Algèbre

Série pour L1 / bac + 1

Notes rédigées par Alexey Muranov

23 janvier 2025

Table des matières

I. Polynômes

CHAPITRE-BROUILLON

I.1. Définitions, opérations, propriétés de base

I.1.1. Définitions et exemples

Tout *polynôme* en une *indéterminée* X à *coefficients* dans un corps $\mathbf{K}$ (on dit aussi : un polynôme *sur* $\mathbf{K}$) s'écrit comme une « expression formelle » de la forme :

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \qquad \text{avec} \quad n \in \mathbf{N},\ a_0, \dots, a_n \in \mathbf{K}.$$

Le symbole X s'appelle une *indéterminée*. Les *polynômes constants* de la forme a_0, avec $a_0 \in \mathbf{K}$, sont autorisés, et on les identifie d'habitude avec les éléments de $\mathbf{K}$. Parmi eux, il y a un polynôme special : *le polynôme nul* 0.

On admet que $X^0 = 1$ et que $0X^n = 0$ pour tout $n \in \mathbf{N}$. Ainsi deux autres façons d'écrire un polynôme à coefficients $a_0, \dots, a_n$ sont les suivantes :

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k = \sum_{k=0}^{\infty} a_kX^k.$$

Dans la dernière écriture, on a posé $a_{n+1} = a_{n+2} = \cdots = 0$.

La representation d'un polynôme par une « expression formelle » n'est pas tout-à-fait unique. Par exemple : $1 + 1X = 1 + 1X + 0X^2 + 0X^3$. On se permet aussi d'écrire X^n au lieu de $1X^n$, d'écrire les *termes* d'un polynôme dans un ordre quelconque, et de ne pas écrire les termes nuls : $1 + 0X + 1X^2 + 0X^3 = 1 + X^2 = X^2 + 1$.

Plus précisément, deux polynômes en l'indéterminée X, chacun écrit sous une forme standard, sont égaux si et seulement si leurs coefficients auprès des mêmes puissances de l'indéterminée sont égaux. (Si X^k n'intervient pas dans une écriture, cela veut dire que le coefficient auprès de X^k est 0.)

L'ensemble de tous les polynômes en X sur $\mathbf{K}$ est noté $\mathbf{K}[X]$.

Le polynôme X^n (avec $n \in \mathbf{N}$) s'appelle le *monôme de degré n*. Ainsi, le monôme de degré 0 est 1.

Les trois opérations algébriques principales définies dans $\mathbf{K}[X]$ sont les suivantes :

(1) addition,

(2) multiplication par un élément de $\mathbf{K}$ (cette opération peut être vue aussi comme un cas particulier de multiplication de deux polynômes),

(3) multiplication.

Ces opérations sont définies des façons naturelles. Pour la multiplication, on utilise la règle :

$$X^m \cdot X^n = X^{m+n} \quad \text{pour tous} \quad m, n \in \mathbf{N}.$$

Nous admettons ici sans démonstration que ces opérations sont bien définies, c'est-à-dire que le résultat ne dépends pas du choix d'écriture de chaque argument, ni de l'ordre dans lequel on applique des règles différents pour développer et après simplifier le résultat. (Une démonstration de ce fait nécessiterait de donner d'abord des définitions précises.)

Définitions précises

Une façon de construire un modèle de $\mathbf{K}[X]$ et ainsi de le définir précisément est la suivante.

On dit que $\mathbf{K}[X]$ est l'ensemble de toutes les suites infinies $(a_n)_{n\in\mathbf{N}}$ des éléments de $\mathbf{K}$ avec la propriété qu'il existe $N \in \mathbf{N}$ tel que pour tout $n > N$, $a_n = 0$.

Après on définit les opérations d'addition de deux éléments de $\mathbf{K}[X]$ et de multiplication d'un élément de $\mathbf{K}[x]$ par un élément de $\mathbf{K}$ naturellement : pour $(a_n)_{n\in\mathbf{N}}, (b_n)_{n\in\mathbf{N}} \in \mathbf{K}[X]$ et $c \in \mathbf{K}$, on pose

$$(a_n)_{n\in\mathbf{N}} + (b_n)_{n\in\mathbf{N}} \overset{\text{déf}}{=} (a_n + b_n)_{n\in\mathbf{N}}, \qquad c(a_n)_{n\in\mathbf{N}} \overset{\text{déf}}{=} (ca_n)_{n\in\mathbf{N}}.$$

Pour définir la multiplication, on utilise une opération sur les suites qui s'appelle « produit de convolution » : pour $(a_n)_{n\in\mathbf{N}}, (b_n)_{n\in\mathbf{N}} \in \mathbf{K}[X]$, on pose

$$(a_n)_{n\in\mathbf{N}} \cdot (b_n)_{n\in\mathbf{N}} \overset{\text{déf}}{=} (a_0b_n + a_1b_{n-1} + \cdots + a_nb_0)_{n\in\mathbf{N}}.$$

Pour justifier le choix de « X » dans « $\mathbf{K}[X]$ », on pose

$$X \overset{\text{déf}}{=} (0, 1, 0, 0, 0, 0, \dots),$$

c'est-à-dire X est la suite $(a_n)_{n\in\mathbf{N}}$ avec $a_0 = 0$, $a_1 = 1$, et $a_2 = a_3 = \cdots = 0$.

Les *monômes* sont les suites avec exactement un terme non nul qui vaut 1. Les *polynômes constants* sont les suite de la forme

$$(a_0, 0, 0, 0, \dots),$$

et on identifie $(a_0, 0, 0, 0, \dots) \in \mathbf{K}[X]$ avec $a_0 \in \mathbf{K}$. Le *polynôme* nul est $(0, 0, 0, \dots)$.

Ce que on a fait ici pour définir $\mathbf{K}[X]$ formellement, c'est de representer tout polynôme par la suite de ses coefficients, et de définir les opérations algébriques directement sur ces suites.

On peut vérifier maintenant que tout $P \in \mathbf{K}[X]$ s'écrit comme

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \quad \text{où} \quad n \in \mathbf{N},\ a_0, \dots, a_n \in \mathbf{K}.$$

En effet, il suffit d'écrire d'abord $P = (a_0, \dots, a_n, 0, 0, 0, \dots)$.

