

Polynômes et Fractions rationnelles

1. Généralités

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié.

On appelle suite presque nulle sur A une suite d'éléments de A dont les termes sont tous égaux à 0_A à partir d'un certain rang.

Remarque

On pose $\mathcal{S}(A) = \{\text{suites de } A\}$ et $\mathcal{S}_0(A) = \{\text{suites presque nulles de } A\}$.

- Rappel : addition usuelle des suites et la multiplication usuelle des suites par un scalaire.

Soient $a, b \in \mathcal{S}(A)$ (ou $\mathcal{S}_0(A)$) et $\lambda \in A$.

$$a = (a_0, a_1, a_2, \dots, a_k, \dots) = (a_n)_{n \in \mathbb{N}}.$$

$$b = (b_0, b_1, b_2, \dots, b_k, \dots) = (b_n)_{n \in \mathbb{N}}.$$

$$a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_k + b_k, \dots) = (a_n + b_n)_{n \in \mathbb{N}}.$$

$$\lambda \cdot a = (\lambda \times a_0, \lambda \times a_1, \lambda \times a_2, \dots, \lambda \times a_k, \dots) = (\lambda \times a_n)_{n \in \mathbb{N}}.$$

- Si A est un corps, $(\mathcal{S}(A), +, \cdot)$ est un A -e.v.
- Si A est uniquement un anneau, $(\mathcal{S}(A), +, \cdot)$ est dit un A -module.
- Si A est un corps, $\mathcal{S}_0(A)$ est un s.e.v. de $(\mathcal{S}(A), +, \cdot)$.
- Si A est uniquement un anneau, $\mathcal{S}_0(A)$ est dit un sous-module de $(\mathcal{S}(A), +, \cdot)$.
- Soient les $(e_i)_{i \in \mathbb{N}}$ les éléments de $\mathcal{S}(A)$ définis par

$$e_0 = (1, 0, 0, 0, 0, \dots, 0, \dots)$$

$$e_1 = (0, 1, 0, 0, 0, \dots, 0, \dots)$$

$$e_2 = (0, 0, 1, 0, 0, \dots, 0, \dots)$$

$$\text{De façon générale : } e_n = (e_k^n)_{k \in \mathbb{N}} \text{ où } e_k^n = \delta_{kn} = 0 \text{ si } k \neq n, \\ = 1 \text{ si } k = n.$$

La famille des $(e_i)_{i \in \mathbb{N}}$ est une famille génératrice de $\mathcal{S}(A)$.

On a donc, pour tout $a \in \mathcal{S}(A)$, si $a = (a_n)_{n \in \mathbb{N}}$, alors $a = a_0 e_0 + a_1 e_1 + a_2 e_2 + \dots + a_n e_n + \dots = \sum_{k=0}^{+\infty} a_k e_k$.

En particulier, si $a \in \mathcal{S}_0(A)$, cette somme est finie et a est une C.L. des $(e_i)_{i \in \mathbb{N}}$.

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié. Soient $a, b \in \mathcal{S}_0(A)$.

On définit une loi \times sur $\mathcal{S}_0(A)$ par :

Si $a = (a_0, a_1, a_2, \dots, a_p, \dots)$ et $b = (b_0, b_1, b_2, \dots, b_p, \dots)$, alors

$$a \times b = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots, c_p, \dots) \quad \text{où } c_p = \sum_{k=0}^p a_k b_{p-k} = \sum_{i+j=p} a_i b_j \text{ pour tout entier } p.$$

Exemple

Si $a = (2, 1, 0, 0, 0, \dots, 0, \dots)$
et $b = (0, 1, 3, 0, 0, \dots, 0, \dots)$
alors $a \times b = (0, 2, 7, 3, 0, \dots, 0, \dots)$

Ce résultat correspond à une vision théorique de $(2 + X)(X + 3X^2) = 2X + 7X^2 + 3X^3$.

Remarque

Si on pose : $1 = (1, 0, 0, 0, 0, \dots, 0, \dots)$
 $X = (0, 1, 0, 0, 0, \dots, 0, \dots)$
 $X^2 = (0, 0, 1, 0, 0, \dots, 0, \dots)$

On a $X \times X^2 = X^3$.

On peut vérifier que, dans un cadre plus général, si n et p sont des entiers naturels, $X^n \times X^p = X^{n+p}$.

En effet, $X^n = (0, 0, 0, 0, 0, \dots, 0, 1, 0, \dots) = (\alpha_k)_{k \in \mathbb{N}}$ où $\alpha_k = 0$ si $k \neq n$
 $\alpha_k = 1$ si $k = n$
 $X^p = (0, 0, 0, 0, 0, \dots, 0, 1, 0, \dots) = (\beta_l)_{l \in \mathbb{N}}$ où $\beta_l = 0$ si $l \neq p$
 $\beta_l = 1$ si $l = p$

$$X^n \times X^p = (\gamma_m)_{m \in \mathbb{N}} \text{ où } \gamma_m = \sum_{i=0}^m \alpha_i \beta_{m-i}$$

Le seul cas où $\alpha_i \beta_{m-i}$ est non nul est lorsque $i = n$ et $m - i = p$
C'est-à-dire $m = p + n$.

Définition - Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié.

L'ensemble des suites presque nulles muni des lois de compositions $+$ et \times précédemment définies est un anneau commutatif unifié appelé anneau des polynômes à une indéterminée, à coefficients dans A et est noté $A[X]$.

Remarque

On note $P = (a_0, a_1, a_2, \dots, a_p, 0, 0, \dots) = \sum_{n=0}^p a_n X^n$.

$X = (0, 1, 0, 0, 0, \dots, 0, \dots)$ est appelée l'indéterminée de $A[X]$.

On vérifie que cette notation correspond bien aux lois que l'on connaît sur les polynômes.

Démonstration

- $(A[X], +)$ est un groupe abélien.
L'associativité et la commutativité proviennent directement de ces mêmes propriétés dans A .
 $0 = (0, 0, 0, \dots, 0, \dots)$ est la suite nulle.
Si $P = (a_0, a_1, a_2, \dots, a_n, \dots)$, on définit $-P = (-a_0, -a_1, -a_2, \dots, -a_n, \dots)$.
- $(A[X], \times)$ est un monoïde commutatif.
Loi de composition interne : voir degré.
Loi commutative : de part la définition.
Élément neutre : $1 = (1, 0, 0, 0, 0, \dots, 0, \dots)$
On vérifie que $1.P = P$.
Loi associative :
Si $P = (a_0, a_1, a_2, \dots, a_n, \dots)$, $Q = (b_0, b_1, b_2, \dots, b_n, \dots)$
et $R = (c_0, c_1, c_2, \dots, c_n, \dots)$,

$$PQ = (d_0, d_1, d_2, \dots, d_n, \dots) \text{ avec } d_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{u+v=k} a_u b_v.$$

$$(PQ)R = (e_0, e_1, e_2, \dots, e_n, \dots) \text{ avec } e_l = \sum_{j=0}^l d_j c_{l-j} = \sum_{r+s=l} d_r c_s = \sum_{r+s=l} \left(\sum_{u+v=r} a_u b_v \right) c_s$$

$$= \sum_{u+v+s=l} a_u b_v c_s.$$

- La loi \times est distributive par rapport à la loi $+$.
Si $P = (a_0, a_1, a_2, \dots, a_n, \dots)$, $Q = (b_0, b_1, b_2, \dots, b_n, \dots)$ et $R = (c_0, c_1, c_2, \dots, c_n, \dots)$.
 $(P+Q) \times R = (e_0, e_1, e_2, \dots, e_n, \dots)$ avec $e_l = \sum_{j=0}^l (a_j + b_j) c_{l-j} = \sum_{j=0}^l a_j c_{l-j} + \sum_{j=0}^l b_j c_{l-j}$.

Remarque

On peut identifier les éléments de A à des éléments de $A[X]$.

Exemples

$P = 1 + 2X - 3X^2$ est un polynôme de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

$P = X + \frac{5}{2}X^3$ est un polynôme de $\mathbb{Q}[X]$, $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

$P = \sqrt{3}X - 1$ est un polynôme de $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

$P = (1 + i) - (2 + 5i)X$ est un polynôme de $\mathbb{C}[X]$.

$P = \bar{2}X + \bar{3}$ est un polynôme de $\mathbb{Z}/2\mathbb{Z}[X]$.

$P = 2$ est un polynôme de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié.

On appelle monôme tout polynôme $P = (a_0, a_1, a_2, \dots, a_n, \dots)$ de $A[X]$ tel qu'un unique a_k soit non nul.

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié.

Soit $P = (a_0, a_1, a_2, \dots, a_n, \dots)$ un polynôme de $A[X]$.

Si P est non nul, le plus grand des entiers k tel que $a_k \neq 0$ est appelé degré de P et est noté $\deg P$.

Si P est nul, on pose $\deg P = -\infty$.

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié.

Soient P et Q deux polynômes de $A[X]$.

On a $\deg(P + Q) \leq \sup(\deg P, \deg Q)$ et $\deg PQ \leq \deg P + \deg Q$.

Propriété

Si A est intègre, alors $A[X]$ est intègre et on a $\deg PQ = \deg P + \deg Q$.

Remarques

- Rappel : $A[X]$ est intègre si et seulement si $\forall P, Q \in A[X], P \times Q = 0 \Rightarrow P = 0$ ou $Q = 0$.
- Par convention et par abus, on pose : $\sup(-\infty, \deg Q) = \deg Q$.
 $-\infty + \deg Q = -\infty$.

Démonstration

On suppose : $P = (a_0, a_1, a_2, \dots, a_n, 0, \dots) \neq 0$ $\deg P = n$
 $Q = (b_0, b_1, b_2, \dots, b_p, 0, \dots) \neq 0$ $\deg Q = p$.

