

ARITHMÉTIQUE DES POLYNÔMES.

FRACTIONS RATIONNELLES

Vous avez sans doute déjà remarqué que \mathbf{Z} et $\mathbf{K}[X]$ possèdent certaines similitudes, à commencer par l'existence d'une division euclidienne.

L'existence d'une décomposition en produit de facteurs irréductibles, rencontrée dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$ est pour sa part similaire à la factorisation première d'un entier. Et nous avons déjà mentionné les similarités existant entre valuation p -adique et multiplicité d'une racine.

Pour autant, certaines différences existent, à commencer par le fait que l'anneau \mathbf{Z} ne possède que deux inversibles : $U(\mathbf{Z}) = \{\pm 1\}$, alors que $\mathbf{K}[X]$ en possède bien plus¹ puisque $U(\mathbf{K}[X]) = \mathbf{K}^*$. Ceci a pour conséquence qu'un polynôme possède toujours une infinité de diviseurs, et explique les précautions prises dans la définition des irréductibles de $\mathbf{K}[X]$, plus complexe que celle de la définition de nombre premier : un entier est premier si et seulement si ses seuls diviseurs positifs sont 1 et lui-même, alors qu'un polynôme P est dit irréductible si ses seuls diviseurs sont soit constants, soit de la forme λP , $\lambda \in \mathbf{K}^*$.

¹ Une infinité si \mathbf{K} est infini.

Dans ce chapitre, nous explorons davantage cette similarité en définissant notamment les notions de PGCD et de PPCM dans $\mathbf{K}[X]$, et allons retrouver un certain nombre de théorèmes d'arithmétique (Bézout et Gauss notamment).

Les preuves sont alors souvent quasiment les mêmes que dans \mathbf{Z} (ce qui nous dispensera éventuellement de certaines preuves).

Dans un second temps, nous définirons le corps $\mathbf{K}(X)$ des fractions rationnelles, qui est à l'anneau $\mathbf{K}[X]$ ce que le corps \mathbf{Q} est à \mathbf{Z} .

Nous reviendrons alors sur un résultat admis en début d'année, à savoir la décomposition en éléments simples.

Dans toute la suite, sans plus de précisions, \mathbf{K} désigne un corps quelconque².

² Et comme d'habitude, le programme officiel me demanderait de m'en tenir à $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$.

34.1 ARITHMÉTIQUE DE $\mathbf{K}[X]$

34.1.1 Previously on «Polynômes»

Rappelons la définition d'un polynôme irréductible : un polynôme **non constant** $P \in \mathbf{K}[X]$ est dit irréductible si ses seuls diviseurs sont les polynômes constants³ et les polynômes de la forme λP , $\lambda \in \mathbf{K}^*$.

Ou encore si les seuls diviseurs de P sont de degré 0 ou de degré $\deg P$.

Notons que le fait d'imposer P non constant est similaire au fait de demander que 1 ne soit pas premier : on ne veut pas qu'un inversible soit premier, essentiellement pour avoir l'unicité dans la décomposition en produit de facteurs premiers.

Enfin, rappelons qu'il n'est généralement pas inutile de préciser sur quel corps on entend l'irréductibilité, en particulier pour les polynômes à coefficients réels, qui peuvent être irréductibles dans $\mathbf{R}[X]$ et pas dans $\mathbf{C}[X]$ (c'est par exemple le cas de n'importe quel polynôme de degré 2 de discriminant strictement négatif).

Enfin, nous avons prouvé à l'aide d'une récurrence que tout polynôme non constant de $\mathbf{K}[X]$ est produit d'irréductibles. Mais n'avons énoncé (et prouvé) de résultat d'unicité que dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$. Ce qui nous suffit à peu près toujours, mais possède l'inconvénient

³ Et non nuls puisque 0 ne divise que le polynôme nul.

Alternative

Une autre manière de le dire : un polynôme $P \notin U(\mathbf{K}[X])$ est irréductible si pour tous $(Q, R) \in \mathbf{K}[X]^2$, si $P = QR$ alors $Q \in U(\mathbf{K}[X])$ ou $R \in U(\mathbf{K}[X])$.
Si on remplace $\mathbf{K}[X]$ par \mathbf{Z} , alors on retrouve la définition de nombre premier (en autorisant des premiers négatifs), et la définition a encore du sens pour d'autres anneaux intègres.

de nécessiter le théorème de d'Alembert–Gauss, qui est l'un des rares théorèmes que nous n'avons pas prouvé.

La plupart de l'arithmétique de \mathbf{Z} nécessitait de savoir traiter le cas des nombres positifs, quitte à ajouter un signe.

Pour $\mathbf{K}[X]$, nous aimerions nous cantonner aux polynômes unitaires, quitte à ajouter ensuite un coefficient dominant. Nous utiliserons alors le vocabulaire suivant :

Définition 34.1 – Deux polynômes non nuls P et Q de $\mathbf{K}[X]$ sont dits **associés** s'il existe $\lambda \in \mathbf{K}^*$ tel que $P = \lambda Q$.

Cette définition permet alors de reformuler celle de polynôme irréductible : un polynôme non constant P est irréductible si ses seuls diviseurs sont les polynômes constants⁴ et les polynômes associés à P .

⁴ Qui sont les polynômes associés à 1.

Notons que parmi tous les polynômes associés à un polynôme non nul donné, un et un seul est unitaire.

Remarquons également que deux polynômes associés ont les mêmes diviseurs.

En d'autres termes

La relation «être associé» est une relation d'équivalence sur $\mathbf{K}[X] \setminus \{0\}$ et toute classe d'équivalence contient un unique polynôme unitaire.

34.1.2 PGCD, PPCM

Si A et B sont deux polynômes de $\mathbf{K}[X]$ avec $A \neq 0$, alors l'ensemble de leurs diviseurs communs est bien évidemment non vide, puisqu'il contient tous les polynômes constants, et tous ces diviseurs ont un degré majoré par $\deg(A)$ (et même par $\min(\deg(A), \deg(B))$ si B est également non nul).

Toute partie non vide et majorée de \mathbf{N} admet un plus grand élément, la définition qui suit a bien du sens :

Définition 34.2 – Soient A et B deux polynômes non simultanément nuls de $\mathbf{K}[X]$. On appelle **plus grand commun diviseur (PGCD)** de A et B tout polynôme qui divise à la fois A et B et qui est de degré maximal parmi les tels polynômes. Par convention, si A et B sont nuls, on décrète que seul le polynôme nul est un PGCD de A et B .

Notons tout de suite une différence avec le cas des entiers : on ne parle pas **du** PGCD, mais **d'un** PGCD, un tel polynôme n'étant pas unique : si D est un PGCD de A et B , alors pour tout $\lambda \in \mathbf{K}^*$, λD en est un aussi.

Une question reste ouverte pour l'instant : deux PGCD de A et B sont-ils nécessairement associés ?

Autrement dit

Tout polynôme associé à un PGCD de A et B est encore un PGCD de A et B .

Il est facile de se convaincre que pour tous scalaires non nuls λ et μ , les PGCD de λA et μB sont exactement ceux de A et B .

Et donc quitte à diviser les polynômes par leur coefficient dominant, on pourra, si nécessaire, supposer A et B unitaires.

Exemple 34.3 Exemple fondamental

Si A est un polynôme non nul, alors les PGCD de A et de $0_{\mathbf{K}[X]}$ sont exactement les polynômes associés à A .

En effet, tout polynôme divisant $0_{\mathbf{K}[X]}$, les diviseurs communs de A et $0_{\mathbf{K}[X]}$ sont exactement les diviseurs de A . Ceux de degré maximum sont alors nécessairement de même degré que A (qui est un diviseur de A).

Et un diviseur de A de même degré que A est nécessairement associé à A , car le degré du quotient est nul.

Si D est un diviseur commun de A et B , alors pour tout $(U, V) \in \mathbf{K}[X]^2$, D est un diviseur de $AU + BV$. Et donc un diviseur commun de B et $AU + BV$.

En particulier, si $A = BQ + R$ est la division euclidienne de A par B , alors tout diviseur commun de A et B est diviseur commun de B et $R = A - BQ$.

Rappel

Comme dans \mathbf{Z} , si D divise à la fois A et B , alors il divise tous les $AU + BV$.

Mieux : il s'agit là d'une équivalence, car si D divise B et $A - BQ$, alors il divise B et $A = (A - BQ) + BQ$.

Donc l'ensemble des diviseurs communs de A et B est aussi l'ensemble des diviseurs communs de B et R .

Cette observation était, dans le cas de \mathbf{Z} , à la base de l'algorithme d'Euclide.

Celui-ci reste alors valable : partons de deux polynômes A et B , avec $\deg(B) \leq \deg(A)$.

Notons alors $R_0 = A$, $R_1 = B$.

Posons alors R_2 le reste de la division euclidienne de A par B .

S'il est non nul, soit alors R_3 le reste de la division euclidienne de R_1 par R_2 .

On définit ainsi une suite de polynôme en posant, tant que R_k est non nul, R_{k+1} le reste de la division euclidienne de R_{k-1} par R_k , etc.

La suite $(\deg R_k)_k$ est alors strictement décroissante, et donc est nécessairement finie : il existe un entier $n \in \mathbf{N}$ tel que $R_n = 0_{\mathbf{K}[X]}$.

Comme à chaque étape les diviseurs communs à R_{k-1} et R_k sont les diviseurs communs à R_k et R_{k+1} , les diviseurs communs à $A = R_0$ et $B = R_1$ sont aussi les diviseurs communs à R_{n-1} et $0_{\mathbf{K}[X]}$.