On vérifie également que les opérations d'addition et de multiplication qu'on a définies dans $\mathbf{K}[X]$ satisfont des propriétés usuelles : associativité, commutativité, distributivité, etc.

Le *terme de degré n* et le *coefficient de degré n* du polynôme $P = \sum_{k\in\mathbf{N}} a_kX^k$ sont respectivement le terme a_nX^n et son coefficient a_n. Le terme de degré 0 est donc a_0X^0, que l'on identifie au coefficient de degré 0, i.e. à $a_0 \in \mathbf{K}$, et que l'on nomme au choix *terme constant* ou *coefficient constant* de P. Nous le noterons $\mathrm{tc}(P)$.

Si tous ses coefficients sont nuls, le polynôme est le polynôme nul. Dans le cas contraire, soit $n \in \mathbf{N}$ le plus grand indice d'un coefficient non nul (il y a bien un tel plus grand indice). On a donc :

$$P = \sum_{i=0}^{n} a_i X^i = a_0 + \cdots + a_n X^n \quad \text{avec} \quad a_n \neq 0.$$

L'entier n est alors appelé le *degré* de P et noté $\deg P$. Par convention, $\deg 0 = -\infty$ (l'avantage est que cela donne des règles de calcul simples et valables dans tous les cas sans exception).

Le terme de degré $\deg P$, c'est-à-dire ici $a_n X^n$, est appelé le *terme dominant* de P et noté $\mathrm{td}(P)$. Son coefficient a_n est appelé le *coefficient dominant* et noté $\mathrm{cd}(P)$.

Un polynôme de degré 0 a la forme suivante : son coefficient constant a_0 est non nul, et tous ses autres coefficients sont nuls. C'est donc un polynôme constant non nul. Le polynôme nul est aussi constant, mais son degré par définition est $-\infty$.

I.1.2. 8 axiomes d'un « anneau commutatif »

Les opérations d'addition et de multiplication dans $\mathbf{K}[X]$ satisfont les propriétés suivantes :

(1) pour tous $P, Q, R \in \mathbf{K}[X]$,

$$P + (Q + R) = (P + Q) + R,$$

(2) pour tous $P, Q \in \mathbf{K}[X]$,

$$P + Q = Q + P,$$

(3) pour tout $P \in \mathbf{K}[X]$,

$$P + 0 = 0 + P = P,$$

(4) pour tout $P \in \mathbf{K}[X]$,

$$P + (-P) = (-P) + P = 0,$$

(5) pour tous $P, Q, R \in \mathbf{K}[X]$,

$$P(QR) = (PQ)R,$$

(6) pour tous $P, Q \in \mathbf{K}[X]$,

$$PQ = QP,$$

(7) pour tout $P \in \mathbf{K}[X]$,

$$P \cdot 1 = 1 \cdot P = P,$$

(8) pour tous $P, Q, R \in \mathbf{K}[X]$,

$$(P + Q)R = PR + QR, \qquad P(Q + R) = PQ + PR.$$

L'ensemble des propriétés se résume en disant que $\mathbf{K}[X]$ muni de l'addition et de la multiplication est un « anneau commutatif ». En revanche, $\mathbf{K}[X]$ n'est pas un « corps », car les seuls polynômes inversibles sont les polynômes de degré 0 — les polynômes constants non nuls. (Or, tout élément non nul d'un corps admet un inverse multiplicatif.)

I.1.3. Propriétés du degré par rapport aux opérations

Soit P un polynôme non nul :

$$P = a_0 + a_1 X + \cdots + a_p X^p \quad \text{avec } a_p \neq 0.$$

Rappelons nous que le terme dominant de P, noté $\mathrm{td}(P)$, est alors $a_p X^p$, que son coefficient dominant, noté $\mathrm{cd}(P)$, est a_p, et que son degré, noté $\deg P$, est l'entier p. Par convention, le polynôme nul 0 est de degré $-\infty$ et n'a pas de terme dominant ni de coefficient dominant.

Voici quelque propriétés du degré par rapport aux opérations.

(1) Si $P, Q \in \mathbf{K}[X]$, alors

$$\deg(P + Q) \leqslant \max(\deg P, \deg Q).$$

Si en plus $\mathrm{td}(P) + \mathrm{td}(Q) \neq 0$, alors

$$\deg(P + Q) = \max(\deg P, \deg Q).$$

(2) Si $P, Q \in \mathbf{K}[X]$, alors

$$\deg(PQ) = \deg P + \deg Q.$$

(On suppose ici que $-\infty + n = -\infty$ pour tout $n \in \mathbf{N}$.)

Pour vérifier ces propriétés, considérons d'abord deux polynômes non nuls

$$P = a_0 + a_1 X + \cdots + a_p X^p \quad \text{avec } a_p \neq 0$$

et

$$Q = b_0 + b_1 X + \cdots + b_q X^q \quad \text{avec } b_q \neq 0.$$

L'addition des polynômes P et Q donne :

$$P+Q=\begin{cases}(a_0+b_0)+\cdots+(a_p+b_p)X^p+b_{p+1}X^{p+1}+\cdots+b_qX^q & \text{si } p<q,\\ (a_0+b_0)+\cdots+(a_q+b_q)X^q+a_{q+1}X^{q+1}+\cdots+a_pX^p & \text{si } q<p,\\ (a_0+b_0)+\cdots+(a_p+b_p)X^p & \text{si } p=q.\end{cases}$$

On en déduit que, si $p\neq q$, le degré de $P+Q$ est le maximum des degrés de P et Q, et que son terme et son coefficient dominants sont ceux de P ou de Q (celui qui a le plus grand degré). Si $p=q$, le degré de $P+Q$ est en général p, sauf dans le cas exceptionnel où $a_p+b_p=0$: dans ce cas, les termes dominants se simplifient et le degré de $P+Q$ diminue strictement. Dans tous les cas, on retiendra la règle suivante :

$$\deg(P+Q)\leqslant\max(\deg P,\deg Q),$$

avec égalité en général, la seule exception étant celle où $\mathrm{td}(P)+\mathrm{td}(Q)=0$. À noter que l'inégalité reste valable si P ou Q est nul.

