Agrégation interne

Polynômes - Fractions rationnelles

UNIVERSITÉ de Cergy-Pontoise

Première partie

Polyômes

$\mathbb{K}$ est un corps commutatif, généralement $\mathbb{R}$ ou $\mathbb{C}$. On se placera aussi parfois sur $\mathbb{Z}/p\mathbb{Z}$ avec p premier et de nombreuses propriétés restent vraies car on a un anneau intègre.

1 Définitions - Premières propriétés

1.1 Définitions

Définition 1 On appelle polynôme à une indéterminée, à coefficients dans $\mathbb{K}$, toute suite $(a_0, a_1, \ldots)$ d'éléments de $\mathbb{K}$, nulle à partir d'une certain rang. Le coefficient de rang 0 ; a_0 est appelé coefficient constant. Le polynôme nul est la suite nulle et est noté 0. Deux polynômes sont égaux si tous leurs coefficients de même rang sont égaux.

Définition 2 Soient $P = (a_0, a_1, \ldots,)$ et $Q = (b_0, b_1, \ldots,)$ deux polynômes, et $\lambda \in \mathbb{K}$. On définit les opérations suivantes :

1. Addition : $P + Q = (a_0 + b_0, a_1 + b_1, \ldots)$
2. Produit par un scalaire : $\lambda P = (\lambda a_0, \lambda a_1, \ldots)$
3. Produit : $pq = (c_1, c_1, \ldots)$ avec $\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

On remarque que ces définitions permettent bien de définir des polynômes.

Théorème 1
1. L'ensemble des polynômes à coefficients dans $\mathbb{K}$, muni de l'addition et du produit par un scalaire, est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$, espace vectoriel des suites de $\mathbb{K}$.
2. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ muni de l'addition et de la multiplication est un anneau commutatif.

1.2 Notation

Notons $X = (0, 1, 0, \ldots)$. En notant $(P)_i$ le coefficient de rang i, on obtient pour tout $n \geq 1$:

$$X^n = (0, 0, \ldots, 1, 0 \ldots) \text{ avec } (X^n)_i = \delta_{i,n}$$

Par convention $X^0 = (1, 0, 0, \ldots)$. On peut donc écrire un polynôme sous la forme :

$$P = (a_0, a_1, \ldots, a_n, 0, \ldots) = \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{+\infty} a_k X^k$$

L'anneau des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

1.3 Exemples

— Pour tout entier n, on a $(X + a)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} X^k$. L'anneau $\mathbb{K}[X]$ est commutatif, donc la formule du binôme s'applique. Dans le cas où $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ avec p premier, on a $(X+a)^p = X^p + a^p$.
— Pour tout $a \in \mathbb{K}$ et tout entier n, on a : $(X - a) \sum_{k=0}^{n} a^k X^{n-k} = X^{n+1} - a^{n+1}$.

— Application :

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}3^kX^k(1-X)^{3n-2k} &= (1-X)^n\sum_{k=0}^{n}\binom{n}{k}3^kX^k(1-X)^{2n-2k}\\ &= (1-X)^n\sum_{k=0}^{n}\binom{n}{k}3^kX^k((1-X)^2)^{n-k}\\ &= (1-X)^n(3X+(1-X)^2)^n = (1-X)^n(X^2+X+1)^n = (1-X^3)^n\end{aligned}$$

1.4 Degré d'un polynôme

Définition 3 Soit $P=\sum_{k=0}^{+\infty}a_kX^k$ un élément de $\mathbb{K}[X]$. Si $P\neq 0$, on appelle degré de P, et on note $\deg P$ le plus grand entier n tel que $a_n\neq 0$. Si $P=0$, on pose : $\deg P=-\infty$.
Si $\deg P$ est un entier n, le coefficient a_n est appelé coefficient dominant de P. De plus, si $a_n=1$, le polynôme P est dit unitaire.

Proposition 1 Soient P et Q deux polynômes de $\mathbb{K}[X]$. On a :

1. $\deg(P+Q)\leq \deg P+\deg Q$ avec égalité lorsque $\deg P\neq \deg Q$.
2. $\deg(PQ)=\deg P+\deg Q$.

Corollaire 1 L'ensemble $\mathbb{K}_n[X]$ des polynômes de degré inférieur ou égal à n est un sous-espace vectoriel de $\mathbb{K}[X]$ et $\dim\mathbb{K}_n[X]=n+1$. La famille $\mathcal{B}=(1,X,\ldots,X^n)$ est une base de $\mathbb{K}_n[X]$, appelée base canonique.

Définition 4 On appelle valuation d'un polynôme P, l'indice du premier terme non nul de P. On la note $\mathrm{Val}(P)$. Par convention, $\mathrm{Val}(0)=+\infty$. On a toujours $\deg P\geq \mathrm{Val}(P)$ sauf si $P=0$ et $\mathrm{Val}(PQ)=\mathrm{Val}(P)+\mathrm{Val}(Q)$.

Théorème 2 L'anneau $\mathbb{K}(X]$ est intègre, i.e.

$$\forall(P,Q)\in(\mathbb{K}[X])^2,\ PQ=0\Rightarrow(P=0 \text{ ou } Q=0)$$

Corollaire 2 Les polynômes inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Corollaire 3 Dans l'anneau $\mathbb{K}[X]$, tout polynôme non nul est régulier : si $PQ=PR$ et $P\neq 0$, alors $Q=R$.