- # si $n < p$, $\deg(P + Q) = p$.
- # si $n > p$, $\deg(P + Q) = n$.
- # si $n = p$, $P + Q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, 0, \dots)$.
 Si $a_n + b_n \neq 0$, $\deg(P + Q) = n = \sup(\deg P, \deg Q)$.
 Si $a_n + b_n = 0$, $\deg(P + Q) < n$.
- $PQ = (c_0, c_1, c_2, \dots, c_k, \dots)$ avec $c_j = \sum_{i=0}^j a_i b_{j-i} = \sum_{r+s=j} a_r b_s$
 Si $j > n + p$, on $r + s > n + p$ donc si $r > n$ alors $a_r = 0$ et $a_r b_s = 0$
 si $r \leq n$ alors $n + s \geq r + s > n + p$
 d'où $s > p$ alors $b_s = 0$ et $a_r b_s = 0$.
 $c_j = 0$, on a donc entre autre la loi de composition interne.
 Si $j = n + p$, de la même façon, on obtient $c_j = a_n b_p$.
 Et donc si A est intègre, $c_{n+p} = a_n b_p \neq 0$.

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié et soit $P = (a_0, a_1, a_2, \dots, a_n, \dots)$ un polynôme de $A[X]$.
 Si P est non nul, le plus petit des entiers k tel que $a_k \neq 0$ est appelé valuation de P et est noté $v(P)$.
 Si P est nul, on pose $v(P) = +\infty$.

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié. Soient P et Q deux polynômes de $A[X]$.
 On a $v(P + Q) \geq \inf(v(P), v(Q))$ et $v(P \times Q) \geq v(P) + v(Q)$.

Propriété

Si A est intègre, alors on a $v(P \times Q) = v(P) + v(Q)$.

Démonstration

$P = (0, 0, \dots, 0, a_r, \dots, a_n, 0, \dots) \neq 0$ $v(P) = r$.

$Q = (0, 0, \dots, 0, b_s, \dots, b_p, 0, \dots) \neq 0$ $v(Q) = s$.

- # si $r < s$, $v(P + Q) = r$.
- # si $r > s$, $v(P + Q) = s$.
- # si $r = s$, $P + Q = (0, 0, \dots, 0, a_r + b_r, \dots, a_n \text{ ou } b_p, 0, \dots)$
 Si $a_r + b_r \neq 0$, $v(P + Q) = r = \inf(v(P), v(Q))$.
 Si $a_r + b_r = 0$, $v(P + Q) > r$.
- $PQ = (c_0, c_1, c_2, \dots, c_k, \dots)$ avec $c_j = \sum_{i=0}^j a_i b_{j-i} = \sum_{k+l=j} a_k b_l$
 Si $j < r + s$, on $l + k < r + s$ donc si $l < r$ alors $a_l = 0$ et $a_l b_k = 0$
 si $l \geq r$ alors $r + k \leq l + k < r + s$
 d'où $k < s$ alors $b_k = 0$ et $a_k b_l = 0$
 D'où $c_j = 0$.
 Si $j = r + s$, de la même façon, on obtient $c_j = a_r b_s$.
 Et donc si A est intègre, $c_{r+s} = a_r b_s \neq 0$.

Remarque

Soit $(A, +, \times)$ un anneau commutatif unifié et soit P un polynôme de $A[X]$.
On a $\deg P \geq v(P)$.

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié intègre.
Les unités de $A[X]$ c'est-à-dire les éléments de $A[X]$ qui sont inversibles sont les polynômes de degré 0
inversibles c'est-à-dire les polynômes identifiés aux scalaires de $U(A)$.

Démonstration

Soient P et Q deux polynômes de $A[X]$.
On suppose $P \times Q = 1$
 A est intègre donc $A[X]$ est intègre et on a $\deg PQ = \deg P + \deg Q$.
Or $\deg 1 = 0$ donc $\deg P = 0$ et $\deg Q = 0$.
D'où, il existe $a \in A$ tel que $P = a1$ et il existe $b \in A$ tel que $Q = b1$.
On a $ab = 1$ donc a et b sont des éléments de $U(A)$.

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié.
Soit P un polynôme non nul de $A[X]$.
On appelle coefficient dominant de P le coefficient de son monôme de plus haut degré.
On dit qu'un polynôme est unitaire si et seulement si son coefficient dominant est 1.

2. Identités remarquables

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié.
Soient a et b deux éléments de A et soit n un entier non nul alors

$$\begin{aligned} a^n - b^n &= (a - b) (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}) \\ &= (a - b) \left(\sum_{p+q=n-1} a^p b^q \right) \\ &= (a - b) \left(\sum_{k=0}^{n-1} a^{n-1-k} b^k \right). \end{aligned}$$

Démonstration

$$\begin{aligned} &(a - b) (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}) \\ &= a^n + a^{n-1}b + a^{n-2}b^2 + \dots + a^2b^{n-2} + ab^{n-1} \\ &\quad - a^{n-1}b - a^{n-2}b^2 - \dots - a^2b^{n-2} - ab^{n-1} - b^n \end{aligned}$$

Corollaire

Soit $(A, +, \times)$ un anneau commutatif unifié.
Dans $A[X]$, on a $X^n - a^n = (X - a) (X^{n-1} + aX^{n-2} + a^2X^{n-3} + \dots + a^{n-2}X + a^{n-1})$

Démonstration

$A[X]$ est un anneau commutatif unifié.

Il suffit de prendre $a = X$ et $b = a$.

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié.

Soient a et b deux éléments de A et soit n un entier non nul alors

$$\begin{aligned} (a+b)^n &= a^n + na^{n-1}b + \frac{n(n-1)}{2}a^{n-2}b^2 + \dots + \frac{n(n-1)}{2}a^2b^{n-2} + nab^{n-1} + b^n \\ &= C_n^0 a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \dots + C_n^{n-(n-2)} a^2b^{n-2} + C_n^{n-(n-1)} ab^{n-1} + C_n^0 b^n \\ &= \sum_{k=0}^n C_n^k a^{n-k} b^k \quad \text{où} \quad C_n^k = \frac{n!}{k!(n-k)!}. \end{aligned}$$

Remarque

On peut trouver les C_n^k grâce au triangle de Pascal suivant :

$$\begin{array}{cccccccc} 1 & & & & & & & \\ 1 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ 1 & 3 & 3 & 1 & & & & \\ 1 & 4 & 6 & 4 & 1 & & & \\ 1 & 5 & 10 & 10 & 5 & 1 & & \text{etc...} \end{array}$$

L'indice de ligne donne n et l'indice de colonne donne k .

Qui provient de la formule $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

$$\begin{aligned} C_{n-1}^{k-1} + C_{n-1}^k &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{(k)!(n-1-k)!} \\ &= \frac{(n-1)!}{(n-1)!} + \frac{(n-1)!}{(n-1)!} \\ &= \frac{(k-1)!(n-k)!}{(n-1)! \times k} + \frac{(k)!(n-1-k)!}{(n-1)! \times (n-k)} \\ &= \frac{(k)!(n-k)!}{(n-1)! \times (k+n-k)} + \frac{(k)!(n-k)!}{(n-1)! \times (k+n-k)} \\ &= \frac{n!}{(k)!(n-k)!} = \frac{n!}{k!(n-k)!} = C_n^k. \end{aligned}$$

Exemple

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Démonstration

Par récurrence :

- Vrai au rangs 1 et 2.
- On suppose vrai au rang n

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)(C_n^0 a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \dots + C_n^{n-(n-2)} a^2b^{n-2} + C_n^{n-(n-1)} ab^{n-1} + C_n^0 b^n) \\ &= C_n^0 a^{n+1} + C_n^1 a^n b + C_n^2 a^{n-1}b^2 + \dots + C_n^{n-(n-2)} a^3b^{n-2} + C_n^{n-(n-1)} a^2b^{n-1} + C_n^0 ab^n \\ &\quad + C_n^0 a^n b + C_n^1 a^{n-1}b^2 + C_n^2 a^{n-2}b^3 + \dots + C_n^{n-(n-2)} a^2b^{n-1} + C_n^{n-(n-1)} ab^n + C_n^0 b^{n+1} \\ &= C_{n+1}^0 a^{n+1} + C_{n+1}^1 a^n b + C_{n+1}^2 a^{n-1}b^2 + \dots + C_{n+1}^{n+1-(n-2)} a^3b^{n-2} + C_{n+1}^{n+1-(n-1)} a^2b^{n-1} + C_{n+1}^0 ab^n. \end{aligned}$$

Corollaire

Soit $(A, +, \times)$ un anneau commutatif unifié.

On a dans $A[X]$:

$$(X+a)^n = X^n + naX^{n-1} + \frac{n(n-1)}{2}a^2X^{n-2} + \dots + \frac{n(n-1)}{2}a^{n-2}X^2 + na^{n-1}X + a^n = \sum_{k=0}^n C_n^k a^{n-k} X^k.$$

Démonstration

$A[X]$ est un anneau commutatif unifié.

Il suffit de prendre $a = X$ et $b = a$

Exercice

En déduire $(a-b)^n$.

3. Divisibilité

Définition

Soit $(A, +, \times)$ un anneau commutatif unifié. Soient A et B deux polynômes de $A[X]$.

On dit que B divise A ou que A est divisible par B ou que A est un multiple de B et on note $B|A$ si et seulement si il existe un polynôme Q de $A[X]$ tel que $A = QB$.

Exemple

$X^3 - 1$ est divisible par $X - 1$ car $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

Remarque

De façon plus générale, on a : $X^n - a^n$ est divisible par $X - a$ (voir corollaire).

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié.

Dans l'ensemble des polynômes unitaires de $A[X]$, la relation \mathcal{R} définie par :

$$P \mathcal{R} Q \Leftrightarrow (P \text{ divise } Q)$$

est une relation d'ordre.