La multiplication des polynômes P et Q donne :

$$PQ=a_0b_0+(a_1b_0+a_0b_1)X+\cdots+(a_pb_{q-1}+a_{p-1}b_q)X^{p+q-1}+a_pb_qX^{p+q}.$$

Le terme dominant de PQ est donc $a_pb_qX^{p+q}$, et l'on a dans tous les cas les formules :

$$\mathrm{td}(PQ)=\mathrm{td}(P)\,\mathrm{td}(Q)\quad\text{et}\quad\mathrm{cd}(PQ)=\mathrm{cd}(P)\,\mathrm{cd}(Q),$$

d'où l'on déduit la règle :

$$\deg(PQ)=\deg P+\deg Q.$$

À noter que la règle reste valable si P ou Q est nul.

Conséquence : « intégrité » de $\mathbf{K}[X]$

Proposition. *Si $P,Q\in\mathbf{K}[X]$, $P\neq0$, et $Q\neq0$, alors $PQ\neq0$.*

Dit dans l'autre sens : si $PQ=0$, alors $P=0$ ou $Q=0$. On exprime cette règle en disant que « l'anneau $\mathbf{K}[X]$ est intègre ».

Corollaire. *Si $A,B,C\in\mathbf{K}[X]$, $A\neq0$, et $AB=AC$, alors $B=C$.*

Démonstration. Si $AB=AC$, alors $A(B-C)=AB-AC=0$. Comme $A\neq0$, alors, par l'« intégrité » de $\mathbf{K}[X]$, $B-C=0$. Ainsi $B=C$. □

Remarque. Cette règle ne va pas de soi ; ainsi, le produit de deux fonctions quelconques peut être nul sans qu'aucune des deux le soit. Prenons les fonctions $f,g\colon\mathbf{R}\to\mathbf{R}$ définies par les formules :

$$f(x)=x-|x|\quad\text{et}\quad g(x)=x+|x|\,.$$

(Ces fonctions sont d'ailleurs continues.) Alors $fg=0$, mais aucune des deux fonctions f,g n'est nulle. Ce phénomène est impossible avec des polynômes, ni avec des fonctions polynomiales sur un corps infini.

I.1.4. Substitution pour l'indéterminée

Si P et Q sont deux polynômes dans $\mathbf{K}[X]$, on peut *substituer* Q dans P pour X. Le résultat est noté $P(Q)$. Si

$$P=a_0+a_1X+a_2X^2+\cdots+a_nX^n,$$

alors

$$P(Q)=a_0+a_1Q+a_2Q^2+\cdots+a_nQ^n.$$

Définition. La substitution d'un élément $a\in\mathbf{K}$ dans un polynôme $P\in\mathbf{K}[X]$ pour obtenir la valeur $P(a)\in\mathbf{K}$ s'appelle l'*évaluation* de P en a.

Définition. Une *racine* de $P\in\mathbf{K}[X]$ est un $r\in\mathbf{K}$ tel que $P(r)=0$.

L'évaluation d'un polynôme $P\in\mathbf{K}[X]$ en éléments de $\mathbf{K}$ donne lieu à une *fonction polynomiale* $f\colon\mathbf{K}\to\mathbf{K},a\mapsto P(a)$.

Définition. Une *fonction polynomiale* dans $\mathbf{K}$ est toute fonction de la forme $f\colon\mathbf{K}\to\mathbf{K},x\mapsto P(x)$, où $P\in\mathbf{K}[X]$.

Tout polynôme $P\in\mathbf{K}[X]$ définit ainsi une fonction polynomiale $\mathbf{K}\to\mathbf{K}$. On verra aussi que dans des corps commutatifs infinis, comme $\mathbf{Q}$, $\mathbf{R}$, ou $\mathbf{C}$, toute fonction polynomiale est définie par un unique polynôme. Cela n'est plus le cas si le corps $\mathbf{K}$ est fini ; en effet, dans tout corps commutatif fini, toute fonction polynomiale est définie par une infinité de polynômes distincts.[1]

Il y a d'autres objets mathématiques qu'on peut substituer pour une indéterminée dans un polynôme, comme, par exemple, des *matrices carrées*, des *opérateurs différentiels*, ou d'autres polynômes.

Si $P,Q\in\mathbf{K}[X]$, alors la substitution de Q dans P pour X donne :

$$P(Q)=a_0+a_1(b_0+\cdots+b_qX^q)+\cdots a_p(b_0+\cdots+b_qX^q)^p.$$

Si Q n'est pas constant, alors le terme dominant de $P(Q)$ est $a_pb_q^pX^{qp}$ et le degré est pq. (On suppose ici que $(-\infty)n=-\infty$ pour tout $n>0$.)

I.2. Divisibilité

Définition. On dit qu'un polynôme B *divise* un polynôme A si et seulement si il existe un polynôme C tel que $A=BC$.

On écrit $B\mid A$ pour noter que B divise A.

Proposition. *La relation de divisibilité dans $\mathbf{K}[X]$ est « transitive » et « réflexive », c'est-à-dire :*

[1] Par exemple, le polynôme $X+X^2\in(\mathbf{Z}/2\mathbf{Z})[X]$ définit la fonction nulle $\mathbf{Z}/2\mathbf{Z}\to\mathbf{Z}/2\mathbf{Z}$, $x\mapsto\bar0$.

(1) *pour tous* $A, B, C \in \mathbf{K}[X]$, *si* $A \mid B$ *et* $B \mid C$, *alors* $A \mid C$,

(2) *pour tout* $A \in \mathbf{K}[X]$, $A \mid A$.

Définition. Un polynôme non constant $P \in \mathbf{K}[X]$ est dite *irréductible* sur $\mathbf{K}$ si et seulement si tout diviseur de P dans $\mathbf{K}[X]$ est soit constant, soit un multiple de P de la forme aP avec $a \in \mathbf{K}$.

I.3. Division euclidienne

Rappelons nous le théorème suivant sur les nombre entiers.

Théorème. *Si* $a, b \in \mathbf{Z}$ *et* $b \neq 0$, *alors il existe un unique couple* $q, r \in \mathbf{Z}$ *tel que* :

(1) $a = bq + r$, *et*

(2) $0 \leqslant r < b$.

Il y a un théorème analogique pour les polynômes.

Théorème. *Si* $A, B \in \mathbf{K}[X]$ *et* $B \neq 0$, *alors il existe un unique couple* $Q, R \in \mathbf{K}[X]$ *tel que* :

(1) $A = BQ + R$, *et*

(2) $\deg R < \deg B$.