1.5 Composition de polynômes

Définition 5 Soient $P=\sum_{k=0}^{n}a_kX^k$ un polynôme de degré n de $\mathbb{K}[X]$ et $Q\in\mathbb{K}[X]$. Le polynôme composé $P\circ Q=P(Q)$ est défini par :

$$P\circ Q=\sum_{k=0}^{n}a_kQ^k=\sum_{k=0}^{+\infty}a_kQ^k$$

Proposition 2

1. Si P ou Q est nul, alors $P\circ Q$ est le polynôme nul. Si P et Q sont non nuls, alors on a : $\deg(P\circ Q)=\deg P\times\deg Q$.
2. Soient λ et μ deux scalaires, P et Q deux polynômes, on a :

$$\begin{aligned}(\lambda P+\mu Q)(R) &= \lambda P(R)+\mu Q(R)\\ (P\times Q)(R) &= P(R)\times Q(R)\end{aligned}$$

Exemple 1 : Considérons l'application φ de $\mathbb{K}_n[X]$ dans $\mathbb{K}_n[X]$ définie par : $\varphi(P)=P(X+1)+P(X)$. Alors φ est un automorphisme de l'espace vectoriel $\mathbb{K}_n[X]$.

— On vérifie que $\varphi(P)$ est bien un élément de $\mathbb{K}_n[X]$. En effet, $\deg(P(X+1)) = \deg X \times \deg P = \deg P \leq n$.
— Pour P, Q dans $\mathbb{K}_n[X]$ et $\lambda \in \mathbb{K}$, on a :

$$\begin{aligned}\varphi(\lambda P + Q) &= (\lambda P + Q)(X+1) + (\lambda P + Q)(X) \\ &= \lambda P(X+1) + Q(X+1) + \lambda P(X) + Q(X) = \lambda\varphi(P) + \varphi(Q)\end{aligned}$$

φ est donc un endomorphisme de $\mathbb{K}_n[X]$.
— Soit $P \in \ker(\varphi)$. Si $P \neq 0$, les coefficients dominants de P et $P(X+1)$ sont égaux. Donc $P(X+1) = -P(X)$ donne une contradiction car le coefficient dominant serait nul. On en déduit que φ est injectif. En utilisant le théorème du rang, on obtient que φ est bien, un automorphisme de $\mathbb{K}_n[X]$.

2 Divisibilité dans $\mathbb{K}[X]$

Dans cette section, on retrouve les résultats obtenus dans $\mathbb{Z}$ pour $\mathbb{K} = \mathbb{R}, \mathbb{C}$, ou $\mathbb{Z}/pZ$ (p premier), puisque qu'alors $\mathbb{K}[X]$ est anneau intègre (comme $\mathbb{Z}$).

2.1 Définition - Propriétés

Définition 6 Un polynôme P est dit associé à un polynôme Q s'il existe un scalaire λ tel que $P = \lambda Q$.

Remarque 1
— Tout polynôme est associé à un unique polynôme unitaire.
— Deux polynômes associés de même coefficient dominant sont égaux.

Définition 7 Soient A et B deux polynômes de $\mathbb{K}[X]$. On dit que A divise B s'il existe un polynôme $C \in \mathbb{K}[X]$ tel que $B = AC$ et on note $A|B$.

Exemple 2 : Le polynôme $X^2 + X + 1$ divise le polynôme $X^3 - 1$.

Proposition 3 Soient A, B, C, D des polynômes de $\mathbb{K}[X]$. On a les propriétés suivantes :

1. Si $A|B$ et $B|C$, alors $A|C$.
2. Si $A|B$ et $B|A$, alors A et B sont associés.
3. Si $A|B$ et $B \neq 0$, alors $\deg A \leq \deg B$.
4. Si $A|B$ et $\deg A = \deg B$, alors A et B sont associés.
5. Si $A|B$ et $A|C$, alors $A|B + C$.
6. Si $A|B$ et $C|D$, alors $AC|BD$.
7. Si $A|B$ alors, pour tout $n \in \mathbb{N}$, $A^n|B^n$.

Exercice 1 Soit $P \in \mathbb{K}[X]$, montrer que $P(X) - X|P(P(X)) - P(X)$.

2.2 Division euclidienne

Théorème 3 Soient A et B deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ tels que : $A = BQ + R$ avec $\deg R < \deg B$.
Q est le quotient et R est le reste de la division euclidienne de A par B.

Exemple 3 : Déterminer les réels p et q tels que $Q = X^2 + 3X - 1$ divise $P = X^3 + pX + q$.

2.3 Idéaux de $\mathbb{K}[X]$

Dans cette sous-section, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

Définition 8 On appelle idéal de l'anneau commutatif $(\mathbb{K}[X], +, \times)$, tout sous-groupe I de $(\mathbb{K}[X], +)$ tel que $(A, P) \in \mathbb{K}[X] \times I \Rightarrow A.P \in I$.

Théorème 4 Soit I un idéal de $\mathbb{K}[X]$. Alors soit $I = \{0\}$, soit il existe un polynôme P tel que $I = (P) = P\mathbb{K}[X]$. Lorsque $I \neq \{0\}$, P est unique si P est unitaire. $\mathbb{K}[X]$ est un anneau commutatif principal.

3 Fonction polynomiale

Définition 9 Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré $n \in \mathbb{N}$.