Démonstration

- Réflexive : $P = 1 \times P$.
- Antisymétrique : $P \mathcal{R} Q \Leftrightarrow (P \text{ divise } Q)$
 $\Leftrightarrow \exists R / Q = RP$
 $Q \mathcal{R} P \Leftrightarrow (Q \text{ divise } P)$
 $\Leftrightarrow \exists R' / P = R'Q$.

Donc $Q = RR'Q$ d'où $RR' = 1$.

C'est-à-dire R inversible i.e. $R = a1$.

Or P et Q sont unitaires donc $a = 1$ c'est-à-dire $P = Q$.

- Transitive : $P \mathcal{R} Q \Leftrightarrow (P \text{ divise } Q)$
 $\Leftrightarrow \exists R / Q = RP.$
 $Q \mathcal{R} T \Leftrightarrow (Q \text{ divise } T)$
 $\Leftrightarrow \exists R' / T = R'Q.$
D'où $T = R'RP.$
C'est-à-dire $P \mathcal{R} T.$

Dans la suite de ce paragraphe, on considère les polynômes à coefficients dans un corps en pratique \mathbb{Q}, \mathbb{R} ou $\mathbb{C}.$

Propriété

Soient A et B deux polynômes non nuls.

Il existe un unique couple (Q, R) de polynômes tels que $\deg R < \deg B$ et $A = BQ + R.$

On dit qu'on a effectué la division euclidienne de A par $B.$

Q est appelé le quotient et R est appelé le reste de cette division.

Remarque

On peut comparer cette propriété à la division euclidienne dans \mathbb{Z} qui donne par exemple lorsque l'on divise 17 par 5 le résultat suivant $17 = 3 \times 5 + 2.$

Démonstration

- *Unicité*
On suppose qu'il existe un deuxième couple (\tilde{Q}, \tilde{R}) de polynômes tels que $\deg \tilde{R} < \deg B$ et $A = B\tilde{Q} + \tilde{R}.$
On a donc $B(Q - \tilde{Q}) = R - \tilde{R}.$
Comme un corps est intègre, $\deg B + \deg(Q - \tilde{Q}) = \deg(R - \tilde{R})$
Or $\deg(R - \tilde{R}) \leq \sup(\deg(R), \deg(\tilde{R}))$ donc $\deg(R - \tilde{R}) < \deg B.$
D'où $\deg B + \deg(Q - \tilde{Q}) < \deg B.$
Ce qui implique $\deg(Q - \tilde{Q}) = -\infty.$
C'est-à-dire $Q = \tilde{Q}.$
 $A = B\tilde{Q} + \tilde{R} = BQ + R.$
 $\Rightarrow BQ + \tilde{R} = BQ + R$
 $\Rightarrow \tilde{R} = R$
- *Existence*
Par récurrence sur $\deg A$ ($\neq +\infty$).
Si $\deg A = 0, A = a_0$ avec $a_0 \neq 0$ car A non nul.
Si $\deg A < \deg B,$ le couple $(0, A)$ convient.
Si $\deg A \geq \deg B,$ alors $B = b_0$ avec $b_0 \neq 0$ et donc le couple $\left(\frac{a_0}{b_0}, 0\right)$ convient.
En effet, $a_0 = b_0 \times \frac{a_0}{b_0} + 0.$
On suppose la proposition vraie pour tout $k \leq n - 1.$
Si $\deg A = n,$
Si $\deg A < \deg B,$ le couple $(0, A)$ convient.
Si $\deg A \geq \deg B,$
 $A = a_0 + a_1X + \dots + a_nX^n$
 $B = b_0 + b_1X + \dots + b_pX^p$ avec $n \geq p$

Soit $A_1 = A - \frac{a_n}{b_p} X^{n-p} B$. On a $\deg A_1 \leq n - 1$.

D'où il existe un couple (Q_1, R_1) de polynômes tels que $\deg R_1 < \deg B$ et $A_1 = BQ_1 + R_1$.

Or $A = A_1 + \frac{a_n}{b_p} X^{n-p} B$.

D'où $A = BQ_1 + R_1 + \frac{a_n}{b_p} X^{n-p} B = B(Q_1 + \frac{a_n}{b_p} X^{n-p}) + R_1$.

Remarque

Si $R = 0$, B divise A .

Exemple

Soit $A = 3X^3 - 2X^2 + 4X - 3$ et $B = X^2 + 3X + 3$.

On obtient $3X^3 - 2X^2 + 4X - 3 = (3X - 11)(X^2 + 3X + 3) + 28X + 30$.

Méthode de calcul

On regarde les termes de plus haut degré dans $3X^3 - 2X^2 + 4X - 3$ et $X^2 + 3X + 3$

Le quotient est $3X$.

On pose la division

$$\begin{array}{r|l} 3X^3 - 2X^2 + 4X - 3 & X^2 + 3X + 3 \\ - (3X^3 + 9X^2 + 9X) & 3X \\ \hline -11X^2 - 5X & \end{array}$$

On recommence avec $-11X^2 - 5X$ et $X^2 + 3X + 3$

$$\begin{array}{r|l} 3X^3 - 2X^2 + 4X - 3 & X^2 + 3X + 3 \\ - (3X^3 + 9X^2 + 9X) & 3X - 11 \\ \hline -11X^2 - 5X - 3 & \\ - (-11X^2 - 33X - 33) & \\ \hline 28X + 30 & \end{array}$$

donc $3X^3 - 2X^2 + 4X - 3 = (X^2 + 3X + 3)(28X + 30) + 28X + 30$

Rappel

Soit $P = aX^2 + bX + c$ un polynôme de degré 2 à coefficients dans \mathbb{R} (resp. \mathbb{C}), on appelle discriminant de P le réel (resp. le complexe) $\Delta = b^2 - 4ac$.

Propriété

Tout polynôme non nul P à coefficients réels se factorise sous la forme d'un produit de facteurs de degré 1 et de facteurs de degré 2 de discriminant négatif.

Exemple

$$X^4 - 16 = (X - 2)(X + 2)(X^2 + 4).$$

Propriété

Soient A un polynôme et B un polynôme dont le terme constant est non nul (de valuation nulle).

Soit n un entier naturel.

Il existe un unique couple (Q, R) de polynômes tels que $\deg Q \leq n$ et $A = BQ + X^{n+1}R$.

On dit qu'on a effectué la division de A par B suivant les puissances croissantes à l'ordre n .

Q est appelé le quotient et R est appelé le reste à l'ordre n de cette division.

Exemple

Soit $A = 1 + X$ et $B = 1 + X + X^2$ et $n = 4$.

On obtient $1 + X = (1 - X^2 + X^3)(1 + X + X^2) - X^5$.

Démonstration

- Unicité*

On suppose qu'il existe un deuxième couple (\tilde{Q}, \tilde{R}) de polynômes tels que $\deg \tilde{Q} \leq n$ et $A = B\tilde{Q} + X^{n+1}\tilde{R}$.

On a donc $B(Q - \tilde{Q}) = X^{n+1}(R - \tilde{R})$.

Comme A est intègre, $\text{val } B + \text{val}(Q - \tilde{Q}) = n + 1 + \text{val}(R - \tilde{R})$

Or $\text{val } B = 0$.

Donc $\text{val}(Q - \tilde{Q}) = n + 1 + \text{val}(R - \tilde{R})$.

D'où $\text{val}(Q - \tilde{Q}) \geq n + 1$.

Or $\deg(Q - \tilde{Q}) \leq \sup(\deg(Q), \deg(\tilde{Q})) \leq n$.

Ce qui implique $\deg(Q - \tilde{Q}) = -\infty$ et $\text{val}(Q - \tilde{Q}) = +\infty$. C'est-à-dire $Q = \tilde{Q}$.

$A = B\tilde{Q} + X^{n+1}\tilde{R} = BQ + X^{n+1}R$.

$\Rightarrow BQ + X^{n+1}\tilde{R} = BQ + X^{n+1}R$

$\Rightarrow X^{n+1}\tilde{R} = X^{n+1}R$

$\Rightarrow \tilde{R} = R$.
- Existence*

Soit n l'ordre désiré.

Par récurrence descendante sur $\text{val } A$.

Si $\text{val } A = +\infty$, $A = 0$.

Le couple $(0, 0)$ convient.

Si $\text{val } A \geq n + 1$.

$A = X^{n+1}C$ le couple $(0, C)$ convient.

On suppose la propriété vraie pour toutes les valuations $\geq p + 1$ où $p \leq n$.

Si $\text{val } A = p$,

$A = a_p X^p + a_{p+1} X^{p+1} + \dots + a_q X^q$

$B = b_0 + b_1 X + \dots + b_p X^p$ avec $b_0 \neq 0$

Soit $A_1 = A - \frac{a_p}{b_0} X^p B$.

On a $\text{val } A_1 = p + 1$.

D'où il existe un couple (Q_1, R_1) de polynômes tels que $\deg Q_1 \leq n$ et $A_1 = BQ_1 + X^{n+1}R_1$.

Or $A = A_1 + \frac{a_p}{b_0} X^p B$.

D'où $A = BQ_1 + X^{n+1}R_1 + \frac{a_p}{b_0} X^p B$.

$$= B \left(Q_1 + \frac{a_p}{b_0} X^p \right) + R_1.$$

Méthode de calcul

Il faut d'abord ordonner le polynôme suivant les puissances croissantes.

On regarde les termes de constants dans $1 + X$ et $1 + X + X^2$

Le quotient est 1.