Définition. Dans ce théorème, les polynômes Q et R s'appellent respectivement le *quotient* et le *reste* de la *division euclidienne* de A par B.

Montrons l'unicité. Pour cela, supposons que

$$A = BQ_1 + R_1 = BQ_2 + R_2, \qquad \deg R_1 < \deg B, \qquad \deg R_2 < \deg B.$$

Alors

$$R_2 - R_1 = B \cdot (Q_1 - Q_2).$$

D'un coté,

$$\deg(R_2 - R_1) \leqslant \max(\deg R_1, \deg R_2) < \deg B,$$

et de l'autre coté,

$$\deg(R_2 - R_1) = \deg(Q_1 - Q_2) + \deg B.$$

Comme $B \neq 0$, cela n'est possible que si $Q_1 - Q_2 = 0$. Ainsi $Q_1 = Q_2$ et $R_1 = R_2$, d'où l'unicité.

Pour montrer l'existence, on peut faire quelques exemples et trouver un algorithme général qui calcule le quotient et le reste.

Théorème. *Si* $P \in \mathbf{K}[X]$ *et* $a \in \mathbf{K}$, *alors le reste de la division euclidienne de* P *par* $X - a$ *est la constante* $P(a)$.

Démonstration. Soient Q et R le quotient et le reste de la division euclidienne de P par $X - a$. Alors

$$P = (X - a)Q + R \qquad (*)$$

et $\deg R < \deg(X - a) = 1$. Comme $\deg R \leqslant 0$, R est constant. Par substitution de a pour X dans l'équation $(*)$, on a :

$$P(a) = (a - a)Q(a) + R(a) = R$$

(vu que $R(a) = R$). □

Corollaire. *Un nombre* $r \in \mathbf{K}$ *est une racine de* $P \in \mathbf{K}[X]$ *si et seulement si* $X - r$ *divise* P.

Racines multiples

Définition. Un nombre $r \in \mathbf{K}$ est une *racine multiple* de $P \in \mathbf{K}[X]$ de *multiplicité* $m \in \mathbf{N}$ si et seulement si $(X - r)^m$ divise P mais $(X - r)^{m+1}$ ne divise pas P.

I.4. Division selon les puissances croissantes

Théorème. *Si* $A, B \in \mathbf{K}[X]$, *le terme constant de* B *n'est pas nul, et* $n \in \mathbf{N}$, *alors il existe un unique couple* $Q, R_0 \in \mathbf{K}[X]$ *tel que* :

(1) $A = BQ + X^{n+1}R_0$, *et*

(2) $\deg Q \leqslant n$.

Définition. Dans ce théorème, les polynômes Q et $X^{n+1}R_0$ s'appellent respectivement le *quotient* et le *reste* de la *division selon les puissances croissantes* de A par B à l'ordre n.

I.5. PGCD

Définition. Un *plus grand commun diviseur* (PGCD) de polynômes P et Q est un polynôme D tel que :

(1) D est un commun diviseur de P et Q (c'est-à-dire, $D \mid P$ et $D \mid Q$),

(2) si C est un commun diviseur de P et Q, alors C est un diviseur de D.

L'unique PGCD de P et Q avec le coefficient dominant 1 est noté $\operatorname{pgcd}(P, Q)$.

Identité de Bézout

Avant d'énoncer un théorème sur l'*identité de Bézout* pour les polynômes, rappelons nous l'identité de Bézout pour les entiers.

Théorème (Identité de Bézout)**.** *Si a et b sont deux entiers, pas tous les deux nuls, alors* $\operatorname{pgcd}(a,b)$ *existe et est unique, et en plus il existe deux entiers m et n tels que*

$$\operatorname{pgcd}(a,b) = am + bn.$$

Théorème (Identité de Bézout)**.** *Si A et B sont deux polynômes sur $\mathbf{K}$, pas tous les deux nuls, alors* $\operatorname{pgcd}(A,B)$ *existe et est unique, et en plus il existe deux polynômes P et Q sur $\mathbf{K}$ tels que*

$$\operatorname{pgcd}(A,B) = AP + BQ.$$

L'idée d'une démonstration : l'*algorithme d'Euclide* (par la division euclidienne) pour trouver le $\operatorname{pgcd}(P,Q)$.

Corollaire (Lemme d'Euclide)**.** *Si A, B, D sont trois polynômes, D divise AB, et que* $\operatorname{pgcd}(B,D) = 1$*, alors D divise A.*

Démonstration. Soient P et Q deux polynômes tels qu'on a l'identité de Bézout :

$$1 = BP + DQ.$$

Par multiplication par A, on trouve :

$$A = (AB)P + D(AQ).$$

Comme $D \mid AB \mid ABP$ et $D \mid DAQ$, on en déduit que $D \mid A$. □

Corollaire. *Si A, B, M sont trois polynômes, A et B divisent M, et que* $\operatorname{pgcd}(A,B) = 1$*, alors AB divise M.*

Démonstration. Posons

$$M = AQ_1.$$

Comme $B \mid M = AQ_1$ et $\operatorname{pgcd}(A,B) = 1$, par le lemme d'Euclide, $B \mid Q_1$. Posons

$$Q_1 = BQ_2.$$

Alors $M = ABQ_2$, et donc $AB \mid M$. □

PPCM

Définition. Un *plus petit commun multiple* (PPCM) de polynômes P et Q est un polynôme M tel que :

(1) M est un commun multiple de P et Q (c'est-à-dire, P et Q sont diviseurs de M),

(2) si N est un commun multiple de P et Q, alors N est un multiple de M.

Proposition. *Soient A et B deux polynômes et D un PGCD de A et B. Posons $A = A_1D$ et $B = B_1D$. Alors A_1B_1D est un PPCM de A et B.*

I.6. Interpolation de Lagrange

Théorème (Interpolation de Lagrange)**.** *Soient $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbf{K}$, où les valeurs a_i sont deux à deux distinctes. Il existe alors un unique polynôme $P \in \mathbf{K}[X]$ de degré $\deg P \leqslant n-1$ tel que $P(a_i) = b_i$ pour $i = 1, \dots, n$.*

Démonstration. L'unicité peut se voir comme suit. Si P et Q sont deux polynômes de degrés $\deg P, \deg Q \leqslant n-1$ et tels que $P(a_i) = Q(a_i) = b_i$ pour $i = 1, \dots, n$, alors le polynôme $P - Q$, dont le degré est $\leqslant n-1$, admet les n racines : $a_1, \dots, a_n$; il est donc nul et $P = Q$.