- Pour $x \in \mathbb{K}$, on définit la valeur de P en x par $P(x) = \sum_{k=0}^{n} a_k x_k$.
- La fonction $\tilde{P}$, appelée fonction polynomiale associée au polynôme P, est définie par : $x \to \tilde{P}(x) = P(x)$. $\tilde{P}$ est une fonction de $\mathbb{K}$ dans $\mathbb{K}$.
- Lorsque $x \in \mathcal{D} \subset \mathbb{K}$, on parle aussi de fonction polynomiale associée en précisant qu'elle est restreinte à $\mathcal{D}$.

Remarque 2 Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, on peut assimiler un polynôme et la fonction de $\mathbb{K}$ dans $\mathbb{K}$ qui lui correspond. Sur $\mathbb{Z}/p\mathbb{Z}$, il faut faire attention. Par exemple, pour tout a, on a $a^p - a = 0$ par le petit théorème de Fermat. Donc la fonction correspondant au polynôme $X^p - X$ est la fonction nulle. Cependant, le polynôme $X^p - X$ n'est pas nul : un polynôme est défini par ses coefficients.

Proposition 4 Soient P et Q deux polynômes de $\mathbb{K}[X]$, λ et μ deux scalaires de $\mathbb{K}$. On a :

1. $\widetilde{(\lambda P + \mu Q)} = \lambda \tilde{P} + \mu \tilde{Q}$
2. $\widetilde{(P \times Q)} = \tilde{P}\tilde{Q}$
3. Si $P = 1$, alors $\tilde{P} = \mathrm{Id}_{\mathbb{K}}$

L'application $P \mapsto \tilde{P}$ est un morphisme injectif d'anneaux.

4 Racines d'un polynôme

4.1 Racines

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

Définition 10 Un élément $x \in \mathbb{K}$ est racine de P si $P(x) = 0$.

Exemple 4 : Soit $P = X^2 + X + 1$. Alors P n'a aucune racine dans $\mathbb{R}$ et a deux racines dans $\mathbb{C}$: j et j^2.

Théorème 5 Soit $x \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Il existe un unique polynôme Q tel que $P = (X - x)Q + P(x)$.

Corollaire 4 Un élément $x \in \mathbb{K}$ est racine de P si, et seulement si, $X - x$ divise P.

Proposition 5 Si $P \in \mathbb{R}[X]$ et si $x \in \mathbb{C}$ est racine de P, alors $\bar{x}$ est aussi racine de P.

Algorithme de Hörner Cette méthode permet de calculer la valeur d'un polynôme P en $x = a$ et fournit les coefficient du polynôme Q tel que $P = (X - a)Q + P(a)$. Soit P un polynôme de degré supérieur ou égal à 1 :

$$P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

On peut aussi écrire P de la façon suivante :

$$P = (((a_x X + a_{n-1}) + a_{n-2})X + \ldots)X + a_0$$

L'algorithme s'écrit alors :

- $P_0 = a_n$
- Pour i allant de 1 à n, faire $P_i = P_{i-1} \times a + a_{n-i}$
- $P(a) = P_n$

Si $Q = b_0 + \ldots + b_{n-1}X^{n-1}$, on montre par récurrence, en posant $P_{-1} = 0$, que $b_{n-i} = ap_{i-1} + a_{n-i} = P_i$.

Corollaire 5 Si $x_1, x_2, \ldots x_o$ sont p racines distinctes de P, alors le polynôme $\prod_{k=1}^{p}(X - x_k)$ divise P.

Corollaire 6 Un polynôme non nul de degré n admet au plus n racines distinctes. De plus, si P est un polynôme de degré n et admet n racines distinctes, alors il existe une constante $\lambda \in \mathbb{K}^*$ telle que $P = \lambda \prod_{k=1}^{n}(X - x_k)$.

Conséquences :

1. Si un polynôme de degré admet au moins $n + 1$ racines, alors $P = 0$.
2. Si deux polynômes P et Q, de degré n, coïncident en $n + 1$ valeurs distinctes, alors ils sont égaux.

Exemple 5 : Considérons l'endomorphisme φ de $\mathbb{K}_n[X]$ défini par $\varphi(P) = P(X + 1) - P(X)$. Déterminons son noyau. Soit $P \in \ker(\varphi)$. Posons $Q(X) = P(X) - P(0)$. Puisque $P \in \ker(\varphi)$, on obtient $Q(X + 1) = Q(X)$. On montre ensuite par récurrence : $\forall n \in \mathbb{N},\ Q(n) = Q(0) = 0$. Donc Q est le polynôme nul et P est le polynôme constant $P(0)$. On a obtenu : $\ker(\varphi) = \mathbb{K}$.

4.2 Racines multiples

Définition 11 Soient P un polynôme de $\mathbb{K}[X]$ et $x \in \mathbb{K}$, racine de P. On dit que x est racine d'ordre $p \in \mathbb{N}^*$ si $(X - x)^p$ divise P et $(X - x)^{p+1}$ ne divise pas P.

Théorème 6 Soient x une racine d'ordre au moins p de $P \in \mathbb{K}[X]$, $P \neq 0$ et $Q \in \mathbb{K}[X]$ tel que $P = (X - x)^p Q$. Alors x est une racine d'ordre p de P si, et seulement si, $Q(x) \neq 0$.

Théorème 7 Si $x_1, x_2, \ldots, x_n$ sont des racines de P de multiplicité respectives au moins égales à $r_1, r_2, \ldots, r_n$, alors le polynôme $\prod_{k=1}^{n}(X - x_k)^{r_k}$ divise P.

4.3 Relations entre coefficients et racines

Définition 12 Un polynôme P non nuls de degré $n \geq 1$ est scindé sur $\mathbb{K}$ s'il peut s'écrire sous la forme : $P = \lambda \prod_{k=1}^{n}(X - x_k)$, avec $\lambda, x_1, \ldots, x_n$ éléments de $\mathbb{K}$, les x_k étant distincts ou non.

