Polynômes

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

Propriété

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

$$\exists (U,V) \in (\mathbb{K}[X])^2 \text{ tels que } AU + BV = A \wedge B$$

Preuve

Nous avons vu que $A \wedge B$ s'obtient grâce à l'algorithme d'Euclide. L'obtention de U et de V aussi. Il suffit de perfectionner un petit peu l'algorithme.
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 $div(A) \cap div(B) = div(B) \cap div(R_0)$
En posant $U_0 = 1$ et $V_0 = -Q_0$ nous avons $R_0 = U_0 A + V_0 B$
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 $B = R_0 Q_1 + R_1$ avec $\deg(R_1) < \deg(R_0)$ et $div(B) \cap div(R_0) = div(R_0) \cap div(R_1)$
$R_1 = B - R_0 Q_1 = B - (U_0 A + V_0 B) Q_1 = -U_0 Q_1 A + B(1 + V_0 Q_1)$
En posant $U_1 = -U_0 Q_1$ et $V_1 = (1 + V_0 Q_1)$ nous avons $R_1 = U_1 A + V_1 B$
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 $R_0 = R_1 Q_2 + R_2$ avec $\deg(R_2) < \deg(R_1)$ et $div(R_0) \cap div(R_1) = div(R_1) \cap div(R_2)$

$$R_2 = R_0 - R_1 Q_2 = U_0 A + V_0 B - (U_1 A + V_1 B) Q_2 = A(U_0 - Q_2 U_1) + B(V_0 - V_1 Q_2)$$

En posant $U_2 = U_0 - Q_2 U_1$ et $V_2 = (V_0 - V_1 Q_2)$ nous avons $R_2 = U_2 A + V_2 B$
Si $R_2 = 0$, l'algorithme est fini sinon reitérons l'opération avec R_1 et R_2.

…….

$\exists (Q_{p+1}, R_{p+1}) \in \mathbb{K}^2[X]$ tels que $R_{p-1} = R_p Q_{p+1} + R_{p+1}$ avec $\deg(R_{p+1}) < \deg(R_p)$ et $div(R_{p-1}) \cap div(R_p) = div(R_p) \cap div(R_{p+1})$
$R_{p+1} = R_{p-1} - R_p Q_{p+1} = U_{p-1} A + V_{p-1} B - (U_p A + V_p B) Q_{p+1} = A(U_{p-1} - Q_{p+1} U_p) + B(V_{p-1} - V_p Q_{p+1})$
En posant $U_{p+1} = U_{p-1} - Q_{p+1} U_p$ et $V_{p+1} = (V_{p-1} - V_p Q_{p+1})$ nous avons $R_{p+1} = U_{p+1} A + V_{p+1} B$
Si $R_{p+1} = 0$, l'algorithme est fini sinon reitérons l'opération avec R_1 et R_2.

……

Nous avons bien l'existence de deux suites (U_n, V_n) telle que $\forall n \in \mathbb{N}$, $R_n = AU_n + BV_n$

Nous avons vu lors de l'existence du $PGCD$ de deux polynômes que $\exists N \in \mathbb{N}$ tel que $R_{N+1} = 0$.
Le dernier reste non nul R_N est un $PGCD$ de A et de B et diffère donc de $A \wedge B$ à une constante multiplicative près.
Il existe donc bien deux polynômes (U_N, V_N) tels que $R_N = AU_N + BV_N$
$R_N = \lambda (A \wedge B)$ avec $\lambda \in \mathbb{R}^*$ donc $A \wedge B = \left(\frac{1}{\lambda}\right)(AU_N + BV_N) = \frac{U_N}{\lambda} A + \frac{V_N}{\lambda} B$

Exemple

Reprenons l'exemple que nous avons exploité pour déterminer un $PGCD$ de
$P = X^4 - 4X^3 + 2X^2 + X + 6$ et de $Q = X^4 - 3X^3 + 2X^2 + X + 5$. Nous avons vu que :

$$(X^4 - 4X^3 + 2X^2 + X + 6) = (X^4 - 3X^3 + 2X^2 + X + 5) * 1 + (-X^3 + 1)$$
$$(X^4 - 3X^3 + 2X^2 + X + 5) = (-X^3 + 1)(-X + 3) + (2X^2 + 2X + 2)$$
$$(-X^3 + 1) = (2X^2 + X + 6)\left(-\frac{1}{2}X + \frac{1}{2}\right) + 0$$

Prenons le dernier reste non nul : $2X^2 + 2X + 2$ qui est aussi un $PGCD$ de P et Q

$$(2X^2 + 2X + 2) = (X^4 - 3X^3 + 2X^2 + X + 5) - (-X^3 + 1)(-X + 3)$$
$$\begin{aligned}(2X^2 + 2X + 2) &= (X^4 - 3X^3 + 2X^2 + X + 5) \\ &\quad - [(X^4 - 4X^3 + 2X^2 + X + 6) - (X^4 - 3X^3 + 2X^2 + X + 5)](-X + 3) \\ &= (X^4 - 3X^3 + 2X^2 + X + 5)[1 + (-X + 3)] - (X^4 - 4X^3 + 2X^2 + X + 6)(-X + 3) \\ &= (X^4 - 3X^3 + 2X^2 + X + 5) * (-X + 4) - (X^4 - 4X^3 + 2X^2 + X + 6) * (-X + 3)\end{aligned}$$

Nous avons donc $2X^2 + 2X + 2 = UP + VQ$ avec $U = (-X + 4)$ et $V = (-X + 3)$

Propriété	Soient $A_1, A_2, \dots A_n$ n polynômes de $\mathbb{K}[X]$ tous non nuls. $\exists (U_1, U_2, \dots U_n) \in (\mathbb{K}[X])^n$ tels que $A_1U_1 + A_2U_2 + \cdots A_nU_n = A_1 \wedge A_2 \wedge \dots A_n$

Preuve

Par récurrence.
Initialisation : C'est le cas $n = 2$. Déjà fait précédemment.
Hérédité : Supposons que ce soit vrai à l'ordre n.
Soient $A_1, A_2, \dots A_{n+1}$ $n+1$ polynômes de $\mathbb{K}[X]$ tous non nuls.
Nous savons que $A_1 \wedge A_2 \wedge \quad \dots A_{n+1} = (A_1 \wedge A_2 \wedge \quad \dots A_n) \wedge A_{n+1}$. Or d'après l'hypothèse de Récurrence
$\exists (U_1, U_2, \dots U_n) \in (\mathbb{K}[X])^n$ tels que $A_1U_1 + A_2U_2 + \cdots A_nU_n = A_1 \wedge A_2 \wedge \dots A_n$
Nous avons donc $(A_1 \wedge A_2 \wedge \quad \dots A_n) \wedge A_{n+1} = (A_1U_1 + A_2U_2 + \cdots A_nU_n) \wedge A_{n+1}$
Nous voilà ramenés au cas $n = 2$.
$\exists (V_1, V_2) \in (\mathbb{K}[X])^2$ tels que : $V_1(A_1U_1 + A_2U_2 + \cdots A_nU_n) + V_2A_{n+1} = (A_1U_1 + A_2U_2 + \cdots A_nU_n) \wedge A_{n+1} = A_1 \wedge A_2 \wedge \quad \dots A_{n+1}$
Nous avons donc $(V_1U_1)A_1 + (V_1U_2)A_2 + \cdots (V_1U_n)A_n + (V_2)A_{n+1} = A_1 \wedge A_2 \wedge \quad \dots A_{n+1}$