = 0$, et $b = -2$.

Finalement, $F = \dfrac{1}{(X+1)^2} - \dfrac{2}{X+1} + \dfrac{2}{X-1}$.

Le résultat suivant s'ajoute à la liste ci-dessus. Il permet de déterminer le coefficient au numérateur de la partie polaire dans le cas d'un pôle simple.

Théorème - Partie polaire dans le cas d'un pôle simple

Si $F = \frac{P}{Q} \in \mathbb{K}(X)$ et $\alpha \in \mathbb{K}$ est une racine simple de Q, alors la partie polaire de F associée à α est donnée par

$$\frac{a}{X-\alpha}, \quad \text{où} \quad a = \frac{P(\alpha)}{Q'(\alpha)}.$$

Démonstration. Le polynôme Q s'écrit $Q = (X-\alpha)R$, où $R \in \mathbb{K}[X]$ vérifie $R(\alpha) \neq 0$. Par ailleurs, la décomposition en éléments simples de F s'écrit $F = \frac{a}{X-\alpha} + G$, où α n'est pas un pôle de G. En multipliant par $X-\alpha$, on a alors

$$(X-\alpha)F = \frac{P}{R} = a + (X-\alpha)G.$$

En évaluant en α, on trouve $a = \frac{P(\alpha)}{R(\alpha)}$. Par ailleurs, on a $Q' = R + (X-\alpha)R'$, donc $Q'(\alpha) = R(\alpha)$ ce qui conclut. □

Remarque. On note que, dans le résultat qui précède, si α est un pôle de F alors il est simple, et s'il n'est pas un pôle de F, alors la partie polaire est nulle, et ne figure donc pas dans la décomposition en éléments simples.

Théorème - Décomposition en élément simples dans $\mathbb{C}(X)$ de $\frac{P'}{P}$

Soit $P \in \mathbb{C}[X]$ non nul, ayant pour racines distinctes $\alpha_1, \ldots, \alpha_r$ de multiplicités respectives $m_1, \ldots, m_r$. Alors

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

Démonstration. Le polynôme s'écrit sous forme factorisée $P = \lambda \prod_{i=1}^{r} (X-\alpha_i)^{m_i}$. Ainsi, on a

$$P' = \sum_{i=1}^{r} m_i (X-\alpha_i)^{m_i-1} \prod_{\substack{j=1 \\ j\neq i}}^{r} (X-\alpha_j)^{m_j} = \sum_{i=1}^{r} m_i \frac{P}{X-\alpha_i} = P \sum_{i=1}^{r} \frac{m_i}{X-\alpha_i}.$$

d'où le résultat. □

V Interpolation de Lagrange

Résoudre un problème d'interpolation, c'est trouver une fonction qui vérifie une série d'évaluations fixées au préalable. Dans le cas présent, on fixe $x_1, \dots, x_n \in \mathbb{K}$ deux à deux distincts, et $y_1, \dots, y_n \in \mathbb{K}$, et on cherche les polynômes $P \in \mathbb{K}[X]$ tels que

$$\forall i \in [\![1, n]\!],\ P(x_i) = y_i.$$

Définition - Polynômes interpolateurs de Lagrange

On appelle *polynômes interpolateurs de Lagrange* associés à $x_1, \dots, x_n$ les polynômes $L_1, \dots, L_n \in \mathbb{K}_{n-1}[X]$ définis par

$$\forall i \in [\![1, n]\!],\ L_i = \prod_{\substack{k=1 \\ k \neq i}}^{n} \frac{X - x_k}{x_i - x_k}.$$

Exemple. Dans le cas où $n = 2$, on a $L_1 = \dfrac{(X - x_2)(X - x_3)}{(x_1 - x_2)(x_1 - x_3)}$, $L_2 = \dfrac{(X - x_1)(X - x_3)}{(x_2 - x_1)(x_2 - x_3)}$, $L_3 = \dfrac{(X - x_1)(X - x_2)}{(x_3 - x_1)(x_3 - x_2)}$.

Remarque. On a alors pour tout $j \in [\![1, n]\!]$, $L_i(x_j) = \delta_{i,j} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{sinon} \end{cases}$

Théorème - Interpolation de Lagrange

Si $x_1, \dots, x_n \in \mathbb{K}$ sont deux à deux distincts et $y_1, \dots, y_n \in \mathbb{K}$, alors il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que $\forall j \in [\![1, n]\!],\ P(x_j) = y_j$, qui est donné par

$$P = \sum_{i=1}^{n} y_i L_i.$$

Démonstration.

- Pour tout $j \in [\![1, n]\!]$, on a $P(x_j) = \sum_{i=1}^{n} y_i L_i(x_j) = \sum_{i=1}^{n} y_i \delta_{i,j} = y_j$, donc P vérifie bien la propriété.
- Supposons que $P, Q \in \mathbb{K}_{n-1}[X]$ vérifient $\forall j \in [\![1, n]\!],\ P(x_j) = Q(x_j) = y_j$. Alors le polynôme $P - Q \in \mathbb{K}_{n-1}[X]$ a n racines distinctes et est donc nul. Ceci donne $P = Q$, donc l'unicité. □

Exercice 1. Montrer que l'ensemble des polynômes $P \in \mathbb{K}[X]$ tels que $\forall i \in [\![1, n]\!],\ P(x_i) = y_i$ est donné par

$$\left\{ \prod_{i=1}^{n} (X - x_i)\, Q + \sum_{i=1}^{n} y_i L_i,\ Q \in \mathbb{K}[X] \right\}.$$

Rappel. Tout polynôme $P \in \mathbb{K}_n[X]$ s'écrit :

$$P = \sum_{i=1}^{n} P(x_i) L_i.$$

Comme on l'a vu, $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$.