Donc en particulier, les PGCD de A et B sont aussi les PGCD de R_{n-1} et $0_{\mathbf{K}[X]}$. Et donc comme expliqué dans l'exemple ci-dessus, ce sont exactement les polynômes associés à R_{n-1} .

Nous venons donc de prouver le fait suivant :

Proposition 34.4 : Soient A et B deux polynômes de $\mathbf{K}[X]$ non simultanément nuls. Alors tous les PGCD de A et B sont associés entre eux. En particulier, un et un seul d'entre eux est unitaire, et on le note $A \wedge B$ et on l'appelle **PGCD unitaire**⁵ de A et B . Par convention, $0_{\mathbf{K}[X]} \wedge 0_{\mathbf{K}[X]} = 0_{\mathbf{K}[X]}$.

En réalité, nous avons même prouvé mieux :

Proposition 34.5 : Soient A et B deux polynômes de $\mathbf{K}[X]$. Alors $P \in \mathbf{K}[X]$ est un diviseur commun de A et B si et seulement si c'est un diviseur de $A \wedge B$.

Démonstration. ► Si $A = B = 0$, alors $A \wedge B = 0$, et il n'y a rien à prouver.

► Si $A \neq 0$ ou $B \neq 0$, alors avec les notations ci-dessus, nous avons prouvé que les diviseurs communs de A et B sont les diviseurs de R_{n-1} . Or $A \wedge B$ est associé⁶ à R_{n-1} , donc les diviseurs de R_{n-1} sont ceux de $A \wedge B$. □

Comme dans le cas de \mathbf{Z} , ceci signifie que le PGCD qui est défini comme «le plus grand» au sens du degré est aussi le plus grand pour la relation de divisibilité (qui est une relation d'ordre si on la restreint à l'ensemble des polynômes unitaires⁷).

Enfin, nous disposons d'un algorithme pour calculer $A \wedge B$: c'est l'unique polynôme **unitaire** associé au dernier reste non nul dans l'algorithme d'Euclide.

Exemple 34.6

Considérons $A = 2X^3 - 4X - 8$ et $B = 3X^2 - 3X - 6$. Alors

$$A = \frac{2}{3}(X+1)B + (2X-4), \quad B = \frac{3}{2}(2X-4)(X+1) + 0$$

et donc $A \wedge B$ est associé à $2X - 4$ et étant unitaire, c'est $X - 2$.

Proposition 34.7 (Identité de Bézout) : Soient A, B deux polynômes de $\mathbf{K}[X]$, non simultanément nuls. Alors il existe $(U, V) \in \mathbf{K}[X]^2$ tels que $AU + BV = A \wedge B$.

Démonstration. Le résultat peut se prouver par exemple par récurrence sur le degré de B , et la preuve ressemble alors beaucoup à celle que nous avons donnée pour les entiers.

Remarque

◀ Nous venons donc de prouver le lemme d'Euclide.

⁵ Et par abus de langage, nous l'appellerons souvent le PGCD de A et B .

⁶ Plus précisément, c'est R_{n-1} divisé par son coefficient dominant.

⁷ Résultat à comparer au fait que la divisibilité n'est pas une relation d'ordre sur \mathbf{Z} , mais l'est sur \mathbf{N} .

Plus précisément, à A non nul fixé, on prouverait $\mathcal{P}(d)$: «pour tout polynôme $B \in \mathbf{K}[X]$ de degré d , il existe $U, V \in \mathbf{K}[X]$ tels que $AU + BV = A \wedge B$ » en procédant à une récurrence forte.

Mais plus simplement, souvenons-nous que, comme dans le cas des polynômes, on peut «remonter les étapes» de l'algorithme d'Euclide pour obtenir une relation de Bézout (et on appelle alors encore ce procédé l'algorithme d'Euclide *étendu*). \square

Exemple 34.8

Dans l'exemple précédent⁸,

$$X - 2 = \frac{1}{2}A - \frac{X + 1}{3}B.$$

On retrouve alors les propriétés déjà connues du PGCD d'entiers, dont les preuves s'adaptent sans difficultés.

Proposition 34.9 : Soit A, B, C trois polynômes de $\mathbf{K}[X]$. Alors :

1. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$ (associativité du PGCD)
2. $(AC) \wedge (BC)$ est associé à $C(A \wedge B)$.

Démonstration. Il s'agit d'adapter les preuves données dans \mathbf{Z} , et seul le cas où $C \neq 0$ nécessite des explications.

1) Si D divise $A \wedge (B \wedge C)$, alors D divise à la fois A et $B \wedge C$, alors il divise A, B et C . En particulier, il divise $A \wedge B$ (puisque'il divise A et B), et divise C . Donc il divise $(A \wedge B) \wedge C$. On prouve sur le même principe que si D divise $(A \wedge B)$ et C , alors il divise $A \wedge (B \wedge C)$. Autrement dit, $(A \wedge B) \wedge C$ et $A \wedge (B \wedge C)$ ont les mêmes diviseurs. Donc ont mêmes diviseurs de plus haut degré, et donc même diviseur unitaire de plus haut degré.

2) Puisque $A \wedge B$ divise A et B , $C(A \wedge B)$ divise AC et BC .
Donc divise $(AC) \wedge (BC)$.

Inversement, puisque C divise AC et BC , il divise $(AC) \wedge (BC)$.

Donc il existe $D \in \mathbf{K}[X]$ tel que $(AC) \wedge (BC) = CD$.

Mais alors $CD \mid AC$, et donc⁹ $D \mid A$. De même $D \mid B$, et donc $D \mid (A \wedge B)$.

Après multiplication par C , $(AC) \wedge (BC) = CD \mid C(A \wedge B)$.

Donc $(AC) \wedge (BC)$ et $C(A \wedge B)$ sont associés. \square

34.1.3 Polynômes premiers entre eux

Définition 34.10 – Deux polynômes non simultanément nuls A et B sont dits **premiers entre eux** si $A \wedge B = 1$ (ce qui est le cas si et seulement si tous¹⁰ leurs PGCD sont constants).

Remarque. Dans $\mathbf{C}[X]$, deux polynômes P et Q sont premiers entre eux si et seulement si ils n'ont pas de racine commune.

En effet, s'ils ont une racine commune α , alors tous deux sont divisibles par $X - \alpha$, et donc $P \wedge Q$ aussi, si bien que $P \wedge Q \neq 1$.

Et inversement, si P et Q ne sont pas premiers entre eux, alors $P \wedge Q$ n'est pas constant, et donc possède une racine α qui est donc une racine commune de P et Q .

Notons que ceci ne vaut plus dans $\mathbf{R}[X]$, par exemple $X^2 + 1$ et $(X^2 + 1)^2$ n'ont pas de racines réelle, donc n'en ont pas en commun. Mais ne sont clairement pas premiers entre eux, puisque l'un divise l'autre.

⁸ Pas totalement intéressant puisqu'il ne s'agit de «remonter» qu'une seule division.

Remarque

Noter la différence subtile avec l'énoncé correspondant pour les entiers, qui était

$$(ka) \wedge (kb) = |k|(a \wedge b).$$

La valeur absolue (dont le but était d'éliminer un éventuel signe moins) a été remplacée par «est associé» (qui sert à éliminer un éventuel coefficient dominant de C).

⁹ Notons qu'on utilise ici l'intégrité de $\mathbf{K}[X]$.

¹⁰ En fait dès que l'un des PGCD est constant, les autres le sont aussi, puisqu'associés à un polynôme constant.

Exercice

Prouver que deux polynômes de $\mathbf{R}[X]$ sont premiers entre eux (en tant que polynômes de $\mathbf{R}[X]$) si et seulement si ils n'ont pas de racine complexe en commun.

Proposition 34.11 (Théorème de Bézout) : Soient $A, B \in \mathbf{K}[X]$. Alors A et B sont premiers entre eux si et seulement si il existe $(U, V) \in \mathbf{K}[X]^2$ tel que $AU + BV = 1$.

Démonstration. Adaptons la preuve donnée dans le cas de \mathbf{Z} . Le sens direct a déjà été fait c'est l'identité de Bézout.

Supposons qu'il existe U et V tels que $AU + BV = 1$. Alors tout diviseur commun de A et B divise $AU + BV$, donc est constant.

En particulier, $A \wedge B$ est donc un polynôme constant unitaire : il vaut 1. \square

Toutes les conséquences directes de Bézout dans \mathbf{Z} restent valables, avec les mêmes preuves dans $\mathbf{K}[X]$.

Corollaire 34.12 – Soient $P, Q_1, \dots, Q_n \in \mathbf{K}[X]$. Alors P est premier avec le produit $Q_1 \cdots Q_n$ si et seulement si il est premier avec chacun des Q_i .

Démonstration. La preuve est la même que dans \mathbf{Z} , il suffit de le prouver pour $n = 2$, puis de raisonner par récurrence.

Pour $n = 2$, supposons que $P \wedge Q_1 = P \wedge Q_2 = 1$.

Alors il existe des polynômes U_1, U_2, V_1, V_2 tels que

$$1 = PU_1 + Q_1V_1, \quad 1 = PU_2 + Q_2V_2.$$

En multipliant ces deux relations, on arrive à

$$1 = P(PU_1U_2 + U_1Q_2V_2 + U_2Q_1V_1) + Q_1Q_2V_1V_2$$

ce qui par le théorème de Bézout nous donne $P \wedge Q_1Q_2 = 1$.