On pose la division

$$\begin{array}{r|l} 1 + X & 1 + X + X^2 \\ - (1 + X + X^2) & 1 \\ \hline & - X^2 \end{array}$$

On recommence jusqu'à l'obtention du degré voulu :

$$\begin{array}{r|l} 1 + X & 1 + X + X^2 \\ - (1 + X + X^2) & 1 - X^2 + X^3 \\ \hline & - X^2 \\ & - (-X^2 - X^3 - X^4) \\ & X^3 - X^4 \\ & - (X^3 + X^4 + X^5) \\ & - X^5 \end{array}$$

4. Racines et polynômes dérivés

Définition

Soit K un corps et soit $P = a_0 + a_1X + \dots + a_nX^n$ un polynôme de $K[X]$.

On appelle polynôme dérivé de P et on note P' le polynôme de $K[X]$ défini par

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

Remarque

On peut remarquer que bien que cette définition a pour but de revenir à la définition que nous connaissons, nous n'avons besoin d'aucune connaissance en analyse (c'est-à-dire limite, dérivation etc....) pour travailler sur les polynômes dérivés.

Propriété

Soit K un corps, soient P et Q deux polynômes de $K[X]$ et soit $\lambda \in K$.

$$\text{On a : } (P + Q)' = P' + Q'$$

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

$$(\lambda P)' = \lambda P'.$$

Remarques

- L'application qui, à un polynôme, associe son polynôme dérivé est une application linéaire.
- On définit de manière récursive la dérivée n ième d'un polynôme P (que l'on note $P^{(n)}$) comme la dérivée du polynôme $P^{(n-1)}$ avec la convention $P^{(0)} = P$.

Propriété

Soit K un corps, soient P et Q deux polynômes de $K[X]$ et soit n un entier non nul.

On a : $(P + Q)^{(n)} = P^{(n)} + Q^{(n)}$.

Propriété (Formule de Leibnitz)

Soit K un corps, soient P et Q deux polynômes de $K[X]$ et soit n un entier non nul.

On a : $(PQ)^{(n)} = \sum_{k=0}^n C_n^k P^{(n-k)} Q^{(k)}$.

Démonstration

- Vrai au rang 1.
- On suppose vrai au rang n .

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

Définition

Soit K un corps. Soit $P = a_0 + a_1X + \dots + a_nX^n$ un polynôme de $K[X]$.

On appelle fonction polynomiale associée à P qui est notée abusivement de la même façon, l'application de K dans K définie par $P(x) = a_0 + a_1x + \dots + a_nx^n$.

Remarque

Soit K un corps. Soient P et Q deux polynômes de $K[X]$.

P et Q sont égaux en tant que polynômes si et seulement si ils ont même coefficients respectifs.

P et Q sont égaux en tant que fonctions polynomiales si et seulement si $\forall x \in K, P(x) = Q(x)$.

Lorsque le corps est infini, par exemple \mathbb{Q} , \mathbb{R} ou \mathbb{C} , les deux définitions sont équivalentes. Mais attention, ce n'est pas le cas pour les corps finis où l'on a juste l'implication $[P = Q \Rightarrow \forall x \in K, P(x) = Q(x)]$. La réciproque étant généralement fautive.

Propriété

Soit K un corps, soit P un polynôme de $K[X]$ et soit a un élément de K .

Il existe un polynôme Q tel que $P = (X - a)Q + P(a)$.

Remarque

Vérifier que cette égalité est bien mathématiquement correcte.

Démonstration

1^{ère} méthode : $P = a_0 + a_1X + \dots + a_nX^n$
 $P(a) = a_0 + a_1a + \dots + a_na^n$
 $P - P(a) = a_0 + a_1X + \dots + a_nX^n - (a_0 + a_1a + \dots + a_na^n).$
 $P - P(a) = a_1(X - a) + \dots + a_n(X^n - a^n).$
Or chacun des $(X^i - a^i)$ est factorisable par $(X - a)$.
D'où le résultat.

2^{ème} méthode : Division euclidienne de P par $(X - a)$.
Il existe un unique couple (Q, R) de polynômes tels que $\deg R \leq 1$ et $P = (X - a)Q + R$.
 $\deg R \leq 1 \Rightarrow R = \text{cste.}$
 $P(a) = (a - a)Q + R \Rightarrow R = P(a).$

Définition

Soit K un corps et soit P un polynôme de $K[X]$.

On dit qu'un élément x_0 de K est racine du polynôme P si et seulement si $X - x_0$ divise P .

Propriété

Soit K un corps et soit P un polynôme de $K[X]$.

x_0 est racine du polynôme P si et seulement si $P(x_0) = 0$.

Démonstration

D'après la propriété précédente, on a $P = (X - x_0) Q + P(x_0)$.

x_0 racine de $P \Leftrightarrow X - x_0 \mid P$
 $\Leftrightarrow P(x_0) = 0.$

Définition

Soit K un corps.

Soit P un polynôme de $K[X]$ et soit q un entier supérieur ou égale à 2.

On dit qu'un élément x_0 de K est une racine multiple d'ordre q du polynôme P si et seulement si $(X - x_0)^q$ divise P .

On dit qu'un élément x_0 de K est racine multiple d'ordre q exactement du polynôme P si et seulement si $(X - x_0)^q$ divise P et $(X - x_0)^{q+1}$ ne divise pas P .

Propriété

Soit K un corps.

Soit P un polynôme de $K[X]$ et soit q un entier supérieur ou égale à 1.

x_0 est racine multiple d'ordre q du polynôme P si et seulement si $P(x_0) = P'(x_0) = \dots = P^{(q-1)}(x_0) = 0$.

x_0 est racine multiple d'ordre q exactement du polynôme P si et seulement si $P(x_0) = P'(x_0) = \dots = P^{(q-1)}(x_0) = 0$ et $P^{(q)}(x_0) \neq 0$.

Démonstration

- Vrai si $m = 1$.
- On suppose vrai au rang m .
Soit P un polynôme tel que $P(x_0) = P'(x_0) = \dots = P^{(m)}(x_0) = 0$ et $P^{(m+1)}(x_0) \neq 0$.
On a $P(x_0) = P'(x_0) = \dots = P^{(m-1)}(x_0) = 0$ donc $P = (X - x_0)^m Q$
$$P^{(m)} = [(X - x_0)^m Q]^{(m)} = \sum_{k=0}^m C_m^k [(X - x_0)^m]^{(k)} Q^{(m-k)}$$
$$= \sum_{k=0}^m C_m^k ((m(m-1) \dots (m-k+1)) (X - x_0)^{m-k} Q^{(m-k)})$$
$$P^{(m)}(x_0) = \sum_{k=0}^m C_m^k ((m(m-1) \dots (m-k+1)) (x_0 - x_0)^{m-k} Q^{(m-k)}(x_0))$$
Si $k \neq m$, on a $(x_0 - x_0)^{m-k} = 0$. Donc $0 = P^{(m)}(x_0) = ((m(m-1) \dots 1) Q(x_0))$.
D'où $Q(x_0) = 0$ et donc $X - x_0$ divise Q et $P = (X - x_0)^{m+1} Q$.

Propriété (Formule de Taylor)

Soit K un corps, soit P un polynôme de $K[X]$ tel que $n = \deg P$ et soit $a \in K$.

Alors $P = P(a) + P'(a) \frac{(X-a)}{1!} + P^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + P^{(n)}(a) \frac{(X-a)^n}{n!}$.

Démonstration

1ère étape : Vrai pour $P = X^k$

En effet : $P^{(i)} = (X^k)^{(i)} = k(k-1) \dots (k-i+1) X^{k-i}$ pour tout $i = 1, n$.

Et donc $P^{(i)}(a) \frac{(X-a)^i}{i!} = C_k^i a^{k-i} (X-a)^i$ pour tout $i = 1, n$ mais aussi pour $i = 0$.

D'où $\sum_{i=1}^k P^{(i)}(a) \frac{(X-a)^i}{i!} = \sum_{i=1}^k C_k^i a^{k-i} (X-a)^i = (X-a+a)^k = X^k$.

2ème étape : Vrai pour Q implique vrai pour λQ

$$Q = Q(a) + Q'(a) \frac{(X-a)}{1!} + Q^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + Q^{(n)}(a) \frac{(X-a)^n}{n!}$$

$$\lambda Q = \lambda \left[Q(a) + Q'(a) \frac{(X-a)}{1!} + Q^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + Q^{(n)}(a) \frac{(X-a)^n}{n!} \right]$$

$$\lambda Q = \lambda Q(a) + \lambda Q'(a) \frac{(X-a)}{1!} + \lambda Q^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + \lambda Q^{(n)}(a) \frac{(X-a)^n}{n!}$$

$$\lambda Q = (\lambda Q)(a) + (\lambda Q)'(a) \frac{(X-a)}{1!} + (\lambda Q)^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + (\lambda Q)^{(n)}(a) \frac{(X-a)^n}{n!}$$

3ème étape : Vrai pour R et pour S implique vrai pour $R + S$.

Sans perte de généralité, on peut supposer $n = \deg R \leq \deg S = q$.

$$\text{On a } R = R(a) + R'(a) \frac{(X-a)}{1!} + R^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + R^{(n)}(a) \frac{(X-a)^n}{n!} \text{ et}$$

$$S = S(a) + S'(a) \frac{(X-a)}{1!} + S^{(2)}(a) \frac{(X-a)^2}{2!} + \dots + S^{(q)}(a) \frac{(X-a)^q}{q!}.$$

Puisque $n \leq q$, on a, pour tout entier $n < k$, $R^{(k)} = 0$.

$$R + S = R(a) + S(a) + (R'(a) + S'(a)) \frac{(X-a)}{1!} + \dots + (R^{(n)}(a) + S^{(n)}(a)) \frac{(X-a)^n}{n!}$$

$$+ S^{(n+1)}(a) \frac{(X-a)^{n+1}}{(n+1)!} + \dots + S^{(q)}(a) \frac{(X-a)^q}{q!}$$

$$R + S = R(a) + S(a) + (R'(a) + S'(a)) \frac{(X-a)}{1!} + \dots + (R^{(n)}(a) + S^{(n)}(a)) \frac{(X-a)^n}{n!}$$

$$+ (R^{(n+1)}(a) + S^{(n+1)}(a)) \frac{(X-a)^{n+1}}{(n+1)!} + \dots + (R^{(q)}(a) + S^{(q)}(a)) \frac{(X-a)^q}{q!}$$

$$R + S = (R+S)(a) + (R+S)'(a) \frac{(X-a)}{1!} + \dots + (R+S)^{(n)}(a) \frac{(X-a)^n}{n!}.$$

5. Polynômes complexes

Définition

Soit $P = \sum_{k=1}^n a_k X^k$ un polynôme de $\mathbb{C}[X]$.