Définition 13 On appelle fonctions symétriques élémentaires des racines $x_1, \ldots, x_n$ d'un polynôme

scindé de degré n, les quantités suivantes :

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{n} x_i \\
\sigma_2 &= \sum_{i<j} x_i x_j \\
\sigma_k &= \sum_{1\leq i_1<\ldots<i_k\leq n} x_{i_1}\ldots x_{i_k} \\
\sigma_n &= \prod_{i=1}^{n} x_i
\end{aligned}$$

Exemple 6 : Soit $P = a_3X^3+a_2X^2+a_1X+a_0 = a_3(X-x_1)(X-x_2)(x-x_3)$ un polynôme scindé de degré 3. En développant P, on obtient : $P = a_3(X^3-(x_1+x_2+x_3)X^2+(x_1x_2+x_1x_3+x_2x_3)X-x_1x_2x_3)$. Le théorème d'égalité des polynômes donne alors :

$$\begin{aligned}
\sigma_1 = x_1+x_2+x_3 &= -\frac{a_2}{a_3} \\
\sigma_2 = x_1x_2+x_1x_3+x_2x_3 &= \frac{a_1}{a_3} \\
\sigma_3 = x_1x_2x_3 &= -\frac{a_0}{a_3}
\end{aligned}$$

On a la généralisation suivante :

Théorème 8 Pour tout polynôme $P = \sum_{k=0}^{n} a_{n-k}X^{n-k} \in \mathbb{K}[X]$ scindé de degré n, on a :

$$P = a_n\left(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} + \ldots + (-1)^k\sigma_kX^{n-k} + \ldots + (-1)^n\sigma_n\right)$$

De plus, pour tout entier $k, 1 \leq k \leq n$, on a : $\sigma_k = (-1)^k\frac{a_{n-k}}{a_n}$.

5 Dérivation

5.1 Définition - Propriétés

Définition 14 Soit $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{K}[X]$, un polynôme de degré n. On appelle polynôme dérivé de P, le polynôme P défini par : $P' = \sum_{k=1}^{n} ka_kX^{k-1}$.

Remarque 3 Lorsque $\mathbb{K} = \mathbb{R}$, la fonction polynomiale associée à P' est exactement la dérivée de la fonction polynomiale associée à P.

Théorème 9 Soit $P \in \mathbb{K}[X]$. On a :
- Si $\deg P \geq 1$, alors $\deg P' = \deg P - 1$.
- Le polynôme P est constant si, et seulement si, $P' = 0$.

5.2 Dérivation et Opérations

Théorème 10 Soient P et Q dans $\mathbb{K}[X]$, λ et μ deux scalaires. On a
- $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
- $(PQ)' = P'Q + PQ'$.
- Pour tout entier $n \geq 1$, $(P^n)' = nP^{n-1}P'$

5.3 Formule de Taylor

Définition 15 Pour tout entier $r \in \mathbb{N}$, on appelle polynôme dérivé d'ordre r, le polynôme défini de la manière suivante :

$$P^{(0)} = P, \text{ et } \forall r \geq 0, P^{(r+1)} = \left(P^{(r)}\right)'$$

Remarque 4
— Pour $r \in \mathbb{N}$, l'application $P \mapsto P^{(r)}$ est un endomorphisme de $\mathbb{K}[X]$.
— Si $\deg P < r$ alors, $P^{(r)} = 0$ et si $\deg P \geq r$, alors $\deg P^{(r)} = \deg P - r$.

Exemple 7 : Pour $n \in \mathbb{N}$ et $p \in \mathbb{N}$, $0 \leq p \leq n$, on a :

$$(X^n)^{(p)} = n(n-1)\dots(n-p+1)X^{n-p} = \frac{n!}{(n-p)!}X^{n-p}$$

Théorème 11 Formule de Leibnitz
Soient P et Q deux polynômes. Alors $(PQ)^{(r)} = \sum_{k=0}^{n} \binom{r}{k} P^{(k)} Q^{(n-k)}$.

Exercice 2 Déterminer de deux manières le coefficient de $P^{(n)}$ pour $P = (X^2-1)^n$ et en déduit la valeur de $\sum_{k=0}^{n} \binom{n}{k}^2$.

Théorème 12 Formule de Taylor
Pour tout polynôme $P \in \mathbb{K}[X]$ de degré n et tout $a \in \mathbb{K}$, on a :

$$P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(X)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{P^{(k)}(X)}{k!}(X-a)^k$$

5.4 Caractérisation de l'ordre d'une racine

Théorème 13 Soient P un élément de $\mathbb{K}[X]$, a un scalaire et $r \in \mathbb{N}^*$. Les conditions suivantes sont équivalentes :

1. a est racine d'ordre r de P.
2. Pour tout k, $0 \leq k \leq r-1$, a est racine de $P^{(k)}$ et non racine de $P^{(r)}$.

6 Arithmétiques dans $\mathbb{K}[X]$

Les démarches sont analogues à celle étudiées dans l'année commutatif $\mathbb{Z}$.

6.1 PGCD

Théorème 14 Soient A et B deux polynômes tels que $B \neq 0$. Si P et R sont le quotient et le reste de la division euclidienne de A par B, alors les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R.