Inversement, si $P \wedge Q_1Q_2 = 1$, alors il existe U, V tels que $PU + Q_1Q_2V = 1$, et donc $PU + Q_1(Q_2V) = 1$, donc $P \wedge Q_1 = 1$, et de même pour Q_2 . \square

Proposition 34.13 (Théorème de Gauss) : Soient A, B, C trois polynômes de $\mathbf{K}[X]$ tels que A divise BC et A soit premier avec B . Alors A divise C .
Autrement dit : $(A \mid BC \text{ et } A \wedge B = 1) \Rightarrow A \mid C$.

Démonstration. Soient U, V tels que $AU + BV = 1$. Alors $ACU + BCV = C$.

Mais A divise ACU et A divise BC , donc BCV . Donc A divise C . \square

On retrouve également le fait que si A et B sont deux polynômes, alors il existe A_0 et B_0 premiers entre eux tels que $A = A_0(A \wedge B)$ et $B = B_0(A \wedge B)$.

Enfin, les polynômes irréductibles étant analogues aux entiers premiers, on retrouve aussi les deux faits suivants¹¹ :

Proposition 34.14 : Soit $P \in \mathbf{K}[X]$ irréductible.

1. Si P ne divise pas Q , alors $P \wedge Q = 1$.
2. P divise un produit si et seulement si il divise l'un de ses facteurs.

¹¹ Analogues aux propositions 16.48 et 16.49, dont les preuves se transposent sans difficultés au cas des polynômes.

34.1.4 Factorisation en produit d'irréductibles

Nous avons déjà mentionné¹² le fait que tout polynôme non nul de $\mathbf{K}[X]$ s'écrit comme produit de polynômes irréductibles.

Où l'on considère que 1 est le produit de zéro irréductibles. Cette décomposition est en fait unique... pour peu qu'on formule bien cette unicité :

¹² Et prouvé dans le chapitre de polynômes.

Théorème 34.15 : Soit $A \in \mathbf{K}[X]$ non constant. Alors il existe $\alpha \in \mathbf{K}^*$, et des polynômes irréductibles **unitaires** P_1, \dots, P_r , deux à deux distincts, et des entiers strictement positifs m_1, \dots, m_r tels que

$$A = \alpha \prod_{i=1}^r P_i^{m_i}.$$

Cette décomposition est unique à l'ordre des facteurs près.

Notons que pour l'unicité, il est important de demander aux polynômes d'être unitaires¹³, faute de quoi on pourrait remplacer l'un des P_i par λP_i , avec $\lambda \neq 0$, quitte à changer α en $\frac{\alpha}{\lambda^{m_i}}$.

«À l'ordre des facteurs près» est suffisamment explicite, mais on pourrait¹⁴ aussi le formuler de la manière suivante : si $A = \alpha \prod_{i=1}^r P_i^{m_i}$ et $A = \beta \prod_{i=1}^p Q_i^{n_i}$ sont deux décompositions de la forme annoncée, alors $\alpha = \beta$, $\{P_1, \dots, P_r\} = \{Q_1, \dots, Q_p\}$ (et donc $r = p$), et pour tout $i \in \llbracket 1, p \rrbracket$, si $P_i = Q_j$, alors $m_i = n_j$.

Démonstration. Il serait tout à fait possible de calquer la preuve faite dans \mathbf{Z} pour l'unicité de la décomposition en produit de nombres premiers.

Donnons une autre preuve pour varier les plaisirs.

Supposons par l'absurde qu'une décomposition ne soit pas toujours unique, et soit P un polynôme de degré minimal parmi ceux possédant deux décompositions distinctes. Considérons alors deux telles décompositions :

$$P = \alpha \prod_{i=1}^r P_i^{m_i} = \beta \prod_{i=1}^p Q_i^{n_i}$$

avec les P_i et les Q_j irréductibles, unitaires, et deux à deux distincts.

Par identification des coefficients dominants, on a tout de suite $\alpha = \beta$. Alors P_1 divise le produit $\prod_{i=1}^p Q_i^{n_i}$.

S'il était premier avec tous les Q_i , il le serait avec le produit, et on aurait alors $P_1 = 1$, contredisant son irréductibilité.

Donc P_1 n'est pas premier avec l'un des Q_i . Quitte à permuter ces derniers, supposons qu'il s'agit de Q_1 .

Mais alors $P_1 \wedge Q_1$ est un diviseur non constant de P_1 et de Q_1 .

Ces deux polynômes étant irréductibles, on a donc $P_1 = P_1 \wedge Q_1 = Q_1$.

Et donc $P_1^{m_1-1} \prod_{i=2}^r P_i^{m_i} = Q_1^{n_1-1} \prod_{i=2}^p Q_i^{n_i}$ est un polynôme de degré strictement plus petit que P , possédant deux décompositions distinctes en produits d'irréductibles, c'est absurde. \square

Comme la description des irréductibles de $\mathbf{C}[X]$ (les polynômes de degré 1) et des irréductibles de $\mathbf{R}[X]$ (les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif) restent valables, ce résultat permet de retrouver, dans un cadre plus général, la décomposition déjà connue.

Notons que les m_i qui apparaissent dans la décomposition sont les analogue polynomiaux de la valuation p -adique. Et pour tout irréductible P , on pourrait noter $v_P(Q)$ la plus grande puissance de P qui divise Q .

Dans le cas de \mathbf{C} , où la description des irréductibles unitaires est extrêmement simple¹⁵, la valuation de $X - \alpha$ n'est rien d'autre que la multiplicité de α en tant que racine de P .

Et on retrouverait alors un moyen de calculer le PGCD de deux polynômes à partir de leurs décompositions en produit d'irréductibles :

$$P \wedge Q = \prod_{R \text{ irréductibles unitaires}} R^{\min(v_R(P), v_R(Q))}.$$

¹³ Tout comme on demandait aux nombres premiers d'être positifs.

¹⁴ Je ne dis pas que c'est là une bonne idée.

¹⁵ Ce sont les $X - \alpha$, $\alpha \in \mathbf{C}$.

Pour finir, notons une vraie différence avec le cas de nombres premiers : dans \mathbf{Z} , on dispose du crible d'Ératosthène qui permet de lister les nombres premiers, et qui tient au fait que les entiers sont ordonnés. Dans $\mathbf{K}[X]$, on n'a rien de tel, donc déterminer si un polynôme est ou non irréductible est déjà potentiellement difficile¹⁶, mais en plus, déterminer quels sont les facteurs irréductibles d'un polynôme donné n'est pas chose aisée.

¹⁶ Sur \mathbf{C} ou sur \mathbf{R} ça ne l'est pas, mais dans $\mathbf{Q}[X]$, ça le devient.

34.1.5 PPCM

Définition 34.16 – Soient $A, B \in \mathbf{K}[X]$ non nuls. On appelle **plus petit commun multiple (PPCM)** de A et B tout polynôme de degré minimal parmi l'ensemble des multiples communs non nuls de A et B (c'est-à-dire l'ensemble des polynômes divisibles à la fois par A et par B).

Si $A = 0$ ou $B = 0$, par convention, 0 est le seul PPCM de A et B (c'est de toutes façons le seul multiple commun de A et B).

Un tel PPCM existe nécessairement : l'ensemble des multiples communs à A et B est non vide (il contient AB), et l'ensemble des degrés des tels multiples communs est donc une partie non vide et minorée¹⁷ de \mathbf{N} , donc contient un plus petit élément d . Tout multiple commun de A et B de degré d est donc un PPCM de A et B .

¹⁷ Par $\max(\deg(A), \deg(B))$.

Comme pour le PGCD, il n'y a pas d'unicité d'un tel polynôme, puisque si P est un PPCM de A et B , alors tous les polynômes associés à P le sont aussi.

Proposition 34.17 : Soient A et B deux polynômes non nuls. Alors il existe un unique PPCM unitaire de A et B qu'on note alors $A \vee B$.

Démonstration. L'existence d'un PPCM unitaire est évidente : il suffit de prendre un PPCM et de le diviser par son coefficient dominant.

Supposons donc que P_1, P_2 soient deux tels PPCM unitaires.

Notons alors $P_1 = P_2Q + R$ la division euclidienne de P_1 par P_2 .

Alors $R = P_1 - P_2Q$ est divisible à la fois par A et par B , donc est un multiple commun de A et B . Étant de degré strictement inférieur à P_2 , il est donc nul.

Donc $P_2 \mid P_1$ et sur le même principe, $P_1 \mid P_2$.

On en déduit que P_1 et P_2 sont associés, et étant tous deux unitaires, ils sont égaux. \square

Corollaire 34.18 – Les PPCM de A et B sont les polynômes associés à $A \vee B$, c'est-à-dire les $\lambda(A \vee B)$, $\lambda \in \mathbf{K}^*$.

Démonstration. Si P est un PPCM de A et B , de coefficient dominant $\lambda \in \mathbf{K}^*$, alors $\frac{P}{\lambda}$ est encore un PPCM de A et B , unitaire.

Par la proposition précédente, c'est donc $A \vee B : \frac{P}{\lambda} = A \vee B \Leftrightarrow P = \lambda(A \vee B)$. \square

Par conséquent, on dispose d'une description de tous les PPCM de A et B : ce sont tous les polynômes associés à $A \vee B$.

On dispose alors d'une caractérisation du PPCM similaire à celle qui existe dans \mathbf{Z} :

Proposition 34.19 : Soient A et B deux polynômes non nuls, et soit $P \in \mathbf{K}[X]$. Alors P est un PPCM de A et B si et seulement si

$$\begin{cases} A \mid P \text{ et } B \mid P \\ \forall Q \in \mathbf{K}[X], (A \mid Q \text{ et } B \mid Q) \Rightarrow P \mid Q \end{cases}$$

Démonstration. \Rightarrow Soit P un PPCM de A et B (donc de la forme $\lambda(A \vee B)$, avec $\lambda \in \mathbf{K}^*$) et soit $Q \in \mathbf{K}[X]$ un multiple commun de A et B . Notons alors $Q = PM + R$ la division euclidienne de Q par P , avec $\deg R < \deg P$.

