Polynômes à coefficients dans IK

1. Définitions

1.1. Définitions

Un polynôme à coefficients dans K est une expression de la forme

$$P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0,$$

avec n ∈N et a0,a1,...,an ∈K.
L'ensemble des polynômes est noté K[X].

– Les a_i sont appelés les coefficients du polynôme.
– Si tous les coefficients a_i sont nuls, P est appelé le polynôme nul, il est noté 0.
– On appelle le degré de P le plus grand entier i tel que $a_i \neq 0$; on le note degP. Pour le degré du polynôme nul on pose par convention deg(0) =−∞.
– Un polynôme de la forme P = a_0 avec $a_0 \in K$ est appelé un polynôme constant. Si $a_0 \neq 0$, son degré est 0.

1.2. Opérations sur les polynômes

Égalité :

Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ deux polynômes à coefficients dans **K**.

$$P = Q \quad \text{ssi} \quad a_i = b_i \text{ pour tout } i$$

et on dit que *P* et *Q* sont égaux.

Addition :

Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$.

On définit :

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)$$

Multiplication :

Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$.

On définit $P \times Q = c_r X^r + c_{r-1} X^{r-1} + \cdots + c_1 X + c_0$ avec $r = n+m$ et $c_k = \sum_{i+j=k} a_i b_i$ pour $k \in \{0,\ldots,r\}$.

Multiplication par un scalaire :

Si $\lambda \in \mathbf{K}$ alors $\lambda \cdot P$ est le polynôme dont le i-ème coefficient est λa_i.

Proposition 1:

Pour P,Q,R ∈ K[X] alors

0+ P = P , P +Q = Q + P, (P +Q)+ R = P +(Q + R) ;

1·P = P , P ×Q = Q × P , (P ×Q)× R = P ×(Q × R) ;

P ×(Q + R) = P ×Q + P × R.

Proposition 2:

Soient P et Q deux polynômes à coefficients dans K.

deg(P ×Q) = degP +degQ

deg(P +Q) ≥ max(degP,degQ)

On note Rn[X] =$\{ P \in IR[X] / degP \leq n\}$. Si P,Q ∈ IRn[X] alors P +Q ∈ IRn[X]

2. Arithmétique des polynômes

2.1. Division euclidienne

Soient $A,B \in \mathbf{K}[X]$, on dit que B ***divise*** A s'il existe $Q \in \mathbf{K}[X]$ tel que $A = BQ$. On note alors $B|A$.
On dit aussi que A est multiple de B ou que A est divisible par B.
Outre les propriétés évidentes comme $A|A$, $1|A$ et $A|0$ nous avons :

Proposition :

Soient A,B,C ∈ K[X].

1. Si A|B et B|A, alors il existe λ ∈ K^* tel que A = λB.
2. Si A|B et B|C alors A|C.
3. Si C|A et C|B alors C|(AU +BV), pour tout U,V ∈ K[X].

Théorème : Division euclidienne des polynômes

Soient A,B ∈ K[X], avec B ≠ 0, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que :

A = BQ + R et degR < degB.

Q est appelé le quotient et R le reste et cette écriture est la division euclidienne de A par B. Notez que la condition degR < degB signifie R = 0 ou bien 0 É degR < degB. Enfin R = 0 si et seulement si B|A.

Exemple

A = $2X^4 - X^3 - 2X^2 + 3X - 1$ et B = $X^2 - X + 1$. Alors on trouve Q = $2X^2 + X - 3$ et R = $-X + 2$. On n'oublie pas de vérifier qu'effectivement A = BQ + R.

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

2.2. PGCD

Soient A,B ∈ K[X], avec A ≠ 0 ou B ≠ 0. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B.
Cet unique polynôme est appelé le pgcd (plus grand commun diviseur) de A et B que l'on note pgcd(A,B)

Remarque

pgcd(A,B) est un polynôme unitaire.

Si A|B et A ≠ 0, pgcd(A,B) = $\frac{1}{\lambda}$ A, où λ est le coefficient dominant de A.

Pour tout λ ∈ K^* , pgcd(λA,B) = pgcd(A,B).

Comme pour les entiers : si A = BQ+R alors pgcd(A,B) = pgcd(B,R). C'est ce qui justifie l'algorithme d'Euclide.

Algorithme d'Euclide

Soient *A* et *B* des polynômes, *B* ≠ 0.