L'ensemble des diviseurs communs à A et B est non vide. En effet, il contient au moins les polynômes constants. Donc l'ensemble D_C des degrés de ces diviseurs communs est non vide. De plus, l'ensemble D_C est majoré par $\max\{\deg A, \deg B\}$. Par conséquent, D_C est une partie non vide majorée de $\mathbb{N}$ et admet donc un élément maximal $d \geq 0$.

Définition 16 Soient A et B deux polynômes non tous nuls. Un PGCD de A et B est un diviseur commun de degré maximal.

Théorème 15 Soient A et B deux polynômes non tous nuls. L'ensemble des polynômes $AU + BV$ où U et V parcourent $\mathbb{K}[X]$ est l'ensemble de tous les multiples d'un polynôme D.

Théorème 16 Soient A et B deux polynômes non tous nuls. Alors

1. Il existe un élément $D \in \mathbb{K}[X]$ possédant la propriété suivante : les diviseurs communs à A et B sont exactement les diviseurs de D.
2. D est unique à une constante non nulle près.
3. Le degré de D majore le degré de tout diviseur commun à A et B.
4. Il existe U et V dans $\mathbb{K}[X]$ tels que $AU+BV = D$. Cette relation est appelée relation de Bezout et les coefficients U et V sont les coefficients de Bezout.

Définition 17 Le PGCD unitaire de A et B est noté $A \wedge B$.

6.2 Algorithme d'Euclide

Cet algorithme fournit une méthode pratique pour calculer un PGCD de deux polynômes A et B non tous nuls.

— Si $B = 0$, alors A est un PGCD de A et B.
— Supposons A et B sont non nuls, et $\deg A \geq \deg B$. Par la division euclidienne de A par B, on a $A = BQ_0 + R_0$ avec $\deg R_0 < \deg B$. De plus, les diviseurs communs à A et B sont les diviseurs communs à B et R_0. On est donc ramené à chercher un PGCD de B et R_0.
— Si $R_0 = 0$, alors B est un PGCD de B et R_0. Si $R_0 \neq 0$, on a alors $B = Q_1R_0 + R_1$ avec $\deg R_1 < \deg R_0$. Les diviseurs communs à B et R_0 sont exactement les diviseurs communs à R_0 et R_1. Donc un PGCD de B et R_0 est un PGCD de R_0 et R_1.
— Les degrés de $B, R_0, \ldots, R_1$ sont strictement décroissants. Finalement, avec au plus $\deg B$ division, on obtient $R_{n-1} = Q_{n+1}R_n + R_{n+1}$ avec $R_{n+1} = 0$.

Finalement un PGCD de A et B est PGCD de R_n et 0, c'est-à-dire R_n qui est le dernier reste non nul.

6.2.1 Coefficients de Bezout

Si on note R_p le dernier reste non nul de l'algorithme d'Euclide. Pour tout entier $p \leq n$, il existe des polynômes U_p et V_p tels que $R_p = AU_p + BV_p$.

— La proposition est vraie pour $p = 0$. En effet, on a $R_0 = A - BQ_0$.
— Supposons la propriété vraie pour tout entier $k < p$ et démontrons la pour tout entier $k < P+1$. Par l'algorithme d'Euclide, pour tout entier $k \leq n$, on a :

$$R_{k-2} = Q_kR_{k-1} + R_k$$

Pour l'entier p, on a alors $R_p = R_{p-2} - Q_pR_{p-1}$. Par hypothèse de récurrence, on a

$$R_{p-2} = AU_{p-2} + BV_{p-2}$$
$$R_{p-1} = AU_{p-1} + BV_{p-1}$$

En remplaçant dans R_p, on obtient :

$$R_p = AU_p + BV_p \text{ avec } U_p = U_{p-2} - Q_pU_{p-1} \text{ et } V_p = V_{p-2} - Q_pV_{p-1}$$

— On obtient ensuite de proche en proche les coefficients de Bezout.

6.3 Plus petit commun multiple

L'ensemble des multiples communs aux deux polynômes non nuls A et B est non vide. Il contient au moins le polynôme AB. Donc l'ensemble M_C des degrés de ces multiples est non vide. De plus, M_C est minoré par $\min\{\deg A, \deg B\}$. M_C est une partie non vide minorée de $\mathbb{N}$ et admet donc un élément minimal $m \geq 0$.

Définition 18 Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. On appelle PPCM de A et B tout multiple commun de degré minimal.

Théorème 17 Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. L'ensemble des multiples de A et B est exactement l'ensemble des multiples d'un unique polynôme unitaire M. Le polynôme M est appelé PPCM de A et B et est noté $A \vee B$.

Corollaire 7 Soient A et B deux polynômes non nuls. Dire que $M = A \vee B$ revient à dire que

$$\forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P) \Leftrightarrow P|M$$

6.4 Polynômes premiers entre eux

Définition 19 Deux polynômes A et B sont premiers entre eux si $A \wedge B = 1$. Les seuls diviseurs communs de A et B sont les polynômes de degré 0.

Théorème 18 Théorème de Bezout
Les polynômes A et B sont premiers entre eux si, et seulement si,il existe U et V dans $\mathbb{K}[X]$ tels que $AU + BV = 1$.

Exemple 8 : Si a et b sont des scalaires distincts, les polynômes $A = X - a$ et $B = X - b$ sont premiers entre eux. En effet, on a $A - B = b - a$. On choisit alors $U = \frac{1}{b-a}$ et $V = \frac{-1}{b-a}$. On obtient alors $AU + BV = 1$. En général, si $AU + BV = k$ où k est un scalaire non nul, alors A et B sont premiers entre eux.