Alors $R = Q - PM$ est divisible à la fois par A et par B , et étant de degré strictement inférieur à celui de P , il est nul.

Donc $P \mid Q$.

\Leftarrow Soit P un polynôme possédant les propriétés requises. Alors c'est un multiple commun de A et B , qui divise¹⁸ $A \vee B$.

Mais par le sens direct, on a également $A \vee B \mid P$, et donc P et $A \vee B$ sont associés, de sorte que P est un PPCM de A et B . \square

¹⁸ C'est la seconde hypothèse de l'accolade ci-dessus, appliquée à $Q = A \vee B$.

On dispose également d'une formule liant PPCM et PGCD, si A et B sont deux polynômes **unitaires** de $\mathbf{K}[X]$, alors $AB = (A \vee B)(A \wedge B)$.

En revanche, si A et B ne sont pas unitaires, il faudra multiplier le terme de droite par le produit des coefficients dominants de A et B pour obtenir l'égalité.

34.1.6 Généralisation à un nombre fini de polynômes

Comme dans \mathbf{Z} , la notion de PGCD se généralise à un nombre fini de polynômes :

Proposition 34.20 : Soient A_1, \dots, A_n des polynômes non tous nuls de $\mathbf{K}[X]$. Alors il existe un unique polynôme unitaire D qui divise tous les A_i et tel que tout polynôme P qui divise tous les A_i divise D .

On dit alors que D est le PGCD de A_1, \dots, A_n , et on le note $A_1 \wedge A_2 \cdots \wedge A_n$ ou $\bigwedge_{i=1}^n A_i$.

Démonstration. Par récurrence sur n , l'idée étant qu'un polynôme P est un diviseur commun à A_1, A_2 et A_3 si et seulement si il divise à la fois $A_1 \wedge A_2$ et A_3 .

Donc si et seulement si il divise à la fois $(A_1 \wedge A_2) \wedge (A_3)$. \square

Remarque

Ce principe montre que

$$\bigwedge_{i=1}^n A_i = \left(\bigwedge_{i=1}^{n-1} A_i \right) \wedge A_n.$$

Proposition 34.21 : Si D est le PGCD de A_1, \dots, A_n , alors il existe $U_1, \dots, U_n \in \mathbf{K}[X]$

tels que $D = \sum_{i=1}^n A_i U_i$.

Définition 34.22 – Des polynômes $A_1, \dots, A_n \in \mathbf{K}[X]$ sont dits **premiers dans leur ensemble** si $A_1 \wedge \cdots \wedge A_n = 1$.

Comme pour les entiers, on ne confondra pas premiers deux à deux et premiers dans leur ensemble. Le premier implique le second, mais la réciproque est fautive.

Exemple 34.23

Dans $\mathbf{C}[X]$, A_1, \dots, A_n sont premiers entre eux dans leur ensemble si et seulement si il n'existe pas de racine commune à tous les A_i , soit encore si

$$\forall \lambda \in \mathbf{C}, \exists i \in \llbracket 1, n \rrbracket, A_i(\lambda) \neq 0.$$

En effet, s'ils sont premiers entre eux, aucun polynôme irréductible ne les divise tous à la fois. Or les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1.

Et inversement, s'ils ont une racine commune λ , alors leur PGCD est divisible par $X - \lambda$, donc les A_i ne sont pas premiers entre eux.

34.2 FRACTIONS RATIONNELLES

34.2.1 Le corps $\mathbf{K}(X)$ des fractions rationnelles

Les fractions rationnelles, que nous avons rencontrées de manière informelle en début d'année sont l'analogie pour $\mathbf{K}[X]$ de ce que \mathbf{Q} est à \mathbf{Z} .

Qu'est-ce qu'un rationnel ? C'est la donnée d'un numérateur et d'un dénominateur, c'est-à-dire d'un couple $(p, q) \in \mathbf{Z} \times \mathbf{Z}^*$.

Mais vous savez que deux fractions peuvent être égales sans avoir le même numérateur ni le même dénominateur.

On identifie les rationnels $\frac{p}{q}$ et $\frac{p'}{q'}$ si et seulement si $pq' = p'q$.

Procédons de même avec des couples de polynômes.

À cet effet, définissons une relation binaire \sim sur $\mathbf{K}[X] \times (\mathbf{K}[X] \setminus \{0\})$ par

$$(P_1, Q_1) \sim (P_2, Q_2) \Leftrightarrow P_1Q_2 = P_2Q_1.$$

Alors \sim est évidemment réflexive et symétrique.

Et si $(P_1, Q_1) \sim (P_2, Q_2)$ et $(P_2, Q_2) \sim (P_3, Q_3)$, alors on a $P_1Q_2 = P_2Q_1$ et $P_2Q_3 = P_3Q_2$ donc en multipliant ces relations,

$$P_1P_2Q_2Q_3 = Q_1P_2Q_2P_3. \quad (\star)$$

- ▶ si $P_2 = 0$, alors $P_1Q_2 = 0$, et Q_2 étant non nul, $P_1 = 0$. Et de même $P_3 = 0$. Donc $P_1Q_3 = 0 = Q_1P_3$, de sorte que $(P_1, Q_1) \sim (P_3, Q_3)$.
- ▶ si $P_2 \neq 0$, alors $P_2Q_2 \neq 0$, et donc par intégrité de $\mathbf{K}[X]$, en simplifiant (\star) par P_2Q_2 , il reste $P_1Q_3 = P_3Q_1$, donc $(P_1, Q_1) \sim (P_3, Q_3)$.

Donc \sim est transitive, et donc est une relation d'équivalence sur $\mathbf{K}[X] \times \mathbf{K}[X] \setminus \{0\}$.

Définition 34.24 – L'ensemble $\mathbf{K}(X)$ des fractions rationnelles sur \mathbf{K} est l'ensemble des classes d'équivalence de la relation \sim .

On note $\frac{P}{Q}$ la classe d'équivalence de (P, Q) . On dit alors que (P, Q) est un **représentant** de la fraction $\frac{P}{Q}$.

La définition est en fait peu importante, et si vous avez compris ce qu'est un nombre rationnel, vous aurez compris ce qu'est une fraction rationnelle : c'est $\frac{P}{Q}$ avec la convention que $\frac{P_1}{Q_1} = \frac{P_2}{Q_2} \Leftrightarrow P_1Q_2 = Q_1P_2$.

Proposition 34.25 : Tout élément F de $\mathbf{K}(X)$ s'écrit $F = \frac{P}{Q}$ avec $P \wedge Q = 1$.
On dit alors que (P, Q) est un représentant irréductible de F .

Démonstration. Supposons que $F = \frac{A}{B}$, avec $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X] \setminus \{0\}$.

Soit alors $D = A \wedge B$, de sorte qu'il existe $P, Q \in \mathbf{K}[X]$ tels que $A = DP$ et $B = DQ$, $P \wedge Q = 1$.

On a alors $AQ = DPQ = PDQ = PB$, de sorte que $\frac{P}{Q} = \frac{A}{B} = F$. □

Par abus de langage, on dira souvent que $\frac{P}{Q}$ est irréductible, plutôt que de dire que (P, Q) est un représentant irréductible de $\frac{P}{Q}$.

Si $\frac{A}{B}$ et $\frac{C}{D}$ sont deux représentants irréductibles de la même fraction, alors $AD = BC$. Puisque $A \wedge B = 1$, par le lemme de Gauss, $A \mid C$. Et de même, $C \mid A$, donc A et C sont associés.

Il existe donc $\lambda \in \mathbf{K}^*$ tel que $C = \lambda A$.

Si $A \neq 0$, on a donc $AD = BC \Leftrightarrow AD = \lambda AB \Leftrightarrow D = \lambda B$.

Autrement dit

Un représentant d'une fraction est donc tout élément dans la classe d'équivalence qu'est cette fraction.

Unicité ?

Vous aurez noté qu'on a là un résultat d'existence, mais pas d'unicité. En effet, multiplier P et Q par une constante donnerait encore deux polynômes premiers entre eux. Une telle unicité serait par exemple garantie en demandant de plus à ce que Q soit unitaire (analogue à l'unicité de la représentation irréductible d'un rationnel où l'on demande au dénominateur d'être positif).

⚠ Attention !

Cette terminologie laisse entendre qu'il existerait des fractions rationnelles irréductibles et d'autres qui ne le sont pas, ce qui n'est pas le cas : il n'y a pas de notion de fraction irréductible. Mais pour toute fraction, il y a des représentants irréductibles.

Ainsi, si $\frac{A}{B} \neq 0$ est irréductible, les autres représentants irréductibles de cette même fraction sont les $\frac{\lambda A}{\lambda B}$, $\lambda \in \mathbf{C}^*$.

Soient $F = \frac{A}{B}$ et $G = \frac{C}{D}$ deux éléments de $\mathbf{K}(X)$.

On définit alors une fraction rationnelle notée $F + G$ de la manière suivante :

$$F + G = \frac{AD + BC}{BD}.$$

Autrement dit, il s'agit de la classe d'équivalence du couple $(AD + BC, BD)$. Mais il n'est pas totalement évident au premier abord que cette classe d'équivalence soit indépendante des représentants de F_1 et F_2 qu'on a choisis précédemment.