On calcule les divisions euclidiennes successives,

$A = BQ_1 + R_1$ $\quad \deg R_1 < \deg B$

$$B = R_1Q_2 + R_2 \qquad \deg R_2 < \deg R_1$$

$$R_1 = R_2Q_3 + R_3 \qquad \deg R_3 < \deg R_2$$

...

$$R_{k-2} = R_{k-1}Q_k + R_k \qquad \deg R_k < \deg R_{k-1}$$

$$R_{k-1} = R_kQ_{k+1}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd est le dernier reste non nul R_k (rendu unitaire).

Exemple :

Calculons le pgcd de A = $X^4 - 1$ et B = $X^3 - 1$. On applique l'algorithme d'Euclide :

$X^4 - 1 = (X^3 - 1) \times X + X - 1$

$X^3 - 1 = (X - 1) \times (X^2 + X + 1) + 0$

Le pgcd est le dernier reste non nul, donc pgcd($X^4 - 1, X^3 - 1$) = X −1.

Définition

Soient A,B ∈ K[X]. On dit que A et B sont premiers entre eux si pgcd(A,B) = 1.

si pgcd(A,B) = D alors A et B s'écrivent :

A = D A' , B = D B' avec pgcd(A' ,B') = 1.

2.3. Théorème de Bézout

Soient A,B ∈ K[X] des polynômes avec A ≠ 0 ou B ≠ 0. On note D = pgcd(A,B).

Il existe deux polynômes U,V ∈ K[X] tels que AU +BV = D.

Ce théorème découle de l'algorithme d'Euclide et plus spécialement de sa remontée comme on le voit sur l'exemple suivant.

Nous avons calculé pgcd($X^4 - 1, X^3 - 1$) = X −1. Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne : $X^4 - 1 = (X^3 - 1) \times X + X - 1$, pour en déduire X −1 = $(X^4 - 1) \times 1 + (X^3 - 1) \times (-X)$. Donc U = 1 et V = −X conviennent.

Corollaire 1

Soient A et B deux polynômes. A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que AU +BV = 1

Corollaire 2

Soient A,B,C ∈ K[X] avec A ≠ 0 ou B ≠ 0. Si C|A et C|B alors C|pgcd(A,B)

Corollaire 3. Lemme de Gauss

Soient A,B,C ∈ K[X]. Si A|BC et pgcd(A,B) = 1 alors A|C.

2.4. PPCM

Soient A,B ∈ K[X] des polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que A|M et B|M.
Cet unique polynôme est appelé le ppcm (plus petit commun multiple) de A et B qu'on note ppcm(A,B).

Proposition
Soient A,B ∈ K[X] des polynômes non nuls et M = ppcm(A,B). Si C ∈ K[X] est un polynôme tel que A|C et B|C, alors M|C.

3. Racine d'un polynôme,factorisation

3.1. Racines d'un polynôme

Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{K}[X]$. Pour un élément $x \in \mathbf{K}$, on note

$P(x) = a_nx^n + \cdots + a_1x + a_0$. On associe ainsi au polynôme P une ***fonction polynôme*** (que l'on note encore P)

$P : \mathbf{K} \to \mathbf{K}, \ x \to P(x) = anxn + \cdots + a1x + a0.$
Soit $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$. On dit que α est une ***racine*** (ou un ***zéro***) de P si $P(\alpha) = 0$

Proposition
$P(\alpha) = 0 \Leftrightarrow X - \alpha$ divise P

Soit $k \in N^*$ On dit que α est une ***racine de multiplicité*** k de P si $(X-\alpha)^k$ divise P alors que $(X-\alpha)^{k+1}$ ne divise pas P. Lorsque $k = 1$ on parle d'une ***racine simple***, lorsque $k = 2$ d'une ***racine double***, etc.

3.2. Théorème de d'Alembert-Gauss

Tout polynôme à coefficients complexes de degré n ≥ 1 a au moins une racine dans C. Il admet exactement n racines si on compte chaque racine avec multiplicité.

Exemple
Soit P(X) = aX2 + bX + c un polynôme de degré 2 à coefficients réels : a,b, c ∈ R et a ≠ 0.
–Si $\Delta = b^2 - 4ac > 0$ alors P admet 2 racines réelles distinctes $\frac{-b+\sqrt{\Delta}}{2a}$ et $\frac{-b-\sqrt{\Delta}}{2a}$.
–Si $\Delta < 0$ alors P admet 2 racines complexes distinctes $\frac{-b+i\sqrt{|\Delta|}}{2a}$ et $\frac{-b-i\sqrt{|\Delta|}}{2a}$.
–Si $\Delta = 0$ alors P admet une racine réelle double $\frac{-b}{2a}$.
En tenant compte des multiplicités on a donc toujours exactement 2 racines.