On appelle polynôme conjugué de P , le polynôme $\bar{P} = \sum_{k=1}^n \bar{a}_k X^k$.

Propriété

Soient P et Q deux polynômes de $\mathbb{C}[X]$

1. $\overline{P+Q} = \bar{P} + \bar{Q}$.
2. $\overline{P \times Q} = \bar{P} \times \bar{Q}$.
3. $\overline{\bar{P}} = P$.
4. $\bar{P} = P \Leftrightarrow P \in \mathbb{R}[X]$.
5. $\forall z \in \mathbb{C}$, on a $\overline{P(z)} = \bar{P}(\bar{z})$.
6. $z_0 \in \mathbb{C}$, z_0 est racine de $P \Leftrightarrow \bar{z}_0$ est racine de \bar{P} .

Démonstration

Ces propriétés découlent directement des propriétés de celle des conjugués dans \mathbb{C} .

En particulier pour le 6°, z_0 est racine de $P \Leftrightarrow \exists p \in \mathbb{N}^*$ et $\exists Q \in \mathbb{C}[X] / P = (X - z_0)^p Q$
 $\Rightarrow \bar{P} = (X - \bar{z}_0)^p \bar{Q}$.

Corollaire

Soit P un polynôme de $\mathbb{R}[X]$.

Si $z_0 \in \mathbb{C}$ est racine de P alors \bar{z}_0 est racine de P .

Démonstration

Découle directement de ce qu'il y a au dessus.

Lemme

Soit C un polynôme de $\mathbb{C}[X]$ et soient A et B deux polynômes de $\mathbb{R}[X]$.

Si $A = BC$ alors $C \in \mathbb{R}[X]$.

Démonstration

Si $A = a_0 + a_1 X + \dots + a_n X^n$, $B = b_0 + b_1 X + \dots + b_p X^p$ et $C = c_0 + c_1 X + \dots + c_q X^q$.

Soit j le plus indice tel que $c_j \notin \mathbb{R}$.

On a $a_j = \sum_{i=0}^j b_i c_{j-i} = \sum_{k+l=j} b_k c_l$, $b_i c_{j-i} \in \mathbb{R}$ pour $i > 0$ et $b_0 c_j \notin \mathbb{R}$ donc $a_j \notin \mathbb{R}$: absurde.

6. Arithmétique des polynômes

Propriété

$\mathbb{R}[X]$ est un anneau principal.

Démonstration

Soit I un idéal de $\mathbb{R}[X]$, on a donc I sous-groupe de $\mathbb{R}[X]$.

- si $I = \{0\}$, on a bien $I = 0 \cdot \mathbb{R}[X]$.
- si $I \neq \{0\}$, soit A un polynôme non nul de degré minimal dans I .
Un tel polynôme existe car l'ensemble des degrés est une partie de \mathbb{N} .
 $\forall B \in I, \exists R, Q \in \mathbb{R}[X] / \deg R < \deg A$ et $B = AQ + R$.
D'où $R = B - AQ$ or $AQ \in I$ car $A \in I, Q \in \mathbb{R}[X]$ et I idéal.
D'où $R = B - AQ \in I$ car $B \in I, AQ \in I$ et I idéal donc sous-groupe.
On a donc $R \in I, \deg R < \deg A$ et A de degré minimal dans I .
Donc $R = 0$ et $B = AQ$ c'est-à-dire $I \subset A \cdot \mathbb{R}[X]$.
On vérifie aisément que $I \supset A \cdot \mathbb{R}[X]$ donc $I = A \cdot \mathbb{R}[X]$.

Propriété

Soit $(A, +, \times)$ un anneau commutatif unifié et soient A et B deux polynômes de $A[X]$.

Si $A|B$ et $B|A$ alors $\exists c \in A$ tel que c inversible et $A = cB$.

Démonstration

Si $A|B$ alors $\exists P \in A[X] / B = AP$.

Si $B|A$ alors $\exists Q \in A[X] / A = BQ$.

Donc $A = BQ = APQ$ c'est-à-dire $1 = PQ$

Or les seuls polynômes inversibles de $A[X]$ sont les éléments inversibles de A .

Remarque

On travaillera de préférence avec un corps K . En pratique, ce sera \mathbb{Q}, \mathbb{R} ou \mathbb{C} .

Rappel

Soient $P \in K[X]$ et $Q \in K[X]$.

- Un élément de $P \cdot K[X] \cap Q \cdot K[X]$ est, à la fois un multiple de P et de Q .
On appelle plus petit multiple commun de P et de Q tout générateur de $P \cdot K[X] \cap Q \cdot K[X]$.
Tout multiple commun à P et Q est un multiple du ppcm(P, Q).
- On appelle plus grand diviseur commun de P et de Q tout générateur de $P \cdot K[X] + Q \cdot K[X]$.
Le pgcd(P, Q) est un diviseur commun à P et à Q .
Tout diviseur autre commun à P et à Q divise le pgcd(P, Q).

Proposition

Le pgcd de deux polynômes est déterminé de manière unique à la multiplication par une constante près.

Le ppcm de deux polynômes est déterminé de manière unique à la multiplication par une constante près.

Remarques

- Cela provient directement du fait que $P.K[X] = Q.K[X]$ si et seulement si $\exists c \in A$ tel que c inversible et $P = cQ$.
- Donc on choisit pour le ppcm et le pgcd le polynôme unitaire engendrant l'idéal.
- Soient $A, B \in K[X]$ et soit $\lambda, \mu \in K^*$, alors $\text{pgcd}(A, B) = \text{pgcd}(\lambda A, \mu B)$ et $\text{ppcm}(A, B) = \text{ppcm}(\lambda A, \mu B)$.
En effet, $A.K[X] = \lambda A.K[X]$ et $B.K[X] = \mu B.K[X]$.

Propriété

Soit $(K, +, \times)$ un corps commutatif et soient A et B deux polynômes de $K[X]$.

Soit $M = \text{ppcm}(A, B)$. M est le multiple unitaire de A et de B de plus petit degré.

- On a :
- (i) $A \mid M$ et $B \mid M$.
 - (ii) $\forall M' \in K[X] / A \mid M'$ et $B \mid M'$ alors $M \mid M'$.

Démonstration

- $M \in A.K[X] \cap B.K[X]$.
Donc $M \in A.K[X]$ c'est-à-dire $A \mid M$. De même $M \in B.K[X]$ c'est-à-dire $B \mid M$.
- Soit $\mathcal{M} = \{P \in K[X] / P \text{ multiple de } A \text{ et } P \text{ multiple de } B\} = \{P \in K[X] / A \mid P \text{ et } B \mid P\}$.
 $\mathcal{M} \neq \emptyset$ car $AB \in \mathcal{M}$ et soit $D = \{\deg P / P \in \mathcal{M}\}$.
 D est un sous-ensemble de \mathbb{N} donc D admet un plus petit élément k .
Soit $M \in \mathcal{M} / \deg M = k$ et M unitaire.
 $\forall M' \in \mathcal{M}$, $M' = MQ + R$ avec $\deg R < \deg M$.
Or $R = M' - MQ \in \mathcal{M}$.
Donc $R = 0$.

Propriété

Soit $(K, +, \times)$ un corps commutatif et soient A et B deux polynômes de $K[X]$.

Soit $D = \text{pgcd}(A, B)$ alors $\exists (U, V) \in K[X] / AU + BV = D$.

Propriété

Soient $A, B \in K[X]$ et $D = \text{pgcd}(A, B)$.

- On a :
- (i) $D \mid A$ et $D \mid B$.
 - (ii) $\forall D' \in K[X] / D' \mid A$ et $D' \mid B$ alors $D' \mid D$.

Démonstration

- $A = A \times 1 + B \times 0 \in A.K[X] + B.K[X] = D.K[X]$ d'où le résultat.
De la même façon, $B = A \times 0 + B \times 1 \in A.K[X] + B.K[X] = D.K[X]$
- $D' \mid A \Leftrightarrow A = D' \times Q_1$ avec $Q_1 \in K[X]$.
 $D' \mid B \Leftrightarrow B = D' \times Q_2$ avec $Q_2 \in K[X]$.
Or $\exists U, V \in K[X] / D = A.U + B.V$ d'où $D = D'.Q_1.U + D'.Q_2.V = D'(Q_1.U + Q_2.V)$.

Propriété

Soient $A, B \in K[X]$ et soit $P \in K[X]$ tel que P unitaire.

Alors $\text{pgcd}(P \times A, P \times B) = P \times \text{pgcd}(A, B)$ et $\text{ppcm}(P \times A, P \times B) = P \times \text{ppcm}(A, B)$.

Démonstration

Soient $D = \text{pgcd}(A,B)$ et $\Delta = \text{pgcd}(P \times A, P \times B)$, on veut montrer que $\Delta = P.D$ c'est-à-dire $\Delta.K[X] = (P.D).K[X]$.