Supposons donc que $F = \frac{A_1}{B_1} = \frac{A_2}{B_2}$ et $G = \frac{C_1}{D_1} = \frac{C_2}{D_2}$. Alors

$$(A_1 D_1 + B_1 C_1) B_2 D_2 = (A_1 B_2) D_1 D_2 + (C_1 D_2) B_1 B_2 = A_2 B_1 D_1 D_2 + C_2 D_1 B_1 B_2 = (A_2 D_2 + B_2 C_2) B_1 D_1$$

de sorte qu'on a bien $\frac{A_1 D_1 + B_1 C_1}{B_1 D_1} = \frac{A_2 D_2 + B_2 C_2}{B_2 D_2}$, et donc $F + G$ est uniquement défini.

Nous définissons donc ainsi une loi interne $+$ sur $\mathbf{K}(X)$.

Il n'est pas très difficile, en utilisant les propriétés des opérations de $\mathbf{K}[X]$ de prouver que $+$ est associative et commutative.

Par exemple, pour l'associativité, on a :

$$\left(\frac{A}{B} + \frac{C}{D}\right) + \frac{E}{F} = \frac{AD + BC}{BD} + \frac{E}{F} = \frac{ADF + BCF + EBD}{BDF} \quad \text{et} \quad \frac{A}{B} + \left(\frac{C}{D} + \frac{E}{F}\right) = \frac{A}{B} + \frac{CF + DE}{DF} = \frac{ADF + BCF + BDE}{BDF}$$

de sorte que ces deux fractions sont égales.

La fraction $0 = \frac{0}{1}$ est alors élément neutre de $+$ puisque

$$\forall \frac{A}{B} \in \mathbf{K}(X), \quad \frac{A}{B} + \frac{0}{1} = \frac{A + 0 \cdot B}{B \cdot 1} = \frac{A}{B}.$$

Et de plus, tout élément de $\mathbf{K}(X)$ est inversible, et l'inverse de $\frac{A}{B}$ est $\frac{-A}{B}$.

Autrement dit, nous venons de prouver que $(\mathbf{K}(X), +)$ est un groupe abélien.

Sur le même principe, on peut définir une seconde loi interne notée \times sur $\mathbf{K}(X)$, définie

$$\text{par } \frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1 P_2}{Q_1 Q_2}.$$

On vérifie alors qu'il s'agit là d'une loi associative et commutative¹⁹, d'élément neutre $\frac{1}{1}$, et qui est distributive par rapport à $+$.

De plus, toute fraction $\frac{A}{B} \neq \frac{0}{1}$ est inversible, d'inverse $\frac{B}{A}$.

Donc $(\mathbf{K}(X), +, \times)$ est un corps.

On note 0 plutôt que $\frac{0}{1}$, et plus généralement, pour tout $P \in \mathbf{K}[X]$, on note P plutôt que $\frac{P}{1}$.

On vérifie aisément que les opérations de $\mathbf{K}(X)$ correspondent à celle de $\mathbf{K}[X]$, et donc qu'en identifiant la fraction rationnelle $\frac{P}{1}$ au polynôme P , $\mathbf{K}(X)$ contient l'anneau $\mathbf{K}[X]$.

Et donc en particulier contient \mathbf{K} , qui est lui-même inclus²⁰ dans $\mathbf{K}[X]$.

La multiplication interne induit alors une opération $\cdot : \begin{cases} \mathbf{K} \times \mathbf{K}(X) & \longrightarrow \mathbf{K}(X) \\ (\lambda, F) & \longmapsto \lambda F \end{cases}$, qui avec l'addition, fait de $\mathbf{K}(X)$ un \mathbf{K} -espace vectoriel²¹.

Cette construction est inévitable si on souhaite définir proprement les fractions rationnelles, mais en pratique, elle ne changera rien à la manière dont vous allez calculer avec des fractions rationnelles. Notons que les mêmes constructions, partant de \mathbf{Z} plutôt que de $\mathbf{K}[X]$ permettent de donner une définition rigoureuse de \mathbf{Q} . Et plus généralement, cette construction est valable dans tout anneau commutatif intègre A , le corps obtenu s'appelant alors le corps des fractions de A .

¹⁹ Cela découle de l'associativité et de la commutativité du produit sur $\mathbf{K}[X]$.

Remarque

Les représentants de 0 sont exactement les $(0, P)$, $P \in \mathbf{K}[X]$. On garde donc bien une propriété usuelle, à savoir qu'une fraction (rationnelle) est nulle si et seulement si son numérateur l'est.

²⁰ Moyennant une identification entre scalaires et polynômes constants.

²¹ De dimension infinie puisqu'il possède $\mathbf{K}[X]$ comme sous-espace vectoriel.

34.2.2 Degré, partie entière, zéros et pôles

Définition 34.26 – Soit $F \in \mathbf{K}(X)$. Alors la quantité $\deg(A) - \deg(B)$ ne dépend pas du représentant $\frac{A}{B}$ de F .
On l'appelle alors le **degré de F** . Notons qu'il s'agit soit d'un entier relatif, soit de $-\infty$, ce qui ne peut se produire que si $F = 0$.

Démonstration. Soient $\frac{A}{B}$ et $\frac{C}{D}$ deux représentants de F .
On a alors $AD = BC$. Et donc


$$\deg(A) + \deg(D) = \deg(B) + \deg(C) \Leftrightarrow \deg(A) - \deg(B) = \deg(C) - \deg(D),$$

donc le degré de F est bien indépendant du représentant choisi. \square

Exemple 34.27

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

Notons que pour un polynôme $P = \frac{P}{1}$, son degré en tant que fraction rationnelle coïncide avec son degré en tant que polynôme.

 Les polynômes sont des fractions rationnelles de degré positif, mais ce n'est pas là une caractérisation de $\mathbf{K}[X]$ dans $\mathbf{K}(X)$: il existe des fractions rationnelles de degré strictement positif qui ne sont pas des polynômes. Par exemple $\frac{X^3}{X^2 - 1}$ est de degré 1, mais n'est pas un polynôme.

Proposition 34.28 : Soient F, G deux fractions rationnelles. Alors

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

Démonstration. Notons $F = \frac{A}{B}$ et $G = \frac{C}{D}$. Alors

$$\begin{aligned} \deg(F + G) &= \deg\left(\frac{AD + BC}{BD}\right) \leq \max(\deg(AD), \deg(BC)) - \deg(BD) \\ &\leq \max(\deg(A) - \deg(B), \deg(C) - \deg(D)) \leq \max(\deg(F), \deg(G)). \end{aligned}$$

Le degré d'un produit est immédiat. \square

Définition 34.29 – Soit $F = \frac{A}{B}$ une fraction rationnelle sous **forme irréductible**.

On appelle alors **zéro de F** toute racine de A et **pôle de F** toute racine de B .

L'**ordre** d'un zéro (resp. d'un pôle) de F est alors sa multiplicité en tant que racine de A (resp. de B).

Si l'on impose à F d'être irréductible dans cette définition, c'est tout simplement pour que les notions de zéro et de pôle soient indépendantes du choix du représentant de F .

Par exemple, $F = \frac{X}{X^2 - 1}$ possède 0 comme seul zéro et ± 1 comme seuls pôles.

Mais on a aussi $F = \frac{X}{X^2 - 1} = \frac{X(X + 3)}{(X^2 - 1)(X + 3)}$.

Cette dernière fraction n'est pas irréductible, et donc bien que -3 soit racine de son numérateur, ce n'est pas un zéro de F .

Définition 34.30 (Fonction rationnelle) – Soit $F = \frac{A}{B}$ une fraction rationnelle sous forme irréductible, et soit E l'ensemble des pôles de F .

On appelle alors **fonction rationnelle associée** à F la fonction

$$\tilde{F} : \begin{cases} \mathbf{K} \setminus E & \longrightarrow \mathbf{K} \\ x & \longmapsto \frac{A(x)}{B(x)}. \end{cases}$$

Encore une fois, prendre une fraction irréductible permet de garantir que le domaine de définition de \tilde{F} est le plus grand possible.

Définition 34.31 – Soit $F \in \mathbf{K}(X)$. Alors il existe un unique couple $(E, Q) \in \mathbf{K}[X] \times \mathbf{K}(X)$, avec $\deg(Q) < 0$ tel que $F = E + Q$.
On dit alors que E est la **partie entière** de F .

Démonstration. L'existence est aisée : si $F = \frac{A}{B}$, notons alors $A = EB + D$ la division euclidienne de A par B , avec $\deg D < \deg B$.

Alors $F = \frac{A}{B} = E + \frac{D}{B}$, avec $\deg \frac{D}{B} = \deg(D) - \deg(B) < 0$.

Pour l'unicité, supposons que $F = E_1 + Q_1 = E_2 + Q_2$, où E_1 et E_2 sont deux polynômes et Q_1, Q_2 deux fractions de degrés strictement négatifs.

Alors $E_1 - E_2 = Q_2 - Q_1$. Mais $\deg(Q_2 - Q_1) \leq \max(\deg Q_2, \deg Q_1) < 0$, et $E_1 - E_2$ est un polynôme, donc de degré positif... sauf s'il est nul !

Il ne peut donc y avoir égalité des degrés que si $E_1 - E_2 = 0 \Leftrightarrow E_1 = E_2$, et alors on a évidemment $Q_1 = Q_2$. \square

Notons tout de suite que l'unicité nous dit que si $\deg F < 0$, alors $F = 0 + F$, donc la partie entière de F est nulle.

Et inversement, une fraction de partie entière nulle est évidemment de degré négatif.

Enfin, il est aisé de prouver que la partie entière d'une somme est la somme des parties entières, mais qu'il n'existe pas de règle analogue pour le produit.

Remarque

Ceci nous donne directement une méthode pour déterminer la partie entière de F : c'est le quotient de la division euclidienne de A par B .