L'existence s'obtient par une construction explicite. On pose d'abord, pour $i = 1, \dots, n$:

$$K_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - a_j) \quad \text{et} \quad L_i = \frac{1}{K_i(a_i)} K_i.$$

(Il est évident que $K_i(a_i) \neq 0$, ce qui justifie cette dernière définition.) On voit que $\deg L_i = n-1$ et que

$$L_i(a_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

En posant

$$P = \sum_{i=1}^{n} b_i L_i,$$

on obtient donc un polynôme P de degré $\deg P \leqslant n-1$ et tel que :

$$P(a_i) = \sum_{j=1}^{n} b_j L_j(a_i) = b_i \quad \text{pour tout} \quad i = 1, \dots, n.$$

C'est bien ce que l'on voulait. □

I.7. Dérivation formelle

I.7.1. Polynôme dérivé

Définition. Si $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{K}[X]$, alors le *polynôme dérivé* de P est

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Propriétés :

(1) $(P+Q)' = P' + Q'$,

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

(3) $P' = 0$ si et seulement si P est constant,

(4) si $\deg P \geqslant 1$, alors $\deg P' = \deg P - 1$.

I.7.2. Dérivation d'ordre supérieur

Notons $P^{(k)}$ la *dérivée k-ième* du polynôme $P^{(k)} \in K[X]$. En particulier, pour $k = 0, 1, 2, 3$, on a :

$$P^{(0)} = P, \quad P^{(1)} = P', \quad P^{(2)} = P'', \quad P^{(3)} = P'''.$$

D'après la règle $\deg P' = \deg P - 1$ (valable pour un polynôme non constant P), on a plus généralement que pour tout $k \leqslant \deg P$,

$$\deg P^{(k)} = \deg P - k.$$

En particulier, si $n = \deg P$, alors $P^{(n)}$ est un polynôme constant non nul et $P^{(n+1)} = 0$.

Réciproquement, si P est un polynôme tel que $P^{(k)} = 0$, alors $\deg P < k$.

Exemple. Les dérivées successives du polynôme X^p sont :

$$(X^p)^{(0)} = X^p, \quad (X^p)^{(1)} = pX^{p-1}, \quad (X^p)^{(2)} = p(p-1)X^{p-2}, \ldots,$$
$$(X^p)^{(p-1)} = p!X, \quad (X^p)^{(p)} = p!, \quad (X^p)^{(p+1)} = 0.$$

Plus précisément : si $0 \leqslant k \leqslant p$, k entier, alors la dérivée k^{e} de X^p est

$$(X^p)^{(k)} = \frac{p!}{(p-k)!}X^{p-k}.$$

Cette dérivée est nulle si $k > p$.

I.7.3. La formule de Leibniz

Les règles concernant la k^{e} dérivée ressemblent un peu à celles concernant la dérivation. On a évidemment :

$$(P+Q)^{(k)} = P^{(k)} + Q^{(k)}.$$

Pour la dérivée k^{e} d'un produit, c'est plus compliqué. On trouve facilement pour les petites valeurs de k :

$$(PQ)'' = P''Q + 2P'Q' + PQ'', \quad (PQ)''' = P'''Q + 3P''Q' + 3P'Q'' + Q'''.$$

La ressemblance avec le carré et le cube de $(a+b)$ s'impose, et l'on peut conjecturer une formule générale utilisant les coefficients binomiaux. C'est la *formule de Leibniz*, qui est en effet vraie.

Théorème (Formule de Leibniz)**.** *Soient $P, Q \in \mathbf{K}[X]$. Pour tout entier naturel k :*

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

Démonstration. Elle se fait par récurrence sur n. Pour $n = 0$, on a l'égalité $PQ = PQ$. Pour $n = 1$, on retrouve la règle de Leibniz $(PQ)' = P'Q + PQ'$. Supposons la formule vérifiée au rang n. Alors :

$$\begin{aligned}
(PQ)^{(n+1)} &= \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)}Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k)}Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k+1)}Q^{(n-k)} + P^{(k)}Q^{(n-k+1)}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)}Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)}Q^{(n-k+1)} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)}Q^{(n-k+1)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)}Q^{(n-k+1)} \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) P^{(k)}Q^{(n-k+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)}Q^{(n-k+1)}.
\end{aligned}$$

C'est la formule voulue au rang $n+1$. □

I.7.4. Formules de Taylor

La formule de Taylor pour les polynômes admet de nombreuses formes. Dans tous les cas, elle permet de développer $P(A+B)$, où P est un polynôme et A, B sont deux expressions (polynômes ou autre chose) ou tout simplement deux nouveaux indéterminés différents de X. Commençons par un petit lemme.

Lemme. *Soit $Q = b_0 + \cdots + b_pX^p$. Alors, pour tout entier naturel k :*

$$Q^{(k)}(0) = \begin{cases} k!\, b_k & \text{si } k \leqslant p, \\ 0 & \text{si } k > p. \end{cases}$$

Démonstration. C'est immédiat à partir du calcul des dérivées successives de chaque X^i dans l'exemple vu plus haut. □

Théorème (Formule de Taylor)**.** *Soit $P \in \mathbf{K}[X]$ un polynôme de degré n et soit $a \in \mathbf{K}$.*

Alors :

$$\begin{aligned}
P(X) &= P(0) + P'(0)X + \frac{1}{2}P''(0)X^2 + \cdots + \frac{1}{n!}P^{(n)}(0)X^n \\
&= \sum_{k=0}^{n} \frac{1}{k!}P^{(k)}(0)X^k, \\
P(X+a) &= P(a) + P'(a)X + \frac{1}{2}P''(a)X^2 + \cdots + \frac{1}{n!}P^{(n)}(a)X^n \\
&= \sum_{k=0}^{n} \frac{1}{k!}P^{(k)}(a)X^k, \\
P(X) &= P(a) + P'(a)(X-a) + \frac{1}{2}P''(a)(X-a)^2 + \cdots \\
&\quad + \frac{1}{n!}P^{(n)}(a)(X-a)^n \\
&= \sum_{k=0}^{n} \frac{1}{k!}P^{(k)}(a)(X-a)^k, \\
P(A+B) &= P(A) + BP'(A) + \frac{1}{2}B^2P''(A) + \cdots + \frac{1}{n!}B^nP^{(n)}(A) \\
&= \sum_{k=0}^{n} \frac{1}{k!}B^kP^{(k)}(A) \quad \textit{pour tous} \quad A, B \in \mathbf{K}[X].
\end{aligned}$$

Démonstration. La première formule est immédiate en appliquant le lemme : si $P = a_0 + \cdots + a_nX^n$, alors $a_k = \frac{1}{k!}P^{(k)}(0)$.

