Polynômes

Dans ce chapitre la lettre $\mathbb{K}$ désignera indifféremment $\mathbb{R}$ ou $\mathbb{C}$. Les lettres n et p désignent des entiers naturels.

Théorème

Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$
Soit $div(A)$ l'ensemble des polynômes diviseurs de A
Soient Q et R les polynômes définis par la division euclidienne de A par B :

$$A = BQ + R \text{ avec } \deg(R) < \deg(B)$$

Alors $div(A) \cap div(B) = div(B) \cap div(R) =$

Preuve

Soit $C \in div(A) \cap div(B)$. $\exists E, F \in \mathbb{K}^2[X]$ tels que $A = CE$ et $B = CF$
$A = BQ + R \Rightarrow CE = CFQ + R \Rightarrow R = C(E - FQ) \Rightarrow C|R \Rightarrow C \in div(B) \cap div(R) \Rightarrow div(A) \cap div(B) \subset div(B) \cap div(R)$
Soit $C \in div(B) \cap div(R)$. $\exists E, F \in \mathbb{K}^2[X]$ tels que $B = CE$ et $R = CF$
$A = BQ + R \Rightarrow A = CEQ + CF \Rightarrow A = C(EQ + F) \Rightarrow C|A \Rightarrow C \in div(A) \cap div(B) \Rightarrow div(B) \cap div(R) \subset div(A) \cap div(B)$
Donc $div(A) \cap div(B) = div(B) \cap div(R)$

Propriété

Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$

$$\exists R \in \mathbb{K}[X] \text{ tel que } div(A) \cap div(B) = div(R)$$

Preuve

La preuve de cette propriété est donnée par l'algorithme d'Euclide.

Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. Réalisons la division euclidienne de A par B.
$\exists (Q_0, R_0) \in \mathbb{K}^2[X]$ tels que $A = BQ_0 + R_0$ avec $\deg(R_0) < \deg(B)$ et $div(A) \cap div(B) = div(B) \cap div(R_0)$
Si $R_0 = 0$, l'algorithme est fini sinon reitérons l'opération avec B et R_0.
$\exists (Q_1, R_1) \in \mathbb{K}^2[X]$ tels que $B = Q_1R_0 + R_1$ avec $\deg(R_1) < \deg(R_0)$ et $div(B) \cap div(R_0) = div(R_0) \cap div(R_1)$
Si $R_1 = 0$, l'algorithme est fini sinon Reitérons l'opération avec R_0 et R_1
$\exists (Q_2, R_2) \in \mathbb{K}^2[X]$ tels que $R_0 = Q_2R_1 + R_2$ avec $\deg(R_2) < \deg(R_1)$ et $div(R_0) \cap div(R_1) = div(R_1) \cap div(R_2)$
……..
Nous obtenons ainsi une famille de polynômes $(R_0, R_1, R_2 \ldots.)$ dont les degrés vérifient $\deg(R_{n+1}) < \deg(R_n)$. La suite des degrés étant strictement décroissante et à valeurs dans $\{\mathbb{N} \cup \{-\infty\}\}$ nous avons l'existence d'un entier N tel que $R_N = 0$. Considérons le dernier reste non nul R_{N-1}
Nous avons $div(A) \cap div(B) = div(R_0) \cap div(R_1) = div(R_1) \cap div(R_2) = \cdots div(R_{N-1}) \cap div(R_N) = div(R_{N-1})$

Définition et propriété

Soient A et B deux polynômes de $\mathbb{K}[X]$ dont l'un au moins est non nul.
On appelle $PGCD(A, B)$ tout polynôme diviseur commun de A et de B de degré maximal.
Parmi ces polynômes, un seul est unitaire on le note $A \wedge B$.

Remarque justifiant la définition

- Si A ou B est nul. Supposons B. Alors $div(A) \cap div(B) = \text{div(A)}$.Donc A est un $PGCD(A, 0)$. Si C est aussi un $PGCD(A, 0)$ cela implique $C|A$ et $\deg(C) = \deg(A)$. Donc $\{\alpha A \text{ avec } \alpha \in \mathbb{R}^*\}$ est l'ensemble des $PGCD(A, 0)$. Dans cet ensemble un seul polynôme est unitaire c'est $A \wedge B$

- Si A et B sont non nuls. Soit F l'ensemble des degrés des polynômes de $div(A) \cap div(B)$. C'est un sous ensemble de $\mathbb{N}$ minoré par 0 et majoré par $\min(degA, degB)$. Il admet donc un plus grand élément n. Soient P et Q deux $PGCD(A, B)$ avec $\deg(P) = \deg(Q) = n$. L'algorithme d'Euclide appliqué à A et B nous donne l'existence d'un R tel que $div(A) \cap div(B) = div(R)$. Nous avons donc P et Q diviseurs de R. Or R est aussi un diviseur de A et de B. P et Q étant les diviseurs de A et de B de degré maximal nous avons $\deg(R) \leq n$.
  Mais P et Q étant diviseurs de R nous avons $\deg(R) = n$. $\exists (\lambda, \mu) \in (\mathbb{K}^*)^2$ tels que $R = \lambda P = \mu Q$
  Nous sommes donc arrrivés au constat suivant : deux polynômes $PGCD(A, B)$ diffèrent donc d'une constante multiplicative non nulle. Dans $PGCD(A, B)$ il n'y a donc qu'un seul polynome unitaire, c'est $A \wedge B$