34.2.3 Décomposition en éléments simples

Théorème 34.32 (Décomposition en éléments simples) : Soit $F = \frac{P}{Q} \in \mathbf{K}(X)$

de degré strictement négatif, et soit $Q = Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}$ la décomposition de Q en produit de facteurs irréductibles unitaires.

Alors il existe une unique famille de polynômes $A_{1,1}, \dots, A_{1,\alpha_1}, \dots, A_{n,1}, \dots, A_{n,\alpha_n}$ tels que :

$$\begin{aligned} F &= \frac{A_{1,1}}{Q_1} + \frac{A_{1,2}}{Q_1^2} + \cdots + \frac{A_{1,\alpha_1}}{Q_1^{\alpha_1}} + \frac{A_{2,1}}{Q_2} + \cdots + \frac{A_{2,\alpha_2}}{Q_2^{\alpha_2}} + \cdots + \frac{A_{n,1}}{Q_n} + \cdots + \frac{A_{n,\alpha_n}}{Q_n^{\alpha_n}} \\ &= \sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{Q_i^k}. \end{aligned}$$

avec $\forall i \in \llbracket 1, n \rrbracket, \forall k \in \llbracket 1, \alpha_i \rrbracket, \deg A_{i,k} < \deg Q_i$.

Si le résultat est à connaître, sa preuve est hors programme.

Démonstration. Nous allons raisonner par un argument d'algèbre linéaire, et notamment de dimension : soit $d = \deg Q$, qu'on peut supposer supérieur ou égal à 1, car si $\deg Q = 0$, il n'existe pas de fraction rationnelle de degré négatif ayant Q pour dénominateur.

Notons également, pour $1 \leq i \leq n$, $d_i = \deg Q_i$, de sorte que $d = d_1 \alpha_1 + \cdots + d_n \alpha_n$.

Soit alors $E_1 = \left\{ \frac{U}{Q}, U \in \mathbf{K}_{d-1}[X] \right\}$ l'ensemble des fractions rationnelles de degré strictement

ment négatif qui ont Q pour dénominateur.

Notons également E_2 l'ensemble des $\sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{Q_i^k}$ où $\forall i \in \llbracket 1, n \rrbracket, \forall k \in \llbracket 1, \alpha_i \rrbracket, \deg A_{i,k} < \deg Q_i$, c'est-à-dire l'ensemble des fractions qui se mettent bien sous la forme annoncée. Alors E_1 et E_2 sont des sous-espaces vectoriels de $\mathbf{K}(X)$.

Il est facile de constater que $E_2 \subset E_1$: il suffit de tout mettre au même dénominateur, et de constater que les conditions sur les degrés sont bien remplies. En effet, pour $1 \leq i \leq n$ et $1 \leq k \leq \alpha_i$, on a

$$\frac{A_{i,k}}{Q_i^k} = \prod_{\substack{j=1 \\ j \neq i}}^n Q_j^{\alpha_j} \frac{Q_i^{\alpha_i - k} A_{i,k}}{Q_1^{\alpha_1} \dots Q_n^{\alpha_n}}$$

et si $\deg A_{i,k} < \deg Q_i$, alors

$$\deg \left(\left(\prod_{\substack{j=1 \\ j \neq i}}^n Q_j^{\alpha_j} \right) Q_i^{\alpha_i - k} A_{i,k} \right) < \sum_{\substack{j=1 \\ j \neq i}}^n \alpha_j d_j + d_i(\alpha_i - k) + d_i \leq \sum_{\substack{j=1 \\ j \neq i}}^n \alpha_j d_j + d_i \alpha_i \leq \deg Q.$$

Puisque $(1, X, X^2, \dots, X^{d-1})$ est une base de $\mathbf{K}_{d-1}[X]$, $\left(\frac{1}{Q}, \frac{X}{Q}, \dots, \frac{X^{d-1}}{Q}\right)$ est une base de E_1 , qui est donc de dimension d .

De même, un polynôme $A_{i,k} \in \mathbf{K}_{d_i-1}[X]$ est combinaison linéaire de $1, X, \dots, X^{d_i-1}$, si bien que la famille

$$\frac{1}{Q_1}, \dots, \frac{X^{d_1-1}}{Q_1}, \frac{1}{Q_1^2}, \dots, \frac{X^{d_1-1}}{Q_1^2}, \dots, \frac{X^{d_1-1}}{Q_1^{\alpha_1}}, \frac{1}{Q_2}, \dots, \frac{X^{d_2-1}}{Q_2^{\alpha_2}}$$

est une famille génératrice de E_2 .

Pour le dire autrement, il s'agit de la famille \mathcal{B} des $\frac{X^j}{Q_i^k}$, $1 \leq i \leq n$, $1 \leq k \leq \alpha_i$, $0 \leq j < d_i$.

Sa liberté n'est pas complètement évidente : soient donc des scalaires $\alpha_{i,j,k}$, avec $1 \leq i \leq n$, $1 \leq k \leq \alpha_i$, $0 \leq j < d_i$ tels que

$$\sum_{i=1}^n \sum_{k=1}^{\alpha_i} \sum_{j=0}^{d_i-1} \frac{\alpha_{i,j,k} X^j}{Q_i^k} = 0.$$

Notons $A_{i,k} = \sum_{j=0}^{d_i-1} \alpha_{i,j,k} X^j \in \mathbf{K}_{d_i-1}[X]$, de sorte que

$$\sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{Q_i^k} = 0.$$

Fixons alors $p \in \llbracket 1, n \rrbracket$, de sorte que par une mise au même dénominateur, on obtient

$$\sum_{\substack{i=1 \\ i \neq p}}^n \left[\left(\prod_{\substack{j=1 \\ j \neq i}}^n Q_j^{\alpha_j} \right) \left(\sum_{k=1}^{\alpha_i} Q_i^{\alpha_i - k} A_{i,k} \right) \right] + \left(\prod_{\substack{j=1 \\ j \neq p}}^n Q_j^{\alpha_j} \right) \left(\sum_{k=1}^{\alpha_p} Q_p^{\alpha_p - k} A_{p,k} \right) = 0.$$

$$\text{Et donc } - \sum_{\substack{i=1 \\ i \neq p}}^n \left[\left(\prod_{\substack{j=1 \\ j \neq i}}^n Q_j^{\alpha_j} \right) \left(\sum_{k=1}^{\alpha_i} Q_i^{\alpha_i - k} A_{i,k} \right) \right] = \left(\prod_{\substack{j=1 \\ j \neq p}}^n Q_j^{\alpha_j} \right) \left(\sum_{k=1}^{\alpha_p} Q_p^{\alpha_p - k} A_{p,k} \right). \quad (\star)$$

Comme Q_p divise le membre de gauche, il divise celui de droite.

Mais étant premier avec $\prod_{\substack{j=1 \\ j \neq p}}^n Q_j^{\alpha_j}$, il divise $\sum_{k=1}^{\alpha_p} Q_p^{\alpha_p - k} A_{p,k}$.

Remarque

Il faudrait plutôt dire : dont un représentant possède Q pour dénominateur. Je ne demande pas nécessairement qu'il s'agisse d'un représentant irréductible.

Rappel

Un polynôme est premier avec un produit si et seulement si il est premier avec chacun de ses facteurs.

Et puisque Q_p divise $\sum_{k=1}^{\alpha_p-1} Q_p^{\alpha_p-k} A_{p,k}$, Q_p divise A_{p,α_p} .

Or $\deg A_{p,\alpha_p} < \deg Q_p$, donc $A_{p,\alpha_p} = 0$.

Sur le même principe, si $\alpha_p \geq 2$, en divisant les deux membres de (\star) par Q_p (ce qui est possible puisque $A_{p,\alpha_p} = 0$), et en tenant le même raisonnement, on prouve que $A_{p,\alpha_p-1} = 0$, et de proche en proche que pour tout $k \in \llbracket 1, \alpha_p \rrbracket$, $A_{p,k} = 0$.

Donc tous les $A_{i,k}$ sont nuls, si bien que par unicité des coefficients d'un polynôme, tous les $\alpha_{i,j,k}$ sont nuls : la famille \mathcal{B} est libre, et donc est une base de E_2 .

Or cette famille est de cardinal $\sum_{i=1}^n \sum_{1 \leq k \leq \alpha_i} d_i = \sum_{i=1}^n d_i \alpha_i = d$.

Donc $\dim E_2 = d = \dim E_1$, et puisqu'on a l'inclusion $E_2 \subset E_1$, alors $E_1 = E_2$.

En particulier, F (notre fraction de départ, qui figure dans l'énoncé du théorème), qui est dans E_1 est dans E_2 .

Ce qui prouve déjà l'existence de la décomposition annoncée.

Et puisque \mathcal{B} est une base de $E_2 = E_1$, une telle décomposition est nécessairement unique. \square

Remarque. Si Q_i est de la forme $X - \lambda_i$, c'est-à-dire lorsque λ_i est un pôle de F , alors les $A_{i,k}$ sont tous de degré négatif, et donc sont des constantes²², et on dit alors que $\sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{(X - \lambda_i)^k}$ est la **partie polaire de F associée au pôle λ_i** .

²² Éventuellement nulles.

Définition 34.33 – Une fraction rationnelle est appelée **élément simple** si elle est de la forme $\frac{P}{Q^k}$, avec Q irréductible, $k \geq 1$ et $\deg P < \deg Q$.

Le théorème ci-dessus nous dit donc que toute fraction rationnelle de degré négatif s'écrit de manière unique comme somme d'éléments simples, et précise même quels peuvent être les dénominateurs des éléments simples en question. En prenant en compte la partie entière, toute fraction rationnelle s'écrit donc de manière unique comme un polynôme plus une somme d'éléments simples.