- Soit $Q \in P.D.K[X] \Leftrightarrow \exists R \in K[X] / Q = P.D.R$
 $\exists U, V \in K[X] / D = A.U + B.V$
D'où $P.D = P.A.U + P.B.V$ et $Q = P.D.R = P.A.U.R + P.B.V.R \in (P.A)K[X] + (P.B)K[X] = \Delta.K[X]$
- Soit $T \in \Delta.K[X]$.
D'après la définition de $(P.A).K[X] + (P.B).K[X]$, il existe alors deux polynômes F et G tels que $T = (P.A).F + (P.B).G = P.(A.F + B.G)$.
Or $A.F + B.G \in A.K[X] + B.K[X] = D.K[X]$ donc $T \in (P.D).K[X]$.

De plus, $AB = \text{pgcd}(A,B) \times \text{ppcm}(A,B)$.

Donc $(PA)(PB) = P \times \text{pgcd}(A,B) \times P \times \text{ppcm}(A,B) = \text{pgcd}(P \times A, P \times B) \times \text{ppcm}(P \times A, P \times B)$.

Remarques

- Soit P un polynôme unitaire non nul. On a $\text{pgcd}(0,P) = P$.
En effet $0.K[X] = \{0\}$, donc $0.K[X] + P.K[X] = \{0\} + P.K[X] = P.K[X]$
- Soit P un polynôme. On a $\text{pgcd}(1,P) = 1$.
En effet $P.K[X] \subset K[X] = 1.K[X]$, d'où $1.K[X] + P.K[X] = 1.K[X]$

Propriété

Soient $A, B \in K[X]$. On a : $(A,B) \neq (0,0) \Leftrightarrow \text{pgcd}(A,B) \neq 0$

Démonstration

- $\text{pgcd}(0,0) = 0$
En effet, $0.K[X] = \{0\}$, donc $0.K[X] + 0.K[X] = \{0\} + \{0\} = \{0\} = 0.K[X]$
- Si $\text{pgcd}(A,B) = 0$, alors $A.K[X] + B.K[X] = \{0\}$.
Or $A.K[X] \subset A.K[X] + B.K[X]$.
Donc $A.K[X] \subset \{0\}$ et $B.K[X] \subset \{0\}$.
On a alors $(A.K[X] = \emptyset \text{ ou } A.K[X] = \{0\})$ et $(B.K[X] = \emptyset \text{ ou } B.K[X] = \{0\})$.
Or $A.K[X]$ et $B.K[X]$ ne peuvent être vides, on a alors obligatoirement $A.K[X] = B.K[X] = \{0\}$.
Donc $A = B = 0$.

Propriété

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié et soient A et B deux polynômes non nuls de $\mathcal{A}[X]$.

Soient Q et $R \in \mathcal{A}[X] / A = BQ + R$ avec $\deg R < \deg B$.

Alors $D = \text{pgcd}(A,B) \Leftrightarrow D = \text{pgcd}(B,R)$.

Démonstration

1ère méthode :

$$\begin{aligned} D &= \text{pgcd}(A,B) \text{ et } D' = \text{pgcd}(B,R) \quad A = BQ + R \\ D|A \text{ et } D|B &\Rightarrow D|R \\ &\Rightarrow D|D' \\ D'|B &\Rightarrow D'|BQ \\ D'|R \text{ et } D'|BQ &\Rightarrow D'|A \qquad \qquad \qquad \Rightarrow D'|D. \end{aligned}$$

2ème méthode : Soit $\mathcal{M}_1 = \{ P \in \mathcal{A}[X] / P|A \text{ et } P|B \}$.
 Soit $\mathcal{M}_2 = \{ P \in \mathcal{A}[X] / P|B \text{ et } P|R \}$.
 On veut montrer que $\mathcal{M}_1 = \mathcal{M}_2$.

$P \in \mathcal{M}_1 \Leftrightarrow P|A \text{ et } P|B$
 $\Leftrightarrow \exists S \in \mathcal{A}[X] / A = PS \text{ et } \exists T \in \mathcal{A}[X] / B = PT$
 $\Rightarrow PS = PTQ + R$
 $\Rightarrow R = PS - PTQ$
 $\Rightarrow R = P(S - TQ)$
 $\Rightarrow P|R$
 $\Rightarrow P \in \mathcal{M}_2$

$P \in \mathcal{M}_2 \Leftrightarrow P|B \text{ et } P|R$
 $\Leftrightarrow \exists S \in \mathcal{A}[X] / B = PS \text{ et } \exists T \in \mathcal{A}[X] / R = PT$
 $\Rightarrow A = PSQ + PT$
 $\Rightarrow A = P(SQ + T)$
 $\Rightarrow P|A$
 $\Rightarrow P \in \mathcal{M}_1$

Corollaire

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié et soient A et B deux polynômes de $\mathcal{A}[X]$.

Soit $D = \text{pgcd}(A, B)$.

D est le polynôme de plus petit degré pour lequel il existe des polynômes U et V tels que $AU + BV = D$.

Définition

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié et soient A et B deux polynômes de $\mathcal{A}[X]$.

On dit que A et B sont premiers entre eux si et seulement si $\text{pgcd}(A, B) = 1$.

Définition

Soit $(K, +, \times)$ un corps commutatif. On dit qu'un polynôme P de $K[X]$ est irréductible si et seulement si :

- $\deg P \geq 1$ (on exclut polynômes inversibles).
- $\forall Q \in K[X], Q|P \Rightarrow Q = \lambda$ ou $Q = \lambda P$ avec $\lambda \in K^*$.

Exemple

Soit $P = X^2 + 1$.

Si on considère P comme un polynôme de $\mathbb{R}[X]$, P est irréductible.

Si on considère P comme un polynôme de $\mathbb{C}[X]$, P n'est pas irréductible car $X^2 + 1 = (X - i)(X + i)$.

Remarque

P est un polynôme irréductible de K si et seulement si les seuls diviseurs de P sont de degré 0 ou de même degré que P .

Propriété

Soient $P, Q \in K[X]$ tels que P soit un polynôme irréductible.

Alors Q n'est pas un multiple de $P \Leftrightarrow Q$ et P sont premiers entre eux.

C'est-à-dire $Q \notin P.K[X] \Leftrightarrow \text{pgcd}(P, Q) = 1$

Démonstration

Soit $D = \text{pgcd}(P, Q)$.

On a, par caractérisation du pgcd, $D \mid P$ et $D \mid Q$

Comme $D \mid P$ alors $D = 1$ ou $D = \lambda P$ avec $\lambda \in K^*$

- Si $Q \in P.K[X]$, alors $P \mid Q$ or $P \mid P$ et donc $P \mid D$.
Donc $D = \lambda P$ avec $\lambda \in K^*$ et $\text{pgcd}(P, Q) \neq 1$.
- Si $Q \notin P.K[X]$, alors on ne peut avoir $D = \lambda P$ avec $\lambda \in K^*$ car comme $D \mid Q$, on aurait $P \mid Q$ ce qui est absurde. Donc $D = 1$, soit $\text{pgcd}(P, Q) = 1$

Propriété

Soit $(K, +, \times)$ un corps commutatif et soient A et B deux polynômes de $K[X]$.

A et B sont premiers entre eux si et seulement si il existe des polynômes U et V tels que $AU + BV = 1$.

Démonstration

(\Rightarrow) déjà fait.

(\Leftarrow) $A.U + B.V = 1$.

Soit $D = \text{pgcd}(A, B)$.

On a $D \mid A \Rightarrow D \mid A.U$

$D \mid B \Rightarrow D \mid B.V \quad \Rightarrow D \mid A.U + B.V \quad \Rightarrow D \mid 1 \quad \Rightarrow D = 1$.

Propriété

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié et soient A, B et C trois polynômes de $\mathcal{A}[X]$.

Si $A \mid BC$ et A, B premiers entre eux alors $A \mid C$.

Démonstration

$A \mid BC \Leftrightarrow \exists S \in \mathcal{A}[X] / BC = AS$.

A, B premiers entre eux $\Leftrightarrow \exists U, V \in \mathcal{A}[X] / AU + BV = 1$.

$$\Rightarrow ACU + BCV = C$$

$$\Rightarrow ACU + ASV = C$$

$$\Rightarrow A(CU + SV) = C$$

$$\Rightarrow A \mid C.$$

Propriété

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié et soient A, B et C trois polynômes de $\mathcal{A}[X]$.

Si A, B premiers entre eux et A, C premiers entre eux alors A et BC sont premiers entre eux.

Démonstration

A, B premiers entre eux $\Leftrightarrow \exists U, V \in \mathcal{A}[X] / AU + BV = 1$.

A, C premiers entre eux $\Leftrightarrow \exists S, T \in \mathcal{A}[X] / AS + CT = 1$.

$$\Rightarrow (AU + BV)(AS + CT) = 1.$$

$$\Rightarrow AAUS + AUCT + BVAS + BVCT = 1.$$

$$\Rightarrow A(AUS + UCT + BVS) + BC(VT) = 1.$$

$$\Rightarrow A, BC \text{ premiers entre eux.}$$

Propriété

Soit $(\mathcal{A}, +, \times)$ un anneau commutatif unifié, soient A et B deux polynômes de $\mathcal{A}[X]$ et soit $D = \text{pgcd}(A, B)$. Si $A = D.A_1$ et $B = D.B_1$ alors A_1, B_1 premiers entre eux.

Démonstration

$$\begin{aligned} \exists U, V \in \mathcal{A}[X] / & \quad AU + BV = D. \\ \Leftrightarrow & \quad D.A_1U + D.B_1V = D \\ \Leftrightarrow & \quad A_1U + B_1V = 1 \end{aligned}$$

Résolution d'équations diophantiennes

Soient A, B et C trois polynômes de $\mathcal{A}[X]$ et soit $D = \text{pgcd}(A, B)$.