La deuxième se prouve en appliquant la première au polynôme $Q(X) = P(X+a)$, dont les dérivées sont données par la relation $Q^{(k)}(X) = P^{(k)}(X+a)$.

La troisième s'obtient en remplaçant X par $X-a$ dans la seconde.

La dernière est la plus général et s'obtient par calcul direct en développant les parties gauche et droite. □

Exemple. En utilisant la troisième formule, on voit maintenant facilement que le reste de la division euclidienne de P par $(X-a)^2$ est $P(a) + P'(a)(X-a)$.

I.8. Polynômes sur C et sur R

Théorème (« Théorème fondamental de l'algèbre »)**.** *Tout polynôme non constant à coefficients complexes admet une racine complexe.*

Théorème. *Si $r \in \mathbf{C}$ est une racine de $P \in \mathbf{R}[X]$, alors $\bar{r}$ (le conjugué complexe de r) est aussi une racine de P, et de la même multiplicité que r.*

L'idée d'une démonstration : si

$$P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{R}[X]$$

et $P(r) = 0$, $r \in \mathbf{C}$, alors on a :

$$\begin{aligned}
\overline{P(r)} &= 0, \\
\overline{a_0 + a_1r + \cdots + a_nr^n} &= 0, \\
a_0 + a_1\bar{r} + \cdots + a_n\bar{r}^n &= 0, \\
P(\bar{r}) &= 0.
\end{aligned}$$

Corollaire. *Tout polynôme dans $\mathbf{R}[X]$ de degré supérieur à 2 est réductible.*

L'idée d'une démonstration : soient $P \in \mathbf{R}[X]$ avec $\deg P \geqslant 3$ et r une racine complexe de P. Si $r \in \mathbf{R}$, alors P est divisible par $X - r \in \mathbf{R}[X]$. Sinon, posons $r = a + \boldsymbol{i}b$, $a, b \in \mathbf{R}$. Alors P est divisible par $(X-r)(X-\bar{r}) = X^2 - 2aX + a^2 + b^2 \in \mathbf{R}[X]$.

Théorème. *Tout polynôme de degré impaire admet une racine réelle.*

L'idée d'une démonstration : appliquer le *Théorème des valeurs intermédiaires*.

I.9. Fractions rationnelles

I.9.1. Définitions

L'ensemble des *fractions rationnelles à coefficients dans* **K** sera noté $\mathbf{K}(X)$ (**K** peut être **Q**, **R** ou **C**, comme avant). Un élément de $\mathbf{K}(X)$ est une « fraction » $\frac{A}{B}$, où $A, B \in \mathbf{K}[X]$ et $B \neq 0$. Les fractions rationnelles $\frac{A}{B}$ et $\frac{C}{D}$ sont déclarées égales si et seulement si $AD = CB$. Ainsi chaque fraction rationnelle $R \in \mathbf{K}(X)$ possède une infinité d'écritures sous la forme $\frac{A}{B}$ avec $A, B \in \mathbf{K}[X]$.

Les opérations d'addition et de multiplication dans $\mathbf{K}(X)$ sont définies par les formules suivantes :

$$\frac{A}{B} + \frac{C}{D} \overset{\text{déf}}{=} \frac{AD + CB}{BD}, \qquad \frac{A}{B} \cdot \frac{C}{D} \overset{\text{déf}}{=} \frac{AC}{BD}.$$

On définit aussi les fractions 0 et 1 :

$$0 \overset{\text{déf}}{=} \frac{0}{1}, \qquad 1 \overset{\text{déf}}{=} \frac{1}{1},$$

et les opération de l'opposé et de l'inverse :

$$-\frac{A}{B} \overset{\text{déf}}{=} \frac{-A}{B}, \qquad \left(\frac{A}{B}\right)^{-1} \overset{\text{déf}}{=} \frac{B}{A} \quad \text{si} \quad A \neq 0.$$

On peut « identifier » tout polynôme $P \in \mathbf{K}[X]$ avec la fraction rationnelle $\frac{P}{1}$ car si l'on applique les règles ci-dessus à des fractions rationnelles de cette forme, on retrouve bien les opérations déjà définies pour les polynômes. Alors on peut considérer $\mathbf{K}[X]$ comme une partie de $\mathbf{K}(X)$ par cette identification : $\mathbf{K}[X] \subset \mathbf{K}(X)$. Après cette identification,

on peut observer que la fraction $\frac{A}{B}$, où $A, B \in \mathbf{K}[X]$, n'est rien d'autre que le résultat de la division de $A = \frac{A}{1}$ par $B = \frac{B}{1}$ dans $\mathbf{K}(X)$.

Pour toute fraction rationnelle $F = \frac{A}{B} \in \mathbf{K}(X)$, on définit le *degré* de F par la formule :

$$\deg F \stackrel{\text{déf}}{=} \deg A - \deg B.$$

Comme $B \neq 0$ (donc $\deg B \in \mathbf{N}$), cette soustraction a un sens même si $A = 0$, dans quel cas l'on trouve $\deg 0 = -\infty$. Cependant, pour être certain que la définition a bien un sens, il faut vérifier qu'elle ne dépend pas de l'écriture particulière choisie pour F. Supposons donc que $F = \frac{A}{B} = \frac{C}{D}$. On a :

$$\begin{aligned} AD = CB &\Rightarrow \deg A + \deg D = \deg C + \deg B \\ &\Rightarrow \deg A - \deg B = \deg C - \deg D, \end{aligned}$$

car on peut soustraire $\deg B + \deg D \neq -\infty$. Pour calculer $\deg F$, on peut donc indifféremment utiliser l'écriture $F = \frac{A}{B}$ ou l'écriture $F = \frac{C}{D}$.

I.9.2. Propriétés algébriques

$\mathbf{K}(X)$ est un « corps commutatif » (il satisfait les 10 axiomes d'un « corps commutatif »).