Corollaire 8
- Si $A \wedge B = 1$ et $A \wedge C = 1$ alors $A \wedge BC = 1$.
- Soit $n \in \mathbb{N}$, $n \geq 2$. Si pour tout i, $1 \leq i \leq n$, $A \wedge B_i = 1$, alors $A \wedge (B_1 \dots B_n) = 1$.
- Si $A \wedge B = 1$, alors pour tout entier $n \in \mathbb{N}^*$, et tout entier $m \in \mathbb{N}^*$, on a $A^n \wedge B^m = 1$.

Théorème 19 Théorème de Gauss
Soient A, B, C trois polynômes de $\mathbb{K}[X]$. Si $A \wedge B = 1$ et si $A|BC$ alors $A|C$.

Théorème 20 Soient A et B dans $\mathbb{K}[X]$. Si A et B sont premiers entre eux et si chacun divise un polynôme C, alors AB divise C.

Corollaire 9 Si des polynômes premiers entre eux divisent un polynôme C, alors leur produit divise C.

Théorème 21 Un produit de polynômes est premier avec un polynôme C si, et seulement si, chacun de ses facteurs est premier avec C.

7 Lien entre PGCD et PPCM

Proposition 6 Si A et B sont premiers entre eux, alors $A \vee B$ est associé à AB.

Corollaire 10 Soient A et B deux polynômes non nuls et unitaires, alors $AB = (A \wedge B) \cdot (A \vee B)$. S'ils ne sont pas unitaires, alors AB et $(A \wedge B) \cdot (A \vee B)$ sont associés.

8 Polynômes irréductibles

8.1 Définition - Propriétés

Définition 20 Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible si :
- $\deg P \geq 1$.
- Les seuls diviseurs de P sont les scalaires de $\mathbb{K}^*$ et les polynômes associés à P.

Exemple 9 : Le polynôme $P = X^2 + 1$ est irréductible dans $\mathbb{R}[X]$. Cependant, le polynôme $Q = (X^2 + 1)^2$ n'a pas de racine dans $\mathbb{R}$ mais n'est pas irréductible dans $\mathbb{R}$.

Théorème 22 Soit P un polynôme irréductible. Alors P est premier avec tous les polynômes qu'il ne divise pas.

Théorème 23 Soient P un polynôme irréductible et A et B dans $\mathbb{K}[X]$. Alors P divise AB si, et seulement si P divise l'un des facteurs.

8.2 Décomposition en facteurs irréductibles

Théorème 24 Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire non nul par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$.

Exemple 10 : Dans $\mathbb{K}[X]$, si A et B sont premiers entre eux, ils n'ont pas de facteurs communs irréductibles, il en est de même pour A^n et B^m avec n et m entiers naturels non nuls.

8.3 Application au PGCD et PPCM

Théorème 25 Soient A et B deux polynômes non nuls tels que

$$A = \lambda \prod_{i=1}^{k} P_i^{\alpha_i}, \text{ et } B = \mu \prod_{i=1}^{k} P_i^{\beta_i}$$

où $P_1, \ldots, P_k$ sont des polynômes irréductibles distincts deux à deux et $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$ sont des entiers naturels éventuellement nuls. On a :

1. $A|B$ si, et seulement si, $\forall i\, 1 \leq i \leq k,\ \alpha_i \leq \beta_i$.
2. $A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i, \beta_i)}$.
3. $A \vee B = \prod_{i=1}^{k} P_i^{\max(\alpha_i, \beta_i)}$.

9 Factorisation

9.1 Factorisation dans $\mathbb{C}[X]$

Définition 21 Un corps dans lequel tout polynôme irréductible est de degré 1 est dit algébriquement clos.

Théorème 26 Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$. Donc $\mathbb{C}$ est algébriquement clos.

Corollaire 11 Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

9.2 Factorisation dans $\mathbb{R}[X]$

Théorème 27 Les polynômes irréductibles de $\mathbb{R}[X]$ sont :
- Les polynômes de degré 1.
- Les polynômes de degré 2 à discriminant strictement négatif.

Théorème 28 Tout polynôme non nul P de $\mathbb{R}[X]$ peut se mettre sous la forme :

$$P = \lambda \prod_{k=1}^{p} (X - a_k)^{r_k} \prod_{k=1}^{q} (X^2 + b_k X + c_k)^{s_k}$$

où p et q sont des entiers naturels, λ est le réel égal au coefficient dominant de P, a_k, b_k, c_k sont des réels vérifiant $\forall k,\ 1 \leq k \leq q,\ b_k - 4a_k c_k < 0$ et r_k, s_k sont des entiers naturels non nuls.

Deuxième partie

Fractions rationnelles

10 Définitions - Propriétés

10.1 Défintions

Définition 22 On sait que $\mathbb{K}[X]$ est un anneau intègre. On construit donc de manière analogue à $\mathbb{Z}$ son corps des fractions rationnelles noté $\mathbb{K}(X)$. Les éléments de $\mathbb{K}(X)$ sont appelés fractions rationnelles en X à coefficients dans $\mathbb{K}$.

- Tout élément F de $\mathbb{K}(X)$ est de la forme $\frac{P}{Q}$ où P et Q sont des polynômes de $\mathbb{K}[X]$ et $Q \neq 0$. Le couple (P, Q) est un représentant de F.
- Pour $\frac{P}{Q}$ et $\frac{P_1}{Q_1}$, on a $\frac{P}{Q} = \frac{P_1}{Q_1} \Leftrightarrow PQ_1 = P_1Q$. On dit alors que les couples (P, Q) et (P_1, Q_1) sont des représentants de la même fraction rationnelle.