On cherche à résoudre l'équation dans $\mathcal{A}[X]$: $AY + BZ = C$ (E)

1. (E) admet des solutions si et seulement si $D | C$ car $AY + BZ = D.A_1Y + D.B_1Z = D(A_1Y + B_1Z)$.
2. $D | C \Leftrightarrow \exists S \in \mathcal{A}[X] / C = DS$.

L'équation (E) devient : $D.A_1Y + D.B_1Z = DS$
 $A_1Y + B_1Z = S$ (E')

Les solutions de (E') sont les mêmes que celles de (E).

Nous savons que A_1, B_1 premiers entre eux donc $\exists U, V \in \mathcal{A}[X] / A_1U + B_1V = 1$

Donc $A_1US + B_1VS = S$

Nous avons déjà un couple de solutions $(US, VS) = (E, F)$.

Soit (X, Y) un autre couple de solutions : $AY + BZ = C$

$$AE + BF = C$$

$$\Rightarrow A(Y - E) + B(Z - F) = 0.$$

$$\Rightarrow A_1D(Y - E) + B_1D(Z - F) = 0.$$

$$\Rightarrow A_1(Y - E) + B_1(Z - F) = 0.$$

$$\Rightarrow A_1(Y - E) = B_1(F - Z).$$

Or A_1, B_1 premiers entre eux donc $B_1 | (Y - E)$ et $A_1 | (F - Z)$

$B_1 | (Y - E) \Leftrightarrow \exists Q \in \mathcal{A}[X] / (Y - E) = B_1Q$.

$$\Rightarrow A_1B_1Q = B_1(F - Z).$$

$$\Rightarrow A_1Q = (F - Z).$$

$$(Y - E) = B_1Q \quad \text{et} \quad A_1Q = (F - Z)$$

$$Y = B_1Q + E \quad \text{et} \quad Z = F - A_1Q$$

$$Y = B_1Q + US \quad \text{et} \quad Z = VS - A_1Q$$

Donc l'ensemble des solutions est $\{(Y, Z) / Y = B_1Q + US \text{ et } Z = VS - A_1Q\}$

Théorème

Tout polynôme de $\mathbb{C}[X]$ de degré ≥ 1 admet au moins une racine.

Corollaire

Soit P un polynôme de $\mathbb{C}[X]$.

P est irréductible si et seulement si $\deg P = 1$.

Démonstration

Découle directement du théorème.

Corollaire

Soit P un polynôme de $\mathbb{C}[X]$ de degré $n \geq 1$.

Alors P admet une décomposition unique à l'ordre près de la forme :

$$P = c(X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_p)^{\alpha_p} \quad \text{où } \alpha_i \text{ est l'ordre de multiplicité de la racine } a_i.$$

Remarque

On a $\alpha_1 + \alpha_2 + \dots + \alpha_p = n$.

Propriété

Soit P un polynôme de $\mathbb{R}[X]$.

P est irréductible si et seulement si

- soit $\deg P = 1$.
- soit $\deg P = 2$ et P de discriminant strictement négatif.

Démonstration

Soit P un polynôme de $\mathbb{R}[X]$ tel que $\deg P \geq 3$.

On sait que P est aussi un polynôme de $\mathbb{C}[X]$ donc admet au moins une racine complexe z_0 .

- Si $z_0 \in \mathbb{R}$, P n'est pas irréductible.
- Si $z_0 \in \mathbb{C}$, alors \bar{z}_0 est racine de P .

On peut donc factoriser P dans $\mathbb{C}[X]$: $\exists Q \in \mathbb{C}[X] / P = (X - z_0)(X - \bar{z}_0)Q$

$$P = (X^2 - (z_0 + \bar{z}_0)X + z_0\bar{z}_0)Q$$

Or $(X^2 - (z_0 + \bar{z}_0)X + z_0\bar{z}_0) \in \mathbb{R}[X]$ donc $Q \in \mathbb{R}[X]$ et $\deg Q \geq 1$.

D'où P n'est pas irréductible.

Corollaire

Soit P un polynôme de $\mathbb{R}[X]$ de degré $n \geq 1$.

Alors P admet une décomposition unique à l'ordre près de la forme :

$$P = c(X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_p)^{\alpha_p} Q_1^{\beta_1} \dots Q_q^{\beta_q} \quad \text{où } \alpha_i \text{ est l'ordre de multiplicité de la racine } a_i.$$

Q_j est un polynôme unitaire de degré 2 et irréductible dans \mathbb{R} .

Remarque

On peut avoir $q = 0$.

7. Fractions rationnelles

Propriété

Soit $(A, +, \times)$ un anneau commutatif intègre.

La relation \mathcal{R} définie sur $A \times A^*$ par $(a, b) \mathcal{R} (c, d) \Leftrightarrow ad = bc$ est une relation d'équivalence.

L'ensemble quotient $A \times A^* / \mathcal{R}$ muni des deux lois de compositions suivantes est un corps appelé corps des fractions :

$$\overline{(a, b)} \times \overline{(c, d)} = \overline{(ac, bd)} \quad \text{et} \quad \overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}.$$

Démonstration

- Relation d'équivalence.
- Relation compatible avec les lois.
- Structure de corps.

Définition

Soit K un corps. On appelle fraction rationnelle à coefficients dans K tout élément du corps des fractions de $K[X]$. L'ensemble de ces fractions est noté $K(X)$.

Remarques

- Un élément $\overline{(P, Q)}$ de $K(X)$ est noté $\frac{P}{Q}$.
- On peut identifier $P \in K[X]$ avec $\frac{P}{1} \in K(X)$.

A partir de maintenant nous nous intéresserons uniquement aux fractions rationnelles de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$.

Propriété

Toute fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ admet un unique représentant $\frac{P}{Q}$ tel que :

- P et Q sont premiers entre eux.
- Q est unitaire

Ce représentant est appelée fraction irréductible (ou réduite) de la fraction.

Démonstration

Soit $\frac{A}{B}$ un représentant quelconque de la fraction.

Soit $D = \text{pgcd}(A, B)$.

On a $A = D.A_1$ et $B = D.B_1$ et A_1, B_1 premiers entre eux.

Soit b le coefficient du terme de plus haut degré de B_1 .

On pose $P = \frac{1}{b}A_1$ et $Q = \frac{1}{b}B_1$

On a P et Q premiers entre eux et Q unitaire.

Et on a bien $\frac{A}{B} = \frac{P}{Q}$ car $AQ = D.A_1 \frac{1}{b}B_1 = D.B_1 \frac{1}{b}A_1 = BP$.

Définition

Soit $\frac{P}{Q}$ une fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$.

Soient $P(x)$ la fonction polynomiale associée à P et $Q(x)$ la fonction polynomiale associée à Q .

On appelle fonction rationnelle associée à $\frac{P}{Q}$ la fonction de \mathbb{R} dans \mathbb{R} ou de \mathbb{C} dans \mathbb{C} qui, à tout réel x ,

associe $\frac{P(x)}{Q(x)}$.

Remarque

Il va sans dire (mais c'est toujours mieux de le dire) qu'il est important de vérifier l'ensemble de définition.

Propriété

Si une fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ admet un représentant $\frac{P}{Q}$ tel que $\deg P < \deg Q$, il en est de même pour tout autre représentant de la fraction. Dans ce cas, on dit que la fraction est pure.

Démonstration

$$\deg P < \deg Q \Rightarrow \deg P - \deg Q < 0.$$

Soit $\frac{A}{B}$ un autre représentant de la fraction.

$$\frac{A}{B} = \frac{P}{Q} \Leftrightarrow AQ = BP$$

$$\Rightarrow \deg A + \deg Q = \deg B + \deg P$$

$$\Rightarrow \deg A - \deg B = \deg P - \deg Q < 0$$

$$\Rightarrow \deg A < \deg B.$$

Propriété

La somme et le produit de deux fractions pures sont pures.

Remarque

On n'a pas "l'équivalent" dans \mathbb{Q} car par exemple : $\frac{5}{7} + \frac{6}{7} = \frac{11}{7}$.

Démonstration

Soient $\frac{A}{B}$ et $\frac{C}{D}$ deux fractions pures de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$. On a $\deg A < \deg B$ et $\deg C < \deg D$.

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

$$\deg AC = \deg A + \deg C < \deg B + \deg D = \deg BD$$

- $\frac{A}{B} + \frac{C}{D} = \frac{AD+BC}{BD}$.

$$\deg A < \deg B \quad \text{donc} \quad \deg AD = \deg A + \deg D < \deg B + \deg D = \deg BD.$$

$$\deg C < \deg D \quad \text{donc} \quad \deg BC = \deg B + \deg C < \deg B + \deg D = \deg BD.$$

$$\deg (AD + BC) \leq \max(\deg AD, \deg BC) < \deg BD.$$

Propriété

Toute fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ se décompose de manière unique en la somme d'un polynôme et d'une fraction pure.

Le polynôme obtenu est appelé partie entière de la fraction.

Démonstration

- *Unicité*

On suppose qu'il existe P, Q deux polynômes de $\mathbb{R}[X]$ et $\frac{R}{T}, \frac{U}{V}$ deux fractions pures tels que

$$\frac{A}{B} = P + \frac{R}{T} = Q + \frac{U}{V}. \text{ On a donc } P - Q = \frac{U}{V} - \frac{R}{T} \text{ et } \frac{P-Q}{1} = \frac{U}{V} - \frac{R}{T}.$$

Or $\frac{U}{V} - \frac{R}{T}$ est une fraction pure donc $\frac{P-Q}{1}$ aussi c'est-à-dire $\deg(P-Q) < \deg 1 = 0$.