I.9.3. Propriétés du degré par rapport aux opérations

Le degré des fractions rationnelles satisfait les propriétés suivantes :

(1) si $F, G \in \mathbf{K}(X)$, alors

$$\deg(F+G) \leqslant \max(\deg F, \deg G),$$

(2) si $F, G \in \mathbf{K}(X)$, alors

$$\deg(FG) = \deg F + \deg G,$$

(3) si $F \in \mathbf{K}(X)$ et $F \neq 0$, alors

$$\deg(1/F) = -\deg F,$$

(4) si $F, G \in \mathbf{K}(X)$ et $G \neq 0$, alors

$$\deg(F/G) = \deg F - \deg G.$$

I.9.4. Évaluation, zéros, pôles

Soit $\frac{A_0}{B_0}$ une forme irréductible de $F \in \mathbf{K}(X)$. On dit que F est *définie* en $\alpha \in \mathbf{K}$ si $B_0(\alpha) \neq 0$. On pose alors :

$$F(\alpha) = \frac{A_0(\alpha)}{B_0(\alpha)} \in \mathbf{K},$$

que l'on appelle *valeur* de F en α. Ces définitions ne dépendent pas du choix d'une forme irréductible : si $\frac{A_1}{B_1}$ est une autre forme irréductible de F, les conditions $B_0(\alpha) \neq 0$ et $B_1(\alpha) \neq 0$ sont équivalentes et $\frac{A_0(\alpha)}{B_0(\alpha)} = \frac{A_1(\alpha)}{B_1(\alpha)}$. De plus, pour toute écriture $\frac{A}{B}$ de F telle que $B(\alpha) \neq 0$, on a encore $F(\alpha) = \frac{A(\alpha)}{B(\alpha)}$. Réciproquement, si F n'est pas définie en α, alors $\frac{A(\alpha)}{B(\alpha)}$ n'est définie pour *aucune* écriture $\frac{A}{B}$ de F.

Exemples.

(1) La fraction rationnelle $\frac{X}{X^2+X} \in \mathbf{K}(X)$ est définie en 0, mais cette écriture particulière ne convient pas pour en calculer la valeur, alors que l'écriture $\frac{X-1}{X^2-1}$ de la même fraction rationnelle convient.

(2) La fraction rationnelle $\frac{1}{X^2-2} \in \mathbf{Q}[X]$ est définie en tout point de $\mathbf{Q}$ mais pas en tout point de $\mathbf{R}$. La fraction rationnelle $\frac{1}{X^2+1} \in \mathbf{R}[X]$ est définie en tout point de $\mathbf{R}$ mais pas en tout point de $\mathbf{C}$.

On appelle *pôle* de F un élément $\alpha \in \mathbf{K}$ en lequel F n'est pas définie. Pour toute forme irréductible $\frac{A_0}{B_0}$ de F, la multiplicité de α en tant que racine de B_0 est la même : on l'appelle l'*ordre* du pôle α.

On appelle *zéro* de F un élément $\alpha \in \mathbf{K}$ en lequel $F(\alpha) = 0$. Pour toute écriture $\frac{A}{B}$ de F, α est alors une racine de A. Pour toute forme irréductible $\frac{A_0}{B_0}$ de F, la multiplicité de α en tant que racine de B_0 est la même : on l'appelle l'*ordre* du zéro α.

Il existe un unique $m \in \mathbf{Z}$ tel que $F = (X-\alpha)^m G$, où G est définie en α et $G(\alpha) \neq 0$: si $m > 0$, α est un zéro d'ordre m de F ; si $m < 0$, c'en est un pôle d'ordre $-m$; si $m = 0$, α n'est ni un zéro ni un pôle. L'entier m est appelé l'*ordre* de F en α.

I.9.5. Fonctions rationnelles

De même que les polynômes servent à « coder » algébriquement les fonctions polynomiales, les fractions rationnelles servent à « coder » algébriquement les *fonctions rationnelles*, c'est-à-dire les fonctions obtenues en divisant une fonction polynomiale par une autre, par exemple

$$x \mapsto f(x) = \frac{x-1}{x^2+x+1}.$$

Pour attacher une *fonction* rationnelle à une fraction rationnelle F, il y a une petite complication due à la multiplicité des écritures $\frac{A}{B}$ de F.

Pour toute fraction rationnelle $F \in \mathbf{K}(X)$ écrite sous forme irréductible $\frac{A}{B}$, l'ensemble des pôles de F, qui est l'ensemble des racines de B dans $\mathbf{K}$, est fini. Son complémentaire dans $\mathbf{K}$ est l'ensemble $\mathcal{D}_F$ des $\alpha \in \mathbf{K}$ tels que $F(\alpha)$ est défini. On l'appelle *ensemble de définition* de F.

Proposition. *Soient $F, G \in \mathbf{K}(X)$. On suppose que pour tout $\alpha \in \mathcal{D}_F \cap \mathcal{D}_G$, $F(\alpha) = G(\alpha)$. Alors $F = G$.*

Démonstration. Si $F = \frac{A}{B}$ et $G = \frac{C}{D}$, on a $(AD - BC)(\alpha) = 0$ pour tout α dans l'ensemble infini $\mathcal{D}_F \cap \mathcal{D}_G$, donc $AD - BC = 0$. □

On peut donc identifier la fraction rationnelle F avec la *fonction rationnelle* $x \mapsto F(x)$ de $\mathcal{D}_F$ dans $\mathbf{K}$. Cette identification est évidemment compatible avec l'addition et la multiplication des fractions rationnelles d'un côté, des fonctions de l'autre. La seule petite difficulté est celle-ci : il peut arriver que $F + G$ ou FG soit défini en un point où F ou G n'est pas défini. Par exemple $\frac{1}{X} - \frac{1}{X}$ et $\frac{X-1}{X} \cdot \frac{X}{X-1}$ sont définies partout.

I.9.6. Décomposition en éléments simples

Si $F = \frac{A}{B} \in K(X)$ est une fraction rationnelle, $A, B \in K[X]$, alors on peut effectuer la division euclidienne de A par B pour écrire : $A = QB + R$. Ainsi on obtient la décomposition suivante de F :

$$F = Q + \frac{R}{B}, \quad \text{où} \quad Q, R \in K[X] \quad \text{et} \quad \deg R < \deg B.$$

Le polynôme Q s'appelle la *partie entière* de F. On va voir maintenant comment décomposer une fraction de la forme $\frac{R}{B}$ avec $\deg R < \deg B$ en somme de fractions plus simples.