Théorème 29

1. $\mathbb{K}(X)$ muni de l'addition et de la multiplication par un scalaire de $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$. L'élément neutre de l'addition est la fraction $0 = \frac{0}{1}$.
2. $\mathbb{K}(X)$ muni de l'addition et du produit de fractions est un corps commutations d'élément neutre multiplicatif $1 = \frac{1}{1}$.

10.2 Représentants irréductibles

Théorème 30 Soit $F \in \mathbb{K}(X)$. Il existe un unique couple (A, B) de polynômes de $\mathbb{K}[X]$, premiers entre eux, avec B unitaire, tels que $F = \frac{P}{Q}$.

Définition 23 La fraction définie au théorème précédent est appelée représentant irréductible unitaire de F. Si B n'est pas unitaire, on parle de représentant irréductible de F.

10.3 Dérivation

Lemme 1 Soit F une fraction rationnelle de $\mathbb{K}(X)$ représentée par les couples (P, Q) et (R, S). On a : $\frac{P'Q-PQ'}{Q^2} = \frac{R'S-RS'}{S^2}$

Définition 24 Pour toute fraction rationnelle irréductible $F = \frac{P}{Q}$, on appelle fraction dérivée, la fraction rationnelle $F' = \frac{P'Q-PQ'}{Q^2}$.

10.4 Fonction rationnelle

Définition 25 Soit $F \in \mathbb{K}(X)$ de représentant irréductible $\frac{P}{Q}$.

- On appelle racine de F toute racine de P.
- On appelle pôle de F toute racine de Q.

Exemple 11 : Soit $F = \frac{X^3-1}{X^2-1} \in \mathbb{R}(X)$. Pour déterminer les racines et les pôles, il faut d'abord déterminer un représentant irréductible de F. On a $F = \frac{X^2+X+1}{X+1}$. On a donc un seul pôle et aucune racine dans $\mathbb{R}$.

Définition 26 Soit $F = \frac{P}{Q}$ une fraction rationnelle réduite. Soit E l'ensemble $\mathbb{K}$ privé des pôles de F. Pour tout $a \in E$, on définit $F(a) = \frac{P(a)}{Q(a)}$. La fonction définie sur E à valeurs dans $\mathbb{K}$ par $x \mapsto F(x)$ est appelée fonction rationnelle associée à la fraction rationnelle F.

11 Décomposition d'une fraction rationnelle

Définition 27 Soit $F = \frac{P}{Q}$ une fraction rationnelle. La quantité $\deg P - \deg Q \in \mathbb{Z} \cup \{-\inf\}$ ne dépend pas du représentant de F. On l'appelle degré de F et on le note $\deg F$.

Théorème 31 Toute fraction rationnelle $F \in \mathbb{K}(X)$ s'écrit de manière unique $F = E + S$ où E est un polynôme de $\mathbb{K}[X]$ appelé partie entière de F et S est une fraction rationnelle de degré strictement négatif.

Proposition 7 La partie entière d'une fraction rationnelle $\frac{P}{Q}$ s'obtient pas la division euclidienne de P par Q. Si $\deg F < 0$, alors sa partie entière est nulle. Si $\deg F = 0$, alors sa partie entière est le polynôme constant égal au rapport des coefficients dominants de P et Q.

Définition 28 On appelle élément simple de $\mathbb{K}(X)$:
- Tout polynôme de $\mathbb{K}[X]$.
- Tout fraction rationnelle $\frac{P}{Q^\alpha}$ où Q est un polynôme irréductible de $\mathbb{K}[X]$, P est un polynôme de $\mathbb{K}[X]$ tel que $\deg P < \deg Q$ et $\alpha \in \mathbb{N}^*$.

Une fraction rationnelle est décomposée en éléments simples lorsqu'elle s'écrit sous la forme :

$$F = E + \sum_{Q \text{ irductible}} \sum_{\alpha \in \mathbb{N}^*} \frac{P}{Q^\alpha}$$

où $E \in \mathbb{K}[X]$.

Exemple 12 :
1. $F = X^2 - 1 + \frac{1}{X} - \frac{2}{X^3} + \frac{1}{(X+1)^2}$ est une décomposition en éléments simples dans $\mathbb{R}(X)$ mais aussi dans $\mathbb{C}(X)$.
2. $F = X + 1 + \frac{X-2}{X^2-X+1}$ est une décomposition en éléments simples dans $\mathbb{R}(X)$ mais pas dans $\mathbb{C}(X)$ car $X^2 - X + 1$ est irréductible dans $\mathbb{R}(X)$ mais pas dans $\mathbb{C}(X)$.

Théorème 32 Toute fraction rationnelle de $\mathbb{K}(X)$ s'écrit de manière unique sous la forme décomposée en éléments simples.

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

Théorème 33 Soit F une fraction rationnelle de $\mathbb{C}(X$ dont les pôles sont les complexes $a_1, \ldots, a_n$ deux à deux distincts et de multiplicités respectives $r_1, \ldots, r_n$. Il existe un unique polynôme $E \in \mathbb{C}[X]$ et une unique famille de scalaire $\lambda_{i,j 1 \leq i \leq n,\, 1 \leq j \leq r_i}$ tels que :

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X - a_i)^j} \right)$$

La quantité $\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X-a_i)^j}$ s'appelle la partie polaire de F relative au pôle a_i.