D'où $\deg(P-Q) = -\infty$ c'est-à-dire $P-Q=0$ et donc $P=Q$.

$$\Rightarrow P-Q = \frac{U}{V} - \frac{R}{T} = 0 \text{ et } \frac{U}{V} = \frac{R}{T}$$

- *Existence*
Soit $\frac{A}{B}$ une fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$.
Il existe un unique couple (Q,R) de polynômes tels que $\deg R < \deg B$ et $A = BQ + R$.
On a $\frac{A}{B} = \frac{BQ+R}{B} = Q + \frac{R}{B}$. La fraction $\frac{R}{B}$ est une fraction pure.

Propriété

Soit une fraction pure de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ qui admet un représentant de la forme $\frac{A}{B_1 B_2}$ où B_1 et B_2 sont premiers entre eux.

Alors elle se décompose de manière unique en somme de deux fractions pures $\frac{A_1}{B_1} + \frac{A_2}{B_2}$.

Démonstration

- *Unicité*
On suppose $\frac{A}{B_1 B_2} = \frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{\tilde{A}_1}{B_1} + \frac{\tilde{A}_2}{B_2}$.
On a $\frac{A_1 - \tilde{A}_1}{B_1} = \frac{\tilde{A}_2 - A_2}{B_2}$ et donc $(A_1 - \tilde{A}_1)B_2 = (\tilde{A}_2 - A_2)B_1$.
Or B_1 et B_2 sont premiers entre eux, donc B_1 divise $A_1 - \tilde{A}_1$.
Or puisque $\frac{A_1}{B_1}$ et $\frac{\tilde{A}_1}{B_1}$ sont des fraction pures $\deg(A_1 - \tilde{A}_1) \leq \max(\deg A_1, \deg \tilde{A}_1) < \deg B_1$.
D'où $A_1 - \tilde{A}_1 = 0$ c'est-à-dire $A_1 = \tilde{A}_1$. De même $A_2 - \tilde{A}_2 = 0$ c'est-à-dire $A_2 = \tilde{A}_2$.

Existence

B_1 et B_2 sont premiers entre eux $\Rightarrow \exists U, V \in A[X] / B_1 U + B_2 V = 1$

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

On peut décomposer $\frac{AV}{B_1} = E + \frac{A_1}{B_1}$ avec $\frac{A_1}{B_1}$ fraction pure.

On obtient $\frac{A}{B_1 B_2} = \frac{A_1}{B_1} + E + \frac{AU}{B_2} = \frac{A_1}{B_1} + \frac{EB_2 + AU}{B_2}$. On pose $A_2 = EB_2 + AU$.

La fraction $\frac{EB_2 + AU}{B_2}$ est bien pure car $\frac{EB_2 + AU}{B_2} = \frac{A}{B_1 B_2} - \frac{A_1}{B_1}$.

Cas particulier

Si la fraction pure est de la forme $\frac{A}{X^n B}$, on obtient la décomposition en effectuant la division suivant les puissances croissantes de A par B à l'ordre $n - 1$.

$$\exists Q, R \in A[X] / \deg Q < n \text{ et } A = QB + X^n R \text{ et donc } \frac{A}{X^n B} = \frac{QB + X^n R}{X^n B} = \frac{Q}{X^n} + \frac{R}{B}$$

Exemple

On considère $\frac{X+1}{X^3(X^2+1)}$.

$$\begin{array}{r|l} 1+X & 1+X^2 \\ X-X^2 & \hline -X^2-X^3 & 1+X-X^2 \\ -X^3+X^4 & \end{array}$$

$$\text{Donc } \frac{X+1}{X^3(X^2+1)} = \frac{(1+X-X^2)(X^2+1)+X^3(X-1)}{X^3(X^2+1)} = \frac{1+X-X^2}{X^3} + \frac{X-1}{X^2+1}$$

Définition

On appelle élément simple une fraction de la forme :

- soit un polynôme c'est-à-dire une fraction de la forme $\frac{P}{1}$.
- soit une fraction de la forme $\frac{P}{Q^n}$ où $n \in \mathbb{N}^*$, $\deg P < \deg Q$ et Q est un polynôme irréductible.

Remarques

- Les éléments simples de $\mathbb{C}(X)$ sont de la forme :
 - soit un polynôme c'est-à-dire une fraction de la forme $\frac{P}{1}$.
 - soit $\frac{a}{(X-c)^n}$ où $a, c \in \mathbb{C}$ et $n \in \mathbb{N}^*$.
- Les éléments simples de $\mathbb{R}(X)$ sont de la forme :
 - soit un polynôme c'est-à-dire une fraction de la forme $\frac{P}{1}$.
 - soit $\frac{a}{(X-c)^n}$ où $a, c \in \mathbb{R}$ et $n \in \mathbb{N}^*$.
 - soit $\frac{aX+b}{Q^n}$ où $a, b \in \mathbb{R}$, $n \in \mathbb{N}^*$ et Q est un polynôme de degré 2 de discriminant < 0 .

Propriété

Soit une fraction pure de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ qui admet un représentant de la forme $\frac{A}{B^n}$ où $n \in \mathbb{N}^*$ et B est un polynôme irréductible (de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$).

Alors elle se décompose de manière unique en la forme suivante :

$$\frac{A}{B^n} = \frac{A_1}{B} + \frac{A_2}{B^2} + \dots + \frac{A_n}{B^n} \quad \text{où chacune de ces fractions est un élément simple.}$$

Remarque

$$\frac{A}{B^n} \text{ fraction pure} \Leftrightarrow \deg A < \deg B^n \Leftrightarrow \deg A < n \deg B.$$

$$\frac{A_i}{B^i} \text{ élément simple} \Rightarrow \deg A_i < \deg B.$$

Démonstration

Par récurrence descendante sur n .

On effectue la division euclidienne de A par B .

$\exists Q, R \in A[X] / \deg R < \deg B$ et $A = QB + R$.

et donc $\frac{A}{B^n} = \frac{BQ + R}{B^n} = \frac{Q}{B^{n-1}} + \frac{R}{B^n}$ on a bien $\frac{R}{B^n}$ élément simple.

Cas particulier

Si la fraction pure est de la forme $\frac{A}{(X-c)^p}$ où $c \in \mathbb{R}$ ou \mathbb{C} , on obtient la décomposition en utilisant la formule de Taylor.

On pose $n = \deg A$. Puisque la fraction est pure $n < p$.

$$\text{On a } A = A(c) + A'(c) \frac{(X-c)}{1!} + A^{(2)}(c) \frac{(X-c)^2}{2!} + \dots + A^{(n)}(c) \frac{(X-c)^n}{n!}.$$

$$\begin{aligned} \text{Et donc } \frac{A}{(X-c)^p} &= \frac{A(c)}{(X-c)^p} + \frac{A'(c)(X-c)}{1!(X-c)^p} + \frac{A^{(2)}(c)(X-c)^2}{2!(X-c)^p} + \dots + \frac{A^{(n)}(c)(X-c)^n}{n!(X-c)^p} \\ &= \frac{A(c)}{(X-c)^p} + \frac{A'(c)}{1!(X-c)^{p-1}} + \frac{A^{(2)}(c)}{2!(X-c)^{p-2}} + \dots + \frac{A^{(n)}(c)}{n!(X-c)^{p-n}}. \end{aligned}$$

Propriété

Toute fraction de $\mathbb{R}(X)$ ou de $\mathbb{C}(X)$ admet une décomposition unique en somme d'éléments simples.

Propriété

Soient A et B deux polynômes non nuls.

Soit F la fraction rationnelle $\frac{A}{B}$.

Il existe un unique couple (Q, R) de polynômes avec $\deg R < \deg B$ tels que :

$$F = Q + \frac{R}{B}.$$

B peut s'écrire sous la forme :

$$B = c U_1^{\alpha_1} U_2^{\alpha_2} \dots U_p^{\alpha_p} D_1^{\beta_1} D_2^{\beta_2} \dots D_m^{\beta_m}$$

où c est un réel

Les U_i sont des polynômes de degré 1 sous la forme $X - a_i$

Les D_j sont des polynômes de degré 2 sous la forme $X^2 + c_j X + d_j$

Les α_i et β_j sont des entiers représentant l'ordre de multiplicité des U_i et D_j .

On admet que l'on peut mettre la fraction $\frac{R}{B}$ sous la forme d'une somme de fractions des formes suivantes

$$\frac{R}{B} = \frac{\gamma_{1,1}}{(x-a_1)} + \frac{\gamma_{1,2}}{(x-a_1)^2} + \dots + \frac{\gamma_{1,\alpha_1}}{(x-a_1)^{\alpha_1}} + \frac{\gamma_{2,1}}{(x-a_2)} + \dots + \frac{\gamma_{2,\alpha_2}}{(x-a_2)^{\alpha_2}} + \dots + \frac{\gamma_{p,1}}{(x-a_p)} + \dots + \frac{\gamma_{p,\alpha_p}}{(x-a_p)^{\alpha_p}}$$

$$+ \frac{\delta_{1,1}x + \zeta_{1,1}}{(X^2 + c_1X + d_1)} + \dots + \frac{\delta_{1,\beta_1}x + \zeta_{1,\beta_1}}{(X^2 + c_1X + d_1)^{\beta_1}} + \dots + \frac{\delta_{m,1}x + \zeta_{m,1}}{(X^2 + c_mX + d_m)} + \dots + \frac{\delta_{m,\beta_m}x + \zeta_{m,\beta_m}}{(X^2 + c_mX + d_m)^{\beta_m}}$$

Cette transformation s'appelle la décomposition en éléments simples de F .

Exemple

$$\frac{X^6}{(X^2 + 1)^2(X + 1)^2} = 1 - \frac{X + \frac{1}{4}}{X^2 + 1} + \frac{\frac{1}{2}X}{(X^2 + 1)^2} - \frac{1}{X + 1} + \frac{\frac{1}{4}}{(X + 1)^2}.$$