En pratique, seuls les deux énoncés suivants seront à connaître²³, pour la décomposition en éléments simples des fractions à coefficients dans \mathbf{R} ou dans \mathbf{C} . Les deux sont uniquement des conséquences du théorème général, couplés à la description des irréductibles de $\mathbf{C}[X]$ ou de $\mathbf{R}[X]$.

²³ Ou en fait surtout à savoir utiliser.

Corollaire 34.34 (Décomposition en éléments simples dans $\mathbf{C}(X)$) :

Soit $F = \frac{A}{B} \in \mathbf{C}(X)$, avec $B = \alpha \prod_{i=1}^n (X - \lambda_i)^{m_i}$. Alors il existe un unique polynôme $E \in \mathbf{C}[X]$ et une unique famille de complexes $\alpha_{1,1}, \dots, \alpha_{1,m_1}, \alpha_{2,1}, \dots, \alpha_{2,m_2}, \dots, \alpha_{n,m_n}$ tels que

$$\begin{aligned} F &= E + \frac{\alpha_{1,1}}{X - \lambda_1} + \dots + \frac{\alpha_{1,m_1}}{(X - \lambda_1)^{m_1}} + \dots + \frac{\alpha_{n,1}}{X - \lambda_n} + \dots + \frac{\alpha_{n,m_n}}{(X - \lambda_n)^{m_n}} \\ &= E + \sum_{i=1}^n \sum_{k=1}^{m_i} \frac{\alpha_{i,k}}{(X - \lambda_i)^k}. \end{aligned}$$

Démonstration. Il suffit de se souvenir que les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1. \square

Exemple 34.35 Une base de $\mathbf{C}(X)$

Comme mentionné précédemment, $\mathbf{C}(X)$ est un \mathbf{C} -espace vectoriel. Le résultat ci-dessus nous donne une base de $\mathbf{C}(X)$, qui est

$$\mathcal{B} = \{X^k, k \in \mathbf{N}\} \cup \left\{ \frac{1}{(X - \lambda)^k}, (\lambda, k) \in \mathbf{C} \times \mathbf{N}^* \right\}.$$

En effet, la décomposition en éléments simples affirme que toute fraction rationnelle s'écrit de manière unique comme combinaison linéaire²⁴ des éléments de \mathcal{B} .

²⁴ Nécessairement finie.

Corollaire 34.36 (Décomposition en éléments simples dans $\mathbf{R}(X)$) :

Soit $F = \frac{A}{B} \in \mathbf{R}(X)$, où la décomposition en produit de facteurs irréductibles de B est

$$B = \alpha \prod_{i=1}^n (X - \lambda_i)^{m_i} \prod_{k=1}^r (X^2 + b_k X + c_k)^{p_k}.$$

Alors il existe un unique polynôme $E \in \mathbf{R}[X]$ et une unique famille de réels $\alpha_{1,1}, \dots, \alpha_{1,m_1}, \dots, \alpha_{n,m_n}, \beta_{1,1}, \dots, \beta_{1,p_1}, \dots, \beta_{r,p_r}, \gamma_{1,1}, \dots, \gamma_{r,p_r}$ tels que

$$F = E + \sum_{i=1}^n \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - \lambda_i)^j} + \sum_{k=1}^r \sum_{\ell=1}^{p_k} \frac{\beta_{k,\ell} X + \gamma_{k,\ell}}{(X^2 + b_k X + c_k)^\ell}.$$

34.2.4 Décomposition en éléments simples : une autre preuve via l'arithmétique des polynômes

Dans cette partie, on donne, pour la culture, ou pour ceux qui préfèrent l'arithmétique à l'algèbre linéaire, une autre preuve de l'existence et l'unicité de la décomposition en éléments simples.

Lemme 34.37. Soit $F = \frac{A}{B} \in \mathbf{K}(X)$ avec $\deg(F) < 0$. On suppose que $B = B_1 B_2$, avec $B_1 \wedge B_2 = 1$.

Alors il existe un unique couple $(A_1, A_2) \in \mathbf{K}[X]$, avec $\deg A_1 < \deg B_1$ et $\deg A_2 < \deg B_2$,

vérifiant $F = \frac{A_1}{B_1} + \frac{A_2}{B_2}$.

Si de plus $\frac{A}{B}$ est irréductible, alors $\frac{A_1}{B_1}$ et $\frac{A_2}{B_2}$ le sont aussi.

Démonstration. Existence : par Bézout, il existe U et V deux polynômes tels que $B_1 U + B_2 V = 1$, et alors $AB_1 U + AB_2 V = A$.

Donc $\frac{A}{B} = \frac{AB_1 U + AB_2 V}{B_1 B_2} = \frac{AU}{B_2} + \frac{AV}{B_1}$.

Cette écriture n'est pas encore tout à fait celle que l'on cherche car rien ne garantit que $\deg AV < \deg B_1$ et idem pour $\deg(AU)$.

Notons alors E_1 et E_2 les parties entières respectives de $\frac{AV}{B_1}$ et $\frac{AU}{B_2}$, de sorte que

$$\frac{AV}{B_1} = E_1 + \frac{A_1}{B_1} \text{ et } \frac{AU}{B_2} = E_2 + \frac{A_2}{B_2}.$$

Et donc $F = \frac{A}{B} = E_1 + E_2 + \frac{A_1}{B_1} + \frac{A_2}{B_2}$.

Mais puisque $\deg F < 0$, sa partie entière est nulle. Or, cette partie entière est $E_1 + E_2$, donc

$E_1 + E_2 = 0$, et donc $F = \frac{A_1}{B_1} + \frac{A_2}{B_2}$.

Unicité : supposons que $\frac{A}{B} = \frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{C_1}{B_1} + \frac{C_2}{B_2}$.

Alors $\frac{A_1 - C_1}{B_1} = \frac{C_2 - A_2}{B_2} \Leftrightarrow B_2(A_1 - C_1) = B_1(C_2 - A_2)$.

Donc B_2 divise $B_1(C_2 - A_2)$, et, étant premier à B_1 , par Gauss, divise²⁵ $C_2 - A_2$.

²⁵ Dans $\mathbf{K}[X]$.

Mais $\deg C_2 < \deg B_2$ et $\deg A_2 < \deg B_2$, donc $\deg(C_2 - A_2) < \deg B_2$.

Si $B_2 \mid (C_2 - A_2)$, c'est donc que $C_2 - A_2 = 0 \Leftrightarrow C_2 = A_2$.

On en déduit alors aisément que $A_1 = C_1$.

Venons en enfin au cas où $\frac{A}{B}$ est irréductible. Alors, par Bézout, il existe U_1, V_1 tels que $AU_1 + BV_1 = 1 \Leftrightarrow AU_1 + B_1B_2V_1 = 1$.

Donc, toujours par Bézout, A est premier avec B_1 et avec B_2 .

Mais B_1 est aussi premier avec V , donc il est premier avec AV .

Donc $A_1 = AV - B_1E_1$ est aussi premier avec B_1 , et donc $\frac{A_1}{B_1}$ est irréductible. \square

Lemme 34.38. Soit $F = \frac{A}{B} \in \mathbf{K}(X)$ avec $\deg(F) < 0$, et supposons que $B = B_1B_2 \cdots B_n$, avec les B_i deux à deux premiers entre eux.

Alors, de manière unique,

$$F = \frac{A_1}{B_1} + \cdots + \frac{A_n}{B_n}, \text{ avec } \deg(A_i) < \deg(B_i).$$

De plus, si $\frac{A}{B}$ est irréductible, alors les $\frac{A_i}{B_i}$ le sont aussi.

Démonstration. Par récurrence sur n , la récurrence ayant été initialisée dans le lemme précédent²⁶.

La seule chose non totalement évidente est l'unicité.

Supposons donc acquise cette unicité lorsque B est un produit de n facteurs premiers deux à deux, et supposons que $B = B_1 \cdots B_{n+1}$, et que

$$F = \frac{A_1}{B_1} + \cdots + \frac{A_{n+1}}{B_{n+1}} = \frac{C_1}{B_1} + \cdots + \frac{C_{n+1}}{B_{n+1}}.$$

$$\text{Alors } F = \frac{A_1B_2 + A_2B_1}{B_1B_2} + \frac{A_3}{B_3} + \cdots + \frac{A_{n+1}}{B_{n+1}} = \frac{C_1B_2 + C_2B_1}{B_1B_2} + \frac{C_3}{B_3} + \cdots + \frac{C_{n+1}}{B_{n+1}}.$$

Par hypothèse de récurrence, qui s'applique car $\frac{A_1B_2 + A_2B_1}{B_1B_2}$ est de degré négatif, on a

$$\frac{A_1B_2 + A_2B_1}{B_1B_2} = \frac{C_1B_2 + C_2B_1}{B_1B_2} \text{ et } A_3 = C_3, \dots, A_{n+1} = C_{n+1}.$$

Soit encore $\frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{C_1}{B_1} + \frac{C_2}{B_2}$, et alors le lemme permet de conclure. \square

Lemme 34.39. Si $F = \frac{A}{B^n}$ ($n \geq 1$) est de partie entière nulle, alors de manière unique

$$F = \frac{A_1}{B} + \frac{A_2}{B^2} + \cdots + \frac{A_n}{B^n} \text{ où } A_i \text{ est un polynôme de degré inférieur strictement à } \deg B.$$

Et si de plus $\frac{A}{B^n}$ est irréductible alors $A_n \neq 0$.

Démonstration. L'existence se prouve par récurrence. Pour $n = 1$, c'est trivial.