Soit P ∈ K[X] de degré n ≥ 1. Alors P admet au plus n racines dans K.

3.3. Polynômes irréductibles

Soit P ∈ K[X] un polynôme de degré≥ 1, on dit que P est irréductible si pour tout Q ∈ K[X] divisant P, alors, soit Q ∈ K^*, soit il existe λ ∈ K^* tel que Q = λP.

Remarque

Un polynôme irréductible P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près).

La notion de polynôme irréductible pour l'arithmétique de K[X] correspond à la notion de nombre premier pour l'arithmétique de Z.

Dans le cas contraire, on dit que P est réductible ; il existe alors des polynômes A,B de K[X] tels que P = AB, avec deg A $\geq$ 1 et degB $\geq$ 1.

Exemple

Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.

$X^2 - 1$ = (X −1)(X +1) $\in$ R[X] est réductible.

$X^2 + 1$ = (X −i)(X +i) est réductible dans C[X] mais est irréductible dans R[X].

$X^2 - 2$ = (X − $\sqrt{2}$)(X + $\sqrt{2}$) est réductible dans R[X] mais est irréductible dans Q[X].

Lemme d'Euclide

Soit P $\in$ K[X] un polynôme irréductible et soient A,B $\in$ K[X].

Si P|AB alors P|A ou P|B

3.4. Théorème de factorisation

Tout polynôme non constant A $\in$ K[X] s'écrit comme un produit de polynômes irréductibles unitaires :

$$A = \lambda P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$$

où λ $\in K^*$, r $\in N^*$, $k_i \in N^*$ et les P_i sont des polynômes irréductibles distincts. De plus cette décomposition est unique à l'ordre près des facteurs.

3.5. Factorisation dans C[X] et R[X]

Les polynômes irréductibles de C[X] sont les polynômes de degré 1.

Donc pour P $\in$ C[X] de degré n $\geq$ 1 la factorisation s'écrit P = $\lambda(X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r}$, où $\alpha_1,...,\alpha_r$ sont les racines distinctes de P et $k_1,...,k_r$ sont leurs multiplicités.

Les polynômes irréductibles de R[X] sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant Δ < 0.

Soit P $\in$ R[X] de degré n $\geq$ 1. Alors la factorisation s'écrit P = $\lambda(X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r} Q_1^{l1} \cdots Q_s^{ls}$, où les α_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2 : $Q_i = X^2 + \beta_i X + \gamma_i$ avec $\Delta = \beta_i^2 - 4\gamma_i$ < 0.

4.Fractions rationnelles

Une fraction rationnelle à coefficients dans IK est une expression de la forme F = $\frac{P}{Q}$ où P,Q ∈ K[X] sont deux polynômes et Q ≠ 0.

Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des « éléments simples ». Mais les éléments simples sont différents sur C ou sur R.

4.1. Décomposition en éléments simples sur C

Soit P/Q une fraction rationnelle avec P,Q ∈ C[X], pgcd(P,Q) = 1 et Q = $(X-\alpha_1)^{k_1}$ …. $(X-\alpha_r)^{k_r}$. Alors il existe une et une seule écriture :

$$\frac{P}{Q} = E + \frac{\alpha_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{\alpha_{1,2}}{(X-\alpha_1)^{k_r-1}} + \cdots + \frac{\alpha_{1,k_1}}{(X-\alpha_1)} + \frac{\alpha_{2,1}}{(X-\alpha_2)^{k_2}} + \cdots + \frac{\alpha_{2,k_2}}{(X-\alpha_2)} + \cdots$$

Le polynôme E s'appelle la partie polynomiale (ou partie entière). Les termes $\frac{a}{(X-a)^i}$ sont les éléments simples sur C.

4.2. Décomposition en éléments simples sur R

Soit P/Q une fraction rationnelle avec P,Q ∈ R[X], pgcd(P,Q) = 1. Alors P/Q s'écrit de manière unique comme somme :

– d'une partie polynomiale E(X),

– d'éléments simples du type $\frac{a}{(X-a)^i}$

– d'éléments simples du type $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$.

Où les X − α et X^2 + αX + β sont les facteurs irréductibles de Q(X) et les exposants i sont inférieurs ou égaux à la puissance correspondante dans cette factorisation