Proposition. *Soit*

$$F = \frac{A}{B_1 B_2}$$

une fraction rationnelle non nulle, $A, B_1, B_2 \in \mathbf{K}[X]$, telle que $\deg F < 0$ (c'est-à-dire, $\deg A < \deg B_1 + \deg B_2$). Supposons que

$$\operatorname{pgcd}(B_1, B_2) = 1.$$

Alors il existe un unique couple de polynômes $R_1, R_2 \in \mathbf{K}[X]$ tel que :

(1)
$$F = \frac{R_1}{B_1} + \frac{R_2}{B_2},$$

(2) $\deg R_1 < \deg B_1$ *et* $\deg R_2 < \deg B_2$.

Démonstration. Montrons d'abord l'unicité. Supposons que

$$F = \frac{R_1}{B_1} + \frac{R_2}{B_2} = \frac{S_1}{B_1} + \frac{S_2}{B_2},$$

$\deg R_1 < \deg B_1$, $\deg R_2 < \deg B_2$, $\deg S_1 < \deg B_1$, $\deg S_2 < \deg B_2$. Alors

$$\frac{R_1 - S_1}{B_1} = \frac{S_2 - R_2}{B_2}, \qquad (R_1 - S_1)B_2 = (S_2 - R_2)B_1.$$

Par le lemme d'Euclide, $B_1 \mid R_1 - S_1$ et $B_1 \mid S_2 - R_2$. Or, $\deg(R_1 - S_1) < \deg B_1$ et $\deg(S_2 - R_2) < \deg B_2$. Donc, $R_1 - S_1 = 0$ et $S_2 - R_2 = 0$, c'est-à-dire, $R_1 = S_1$ et $R_2 = S_2$.

Montrons maintenant l'existence. Soit l'identité de Bézout pour B_1 et B_2 :

$$1 = B_1 P_2 + B_2 P_1, \quad P_1, P_2 \in \mathbf{K}[X].$$

Alors

$$F = \frac{A}{B_1 B_2} = \frac{A(B_1 P_2 + B_2 P_1)}{B_1 B_2} = \frac{AP_1}{B_1} + \frac{AP_2}{B_2}.$$

Effectuions les divisions euclidiennes de AP_1 par B_1 et de AP_2 par B_2 :

$$AP_1 = B_1 Q_1 + R_1, \qquad \deg R_1 < \deg B_1,$$
$$AP_2 = B_2 Q_2 + R_2, \qquad \deg R_2 < \deg B_2.$$

Alors

$$F = Q_1 + \frac{R_1}{B_1} + Q_2 + \frac{R_2}{B_2}.$$

Il reste à montrer que $Q_1 + Q_2 = 0$. En effet,

$$Q_1 + Q_2 = F - \frac{R_1}{B_1} - \frac{R_2}{B_2},$$

donc $\deg(Q_1 + Q_2) < 0$ (car $\deg F < 0$, $\deg R_1 < \deg B_1$, $\deg R_2 < \deg B_2$). Ainsi $Q_1 + Q_2 = 0$ et

$$F = \frac{R_1}{B_1} + \frac{R_2}{B_2}.$$ □

Proposition. *Soit*

$$F = \frac{A}{B^m}$$

une fraction rationnelle non nulle, $A, B \in \mathbf{K}[X]$, $m \geqslant 1$, telle que $\deg F < 0$ (c'est-à-dire, $\deg A < m \deg B$). Il existe alors un unique m-uple de polynômes $R_1, \ldots, R_m \in \mathbf{K}[X]$ tel que :

(1)

$$F = \frac{R_1}{B} + \frac{R_2}{B^2} + \cdots + \frac{R_m}{B^m},$$

(2) $\deg R_i < \deg B$ *pour tout* $i \in \{1, \ldots, m\}$.

Démonstration. Il suffit de décomposer A comme

$$A = B^{m-1}R_1 + B^{m-2}R_2 + \cdots + BR_{m-1} + R_m$$

avec $\deg R_i < \deg B$ pour tout $i \in \{1, \ldots, m\}$. Pour cela, on peut, par exemple, effectuer les divisions euclidiennes suivantes. D'abord, la division euclidienne de A par B :

$$A = BQ_m + R_m.$$

Ensuite, la division euclidienne de Q_m par B :

$$Q_m = BQ_{m-1} + R_{m-1}.$$

Et ainsi de suite, jusqu'à la division euclidienne de Q_2 par B :

$$Q_2 = BQ_1 + R_1.$$

Vu que $\deg A < m \deg B$, $\deg Q_m \leqslant \deg A - \deg B$, $\deg Q_{m-1} \leqslant \deg Q_m - \deg B$, et ainsi de suite, et $\deg Q_1 \leqslant \deg Q_2 - \deg B$, on peut conclure que $\deg Q_1 < 0$, donc $Q_1 = 0$. D'où,

$$A = R_m + BR_{m-1} + \cdots + B^{m-2}R_2 + B^{m-1}R_1.$$

□

Définition. La *decomposition en éléments simples* d'une fraction rationnelle $F \in \mathbf{K}(X)$ est une écriture de F comme la somme d'un polynôme (la partie entière de F) et de fractions de la forme $\dfrac{R}{P^m}$, avec $P, R \in \mathbf{K}[X]$ et $m \geqslant 1$, où P est un polynôme irréductible (premier) et $\deg R < \deg P$.

Exemple.

$$\begin{aligned}\frac{X^5 + X^4 + X^3 + X^2 + X + 1}{X^4 - 2X^2 + 1} &= a_0 + a_1X + \frac{b_0 + b_1X + b_2X^2 + b_3X^3}{(X-1)^2(X+1)^2} \\ &= a_0 + a_1X + \frac{c_0 + c_1X}{(X-1)^2} + \frac{d_0 + d_1X}{(X+1)^2} \\ &= a_0 + a_1X + \frac{\alpha_1}{X-1} + \frac{\alpha_2}{(X-1)^2} + \frac{\beta_1}{X+1} + \frac{\beta_2}{(X+1)^2}.\end{aligned}$$