Propriété

Soient A et B deux polynômes de $\mathbb{K}[X]$ dont l'un au moins est non nul.
Soit C un troisième polynôme

$$C \text{ est un } PGCD(A, B) \Leftrightarrow div(A) \cap div(B) = div(C)$$

Et en particulier $div(A) \cap div(B) = div\ (A \wedge B)$

Preuve

Montrons : $C\ est\ un\ PGCD(A,B) \Rightarrow div(A) \cap div(B) = div(C)$

- Nous avons vu plus haut que si un des deux polynômes est nul, supposons $B, \{\alpha A$ avec $\alpha \in \mathbb{R}^*\}$ est l'ensemble des $PGCD(A,0)$. Or $\forall \alpha \in \mathbb{R}^*\ div(\alpha A) = div(A) \cap div(0)$
- Si A et B sont non nuls. Nous avons vu là encore plus haut que si P est un $PGCD(A,B)$ alors $\exists(\lambda) \in \mathbb{K}^*$ tel que $P = \lambda R, R$ étant défini par l'algorithme d'Euclide : $div(A) \cap div(B) = div(R)$. Nous avons donc bien

$$div(P) = div(R) = div(A,B)$$

Réciproquement : supposons $div(A) \cap div(B) = div(C)$
Supposons $\exists P \in\ div(A) \cap div(B)$ avec $\deg(P) > \deg(C)$ cela implique $P \in\ div(C)$ ce qui est impossible car $deg(P) > deg(C)$ donc C est bien un diviseur de A et de B de degré maximal. C'est bien un $PGCD(A,B)$
$A \wedge B$ est un $PGCD$ parmi d'autres donc la propriété $div(A) \cap div(B) = div\ (A \wedge B)$ en découle.

Remarque	Trouver un $PGCD$ de deux polynômes A et B ou plus spécifiquement $A \wedge B$ revient donc à appliquer l'algorithme d'Euclide.
Exemple	Soient $P = X^4 - 4X^3 + 2X^2 + X + 6$ et $Q = X^4 - 3X^3 + 2X^2 + X + 5$. Déterminons $PGCD(P,Q)$

Solution

Appliquons l'algorithme d'Euclide :

$$(X^4 - 4X^3 + 2X^2 + X + 6) = (X^4 - 3X^3 + 2X^2 + X + 5) * 1 + (-X^3 + 1)$$
$$(X^4 - 3X^3 + 2X^2 + X + 5) = (-X^3 + 1)(-X + 3) + (2X^2 + 2X + 2)$$
$$(-X^3 + 1) = (2X^2 + X + 6)(-\frac{1}{2}X + \frac{1}{2})$$

Le dernier reste non nul $R = 2X^2 + 2X + 2$ est un $PGCD(A,B)$.
En divisant ses coefficients par deux pour le rendre unitaire on obtient $P \wedge Q$

Définition	La définition du PGCD se généralise sur plusieurs polynômes. Soient $A_1, A_2, \dots A_n$ n polynômes de $\mathbb{K}[X]$ tous non nuls. On appelle $PGCD(A_1, A_2, \dots A_n)$ tout polynôme diviseur commun de $A_1, A_2, \dots A_n$ de degré maximal. Parmi ces polynômes, un seul est unitaire on le note $A_1 \wedge A_2 \wedge\ \dots A_n$

Preuve

L'existence d'un tel PGCD se détermine par récurrence.
Soit $P(n)$: $\exists P \in\ \mathbb{K}[X]$ tel que $div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(P)$
Initialisation : cas $n = 2$. Déjà fait précédemment.
Hérédité : Supposons que ce soit vrai à l'ordre n. Montrons-le à l'ordre $n+1$

$$div(A_1) \cap div(A_2) \dots \cap div(A_{n+1}) = [div(A_1) \cap div(A_2) \dots \cap div(A_n)] \cap div(A_{n+1})$$
$$div(A_1) \cap div(A_2) \dots \cap div(A_{n+1}) = div(P) \cap div(A_{n+1})$$
$$div(A_1) \cap div(A_2) \dots \cap div(A_{n+1}) = div(P \wedge A_{n+1})$$

La récurrence est donc démontrée.

$$\forall n, \exists P \in\ \mathbb{K}[X] \text{ tel que } div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(P)$$