Mise en pratique

1. Soit F une fraction rationnelle admettant a comme pôle d'ordre 1 : $F = \frac{P}{Q} = \frac{P}{(X-a)Q_1}$. où $Q_1(a) \neq 0$. Il existe alors un scalaire λ_1 et une fraction rationnelle F_1 n'admettant pas a pour pôle tels que $F = \frac{\lambda_1}{X-a} + F_1$. En multipliant par $X - a$, on obtient : $\frac{P}{Q_1} = \lambda_1 + (X - a)F_1$. En évaluant en a, on a : $\lambda_1 = \frac{P(a)}{Q_1(a)}$. Puisque $Q' = Q_1 + (X - a)Q_1'$, on obtient : $\lambda_1 = \frac{P(a)}{Q_1(a)} = \frac{P(a)}{Q'(a)}$.
2. Si a est un pôle d'ordre n de F, alors $F = \frac{P}{(X-a)^n Q_n}$ avec $Q_n(a) \neq 0$. La partie polaire de F relative au pôle $a$est donnée par $\sum_{k=1}^{n} \frac{\lambda_k}{(X-a)^k}$ avec $\lambda_n = \frac{P(a)}{Q_n(a)}$. En utilisant la formule de Taylor, on a $Q_n(a) = \frac{Q^{(n)}(a)}{n!}$. Pour obtenir λ_{n-1}, on va soustraire $\frac{\lambda_n}{(X-a)^n}$ pour se ramener à une fraction rationnelle ayant un pôle d'ordre $n - 1$ et on calcule alors λ_{n-1} et ainsi de suite.

3. Les coefficients $\lambda_{i,j}$ lorsque la multiplicité est strictement supérieure à 1 peuvent aussi se calculer par le méthode de changement de variable $t = x - a_i$. On se ramène à un pôle en $t = 0$. Pour calculer les coefficients associés à ce pôle, on fait la division suivant les puissances croissantes de t du numérateur à l'ordre $r_i - 1$, c'est-à-dire que l'on s'arrête lorsque le reste ne contient que des termes de degré supérieur où égal à r_i de façon à pouvoir mettre en facteur t^{r_i}. Le quotient donne alors tous les coefficients associés au pôle a_i.

13 Décomposition en éléments simples dans $\mathbb{R}[X]$

Théorème 34 Soit $F \in \mathbb{R}(X)$ une fraction rationnelle et $\frac{P}{Q}$ sa forme irréductible unitaire. Soit

$$Q = \prod_{k=1}^{p} (X - a_k)^{r_k} \prod_{k=1}^{q} (X^2 + \beta_k X + \gamma_k)^{s_k}$$

la factorisation de Q dans $\mathbb{R}[X]$.
Il existe un unique polynôme $E \in \mathbb{R}[X]$, et des réels $a_{i,j}$, $1 \leq i \leq p$, $1 \leq j \leq r_i$, $b_{i,j}, c_{i,j}$, $1 \leq i \leq q$, $1 \leq j \leq s_i$ tels que

$$F = E + \sum_{i=1}^{p} \left(\sum_{j=1}^{r_i} \frac{a_{i,j}}{(X - a_i)^j} \right) + \sum_{i=1}^{q} \left(\sum_{j=1}^{s_i} \frac{b_{i,j} X + c_{i,j}}{(X^2 + \beta_k X + \gamma_k)^j} \right)$$

Méthode

1. Dans le cas des pôles réels, la méthode est la même que celle utilisée pour $\mathbb{C}$.
2. Dans le cas des pôles non réels complexes d'ordre 1 et conjugués, on n'est pas obligé de passer par la décomposition dans $\mathbb{C}$. Soit $F = \frac{P}{(X^2+bX+c)Q}$ une fraction rationnelle de $\mathbb{C}(X)$ de degré négatif et telle que $b^2 - 4ac < 0$. Il existe des réels c, d et un polynôme $P_1 \in \mathbb{R}[X]$ avec $\deg P_1 \leq \deg Q$ tels que :
$$F = \frac{cX + d}{X^2 + bX + c} + \frac{P_1}{Q}$$
En multipliant par X^2+bX+c, on a $\frac{P}{Q} = cX+d+(X^2+bX+c)\frac{P_1}{Q}$. En évaluant cette quantité en ρ l'une des racine complexes de $X^2 + bX + c$, on obtient $\frac{P(\rho)}{Q(\rho)} = c\rho + d$. En écrivant cette expression dans la base $(1, \rho)$, o obtient les valeurs de c et d.
3. Dans certains cas, on peut utiliser la parité de la fraction rationnelle.
4. Dans le cas de pôles complexes non réels conjugués d'ordre 2 au moins, la méthode utilisée pour les pôles non réels complexes conjugués permet de trouver les coefficients réels a et b de l'expression $\frac{aX+b}{(X^2+\beta X+\gamma)^p}$ où p est le degré maximal du facteur $(X^2+\beta X+\gamma)$ dans la décomposition du dénominateur Q en facteurs irréductibles dans $\mathbb{R}[X]$. On peut ensuite procéder par soustraction mais cela demande beaucoup de calculs. On essaye plutôt des évaluations plus astucieuses (limites, évaluation en un point, identification).

14 Factorisation de $\frac{P'}{P}$

Théorème 35 Soit P un polynôme non constant de $\mathbb{C}[X]$ admettant p racines $a_1, \ldots, a_p$ de multiplicités respectives $m_1, \ldots, m_p$. Alors $\frac{P}{P'} = \sum_{k=1}^{p} \frac{m_p}{X - a_k}$