Supposons le résultat vrai pour n , et soit $F = \frac{A}{B^{n+1}}$ de la forme annoncée.

Soit $A = BQ + R$ la division de A par B . Alors $\frac{A}{B^{n+1}} = \frac{Q}{B^n} + \frac{R}{B^{n+1}}$, avec $\deg R < \deg B$.

Puisque F et $\frac{R}{B^{n+1}}$ sont de parties entières nulles²⁷, il en est de même de $\frac{Q}{B^n}$. Et donc par hy-

pothèse de récurrence, il existe A_1, \dots, A_n , avec $\deg(A_i) < \deg(B)$ tels que $\frac{Q}{B^n} = \frac{A_1}{B} + \cdots + \frac{A_n}{B^n}$.

$$\text{Et donc } \frac{A}{B^{n+1}} = \frac{A_1}{B} + \cdots + \frac{A_n}{B^n} + \frac{R}{B^{n+1}}.$$

Unicité : encore par récurrence, en notant, comme dans la preuve de l'existence, que A_n est le reste de la division euclidienne de A par B^n , et donc est unique.

Enfin, pour le dernier point, si on avait $A_n = 0$, on écrirait alors $\frac{A}{B^n} = \frac{Q}{B^{n-1}}$, et $AB^{n-1} = B^nQ$,

donc $A = BQ$, de sorte que $B \mid A$, et donc $\frac{A}{B^n}$ ne serait pas irréductible. \square

²⁶ Lemme qui sert aussi pour l'hérédité.

²⁷ C'est-à-dire de degré strictement négatif.

Théorème 34.40 (Décomposition en éléments simples) : Soit $F = \frac{A}{B}$ une fraction rationnelle. Alors F s'écrit de manière unique comme somme d'un polynôme et d'un nombre fini d'éléments simples. Plus précisément si $B = B_1^{\alpha_1} \cdots B_n^{\alpha_n}$ est la décomposition de B en produit de facteurs irréductibles de $\mathbf{K}[X]$. Alors il existe une unique famille de polynômes $E, A_{1,1}, \dots, A_{1,\alpha_1}, \dots, A_{n,1}, \dots, A_{n,\alpha_n}$ tels que :

$$\begin{aligned} F &= E + \frac{A_{1,1}}{B_1} + \frac{A_{1,2}}{B_1^2} + \cdots + \frac{A_{1,\alpha_1}}{B_1^{\alpha_1}} + \frac{A_{2,1}}{B_2} + \cdots + \frac{A_{n,\alpha_n}}{B_n^{\alpha_n}} \\ &= E + \sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{B_i^k}. \end{aligned}$$

avec $\forall i \in \llbracket 1, n \rrbracket, \forall k \in \llbracket 1, \alpha_i \rrbracket, \deg A_{i,k} < \deg B_i$.

Démonstration. Il est évident que E doit être la partie entière²⁸ de F et donc il suffit de prouver le résultat lorsque $\deg F < 0$.

L'existence est alors assez facile, puisque les $B_i^{\alpha_i}$ sont deux à deux premiers entre eux, le lemme 34.38 prouve que F s'écrit sous la forme $\frac{A_1}{B_1^{\alpha_1}} + \cdots + \frac{A_n}{B_n^{\alpha_n}}$, avec $\deg A_i < \deg B_i^{\alpha_i}$.

Et alors le lemme 34.39 termine le boulot.

Pour l'unicité, il s'agit de remarquer qu'on a unicité dans les deux lemmes en question. Et donc si F , une fraction de degré négatif possède deux décompositions en éléments simples, quitte à ajouter des termes nuls, on peut supposer que les dénominateurs qui apparaissent dans ces deux décompositions²⁹ sont les mêmes, notons-les B_1, \dots, B_n avec les mêmes puissances $\alpha_1, \dots, \alpha_n$:

$$F = \sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{B_i^k} = \sum_{i=1}^n \sum_{k=1}^{\alpha_i} \frac{C_{i,k}}{B_i^k}$$

où les B_i sont irréductibles.

En «mettant au même dénominateur», on peut alors écrire, pour $i \in \llbracket 1, n \rrbracket$,

$$\sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{B_i^k} = \frac{A_i}{B_i^{\alpha_i}}$$

où A_i est un polynôme de degré strictement inférieur à $\deg B_i^{\alpha_i}$.

De même $\sum_{k=1}^{\alpha_i} \frac{C_{i,k}}{B_i^k} = \frac{C_i}{B_i^{\alpha_i}}$.

Donc $F = \sum_{i=1}^n \frac{A_i}{B_i^{\alpha_i}} = \sum_{i=1}^n \frac{C_i}{B_i^{\alpha_i}}$, et alors l'unicité du lemme 34.38 nous donne $A_i = C_i$.

Reste alors à utiliser l'unicité du lemme 34.39 pour montrer que pour tout i et tout k , $A_{i,k} = C_{i,k}$. \square

34.2.5 Pratique de la décomposition en éléments simples

Les méthodes rencontrées en début d'année pour le calcul de la décomposition en éléments simples restent valables.

Ajoutons deux choses :

► Si α est un pôle simple de F , c'est-à-dire si $F = \frac{P}{Q} = \frac{P}{(X - \alpha)Q_1}$, avec $Q_1(\alpha) \neq 0$.

Alors la partie polaire de F associée à α est de la forme $\frac{\lambda}{X - \alpha}$ et donc $F = \frac{\lambda}{X - \alpha} + G$, où $G \in \mathbf{K}(X)$ n'a pas α pour pôle.

En multipliant par $X - \alpha$, il vient $\frac{P}{Q_1} = \lambda + (X - \alpha)G$ et donc $\frac{P(\alpha)}{Q_1(\alpha)} = \lambda$.

²⁸ Qu'on sait être unique.

²⁹ Les B_i^k ci-dessus.

Remarque
Multiplier par $X - \alpha$ est bien la méthode que nous employons en début d'année.

Par ailleurs, on a $Q' = [(X - \alpha)Q_1]' = (X - \alpha)Q_1' + Q_1$ et donc $Q'(\alpha) = Q_1(\alpha)$.

Donc la partie polaire associée à α est $\frac{P(\alpha)}{Q'(\alpha)} \frac{1}{X - \alpha}$.

► Dans le cas où la fraction rationnelle est paire/impair, et si a est un pôle de F d'ordre n , alors $-a$ est aussi un pôle de F d'ordre n .

Et alors la comparaison des décompositions en éléments simples de $F(X)$ et $F(-X) = \pm F(X)$ fournit des relations entre les coefficients.

Exemple 34.41

Soit $F = \frac{4}{(X^2 - 1)^2} \in \mathbf{R}(X)$. Alors la décomposition en éléments simples de F est de la forme

$$F(X) = \frac{a}{X - 1} + \frac{b}{X + 1} + \frac{c}{(X - 1)^2} + \frac{d}{(X + 1)^2}.$$

Mais alors F est paire donc

$$F(X) = F(-X) = \frac{a}{-X - 1} + \frac{b}{-X + 1} + \frac{c}{(-X - 1)^2} + \frac{d}{(-X + 1)^2} = \frac{-a}{X + 1} + \frac{-b}{X - 1} + \frac{c}{(X + 1)^2} + \frac{d}{(X - 1)^2}.$$

L'unicité de la décomposition en éléments simples nous donne alors immédiatement $-a = b$ et $c = d$.

En multipliant par $(X - 1)^2$, et en évaluant en $X = 1$, on a immédiatement $c = \frac{4}{(1+1)^2} = 1$, et donc $d = 1$.

Puis en évaluant en $X = 0$, il reste $4 = -a - a + 1 + 1 \Leftrightarrow a = -1$.

$$\text{Et donc } F(X) = \frac{-1}{X - 1} + \frac{1}{X + 1} + \frac{1}{(X - 1)^2} + \frac{1}{(X + 1)^2}.$$

Enfin, terminons par un cas particulier, qui est à connaître : si $P = \alpha \prod_{i=1}^n (X - \lambda_i)$ est scindé³⁰, où les λ_i ne sont pas nécessairement distincts. Alors

³⁰ Ce qui est automatique sur \mathbf{C} .

$$P' = \alpha \sum_{i=1}^n (X - \lambda_i) \cdots \underbrace{(X - \lambda_i)'}_{=1} \cdots (X - \lambda_n) = \alpha \sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (X - \lambda_j).$$

$$\text{Et donc } \frac{P'}{P} = \frac{\alpha \sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (X - \lambda_j)}{\alpha \prod_{j=1}^n (X - \lambda_j)} = \sum_{i=1}^n \frac{1}{X - \lambda_i}.$$

En particulier, si P possède des racines multiples, alors certains termes de la somme ci-dessus sont identiques. Si on note $P = \alpha \prod_{i=1}^n (X - \lambda_i)^{m_i}$, où cette fois les λ_i sont distincts, et m_i la multiplicité de λ_i , alors

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

Cette formule n'est pas tellement surprenante dans le cas où P est un polynôme de $\mathbf{R}[X]$, scindé sur \mathbf{R} . En effet, si $P = \alpha \prod_{i=1}^n (X - \lambda_i)^{m_i}$, on reconnaît que $\frac{P'}{P}$ est la dérivée (sur $\mathbf{R} \setminus \{\lambda_1, \dots, \lambda_n\}$) de $\ln |P|$.

Mais pour $x \notin \{\lambda_1, \dots, \lambda_n\}$, $\ln |P(x)| = \ln(|\alpha|) + \sum_{i=1}^n m_i \ln(|x - \lambda_i|)$.

$$\text{Et donc } (\ln |P|)'(x) = \sum_{i=1}^n \frac{m_i}{x - \lambda_i}.$$