Prenons maintenant Q un diviseur commun de $A_1, A_2, \dots A_n$ de degré maximal. Nous savons que $\exists P \in\ \mathbb{K}[X]$ tel que $div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(P)$. Nous avons $Q|P \Rightarrow \deg(Q) \leq \deg(P)$. Mais $P \in\ div(A_1) \cap div(A_2) \dots \cap div(A_n)$ donc $\deg(P) \leq \deg(Q)$. Il vient $\deg(P) = \deg(Q)$. Donc nous avons donc montré que $\exists \lambda \in\ \mathbb{K}^*$ tel que $Q = \lambda P$
Tous les polynômes diviseurs communs de $A_1, A_2, \dots A_n$ de degré maximal s'écrivent donc sous la forme λP avec $\lambda \in\ \mathbb{K}^*$. La réciproque est évidente :
Tout polynôme Q de la forme $Q = \lambda P$ avec $\lambda \in\ \mathbb{K}^*$ vérifie $div(Q) = div(P) = div(A_1) \cap div(A_2) \dots \cap div(A_n)$. C'est donc un diviseur commun de $A_1, A_2, \dots A_n$. Supposons qu'il existe un diviseur commun à $A_1, A_2, \dots A_n$ de degré supérieur. Ce diviseur sera alors un diviseur de Q ce qui amène une contradiction.
Nous avons donc $Q\ PGCD(A_1, A_2, \dots A_n)\ ssi\ Q = \lambda P$ avec $\lambda \in\ \mathbb{K}^*$
Parmi ces polynômes, un seul est unitaire on le note $A_1 \wedge A_2 \wedge\ \dots A_n$

Propriété	Soient $A_1, A_2, \dots A_n$ n polynômes de $\mathbb{K}[X]$ tous non nuls. Soit C un polynôme de $\mathbb{K}[X]$ $C\ est\ un\ PGCD(A_1, A_2, \dots A_n) \Leftrightarrow div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(C)$

Preuve

Nous avons vu plus haut que $\exists P \in\ \mathbb{K}[X]$ tel que $div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(P)$
Nous avons aussi vu que si :
$C\ est\ un\ PGCD(A_1, A_2, \dots A_n) \Rightarrow C = \lambda P$ avec $\lambda \in\ \mathbb{K}^* \Rightarrow div(C) = div(P) = div(A_1) \cap div(A_2) \dots \cap div(A_n)$
Réciproquement :
Soit C tel que $div(A_1) \cap div(A_2) \dots \cap div(A_n) = div(C)$ Nous avons C diviseur commun de $A_1, A_2, \dots A_n$. De plus $div(C) = div(P) \Leftrightarrow \exists\ \lambda \in\ \mathbb{K}^*$ tel que $C = \lambda P$. Supposons que $\exists D \in\ \mathbb{K}[X]$ tel que $D \in div(A_1) \cap div(A_2) \dots \cap div(A_n)$ et $\deg(D) > \deg(C)$. C'est impossible car $D \in\ div(C)$. C est bien un diviseur commun de $A_1, A_2, \dots A_n$ de degré maximal

Propriété	La notion de $PGCD$ est associative. Soient A, B, C trois polynômes non tous nuls de $\mathbb{K}[X]$ Nous avons $(A \wedge B) \wedge C = A \wedge (B \wedge C)$

Preuve

Nous savons que $div\big((A \wedge B) \wedge C\big) = div(A \wedge B) \cap div(C)$

Or $div(A \wedge B) \cap div(C) = div(A) \cap div(B) \cap div(C) = div(A) \cap div(B \wedge C) = div\ (A \wedge (B \wedge C))$

Donc $div\big((A \wedge B) \wedge C\big) = div\ (A \wedge (B \wedge C))$. $(A \wedge B) \wedge C$ et $A \wedge (B \wedge C)$ se divisent mutuellement. Ils ont donc même degré et diffèrent à une constante multiplicative près. Les deux sont unitaires. La constante est donc égale à 1. Nous avons donc $(A \wedge B) \wedge C = A \wedge (B \wedge C)$

Propriété	**Factorisation du $PGCD$**	Soient A et B deux polynômes de $\mathbb{K}[X]$. Soit $P \in \mathbb{K}[X]$ non nul et unitaire. $(PA) \wedge (PB) = P(A \wedge B)$

Preuve

$P(A \wedge B)$ est un diviseur de PA et de PB.

Donc $P(A \wedge B) \in div(PA) \cap div(PB)$. Par définition $div(PA) \cap div(PB) = div(PA \wedge PB)$

donc $P(A \wedge B) \in div(PA \wedge PB)$

Il vient $\exists R \in \mathbb{K}[X]$ tel que $PA \wedge PB = RP(A \wedge B)$

Nous avons donc $RP(A \wedge B) \mid PA$ et $RP(A \wedge B) \mid PB$ ce qui implique $R(A \wedge B) \mid A$ et $R(A \wedge B) \mid B$ (car P non nul)

R est donc de degré nul, sinon cela contredirait le fait que $A \wedge B$ soit le diviseur commun de A et de B de degré maximal.

R est donc un scalaire. De l'expression $PA \wedge PB = RP(A \wedge B)$ nous remarquons que $PA \wedge PB$ est unitaire, $A \wedge B$ est unitaire, P est unitaire donc R doit être unitaire. Nous en déduisons $R = 1$

Donc $\boldsymbol{PA \wedge PB = P(A \wedge B)}$