Chapitre 20

Arithmétique des polynômes

Dans tout ce chapitre, K est un corps (habituellement $\mathbb{R}$ ou $\mathbb{C}$), et les lettres majuscules désignent des polynômes à coefficients dans K.

Pour un polynôme $P \in K[X]$, on note $\mathcal{D}(P)$ l'ensemble de ses diviseurs. On rappelle que $\mathcal{D}(0) = K[X]$, et que si $Q \in K[X]$, alors $P \sim Q$ si et seulement si $\mathcal{D}(P) = \mathcal{D}(Q)$.

1 PGCD

1.1 Définition et caractérisation

Définition 1.1 (PGCD)

Soient $A, B \in K[X]$ tels que $A \neq 0$ ou $B \neq 0$. Un pgcd de A et B est un diviseur commun à A et B de degré maximal, *i.e.* un polynôme $D \in K[X]$ tel que

1. $D|A$ et $D|B$.
2. Si $P \in K[X]$, et $P|A$ et $P|B$, alors $\deg(P) \leqslant \deg(D)$.

Remarques.

1. Par définition, un pgcd de A et B divise A et B.
2. Un pgcd de A et 0 (si $A \neq 0$) est A.
3. Diviser par un polynôme A ou par λA, $\lambda \in K^*$, c'est la même chose.

Proposition 1.2 (PGCD et polynômes associés)

Soient $A, B, C, D, P, Q \in K[X]$, avec A et C non nuls.

1. Si $A \sim C$ et $B \sim D$, les pgcd de A et B sont les mêmes que ceux de C et D.
2. Si $P \sim Q$, alors P est un pgcd de A et B si et seulement si Q en est un.

Proposition 1.3

Soient $A, B \in K[X]$ avec $A \neq 0$. Alors $A|B$ si et seulement si un pgcd de A et B est A.

Proposition 1.4

Soient $A, B, Q, R \in K[X]$ tels que $A = BQ + R$. Alors

1. Les diviseurs communs à A et B sont les diviseurs communs à B et R, *i.e.* $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R) \cap \mathcal{D}(B)$.
2. Les pgcd de A et B sont les pgcd de B et R (si ces pgcd sont définis).

Cas particulier important : Q est le quotient et R le reste de la division de A par $B \neq 0$.

Remarque.

On retiendra que "les pgcd ne changent pas lorsqu'on retranche à un des polynômes un multiple de l'autre".

Théorème 1.5 (Caractérisation du PGCD)

Soient $A, B, D \in K[X]$ avec $A \neq 0$ ou $B \neq 0$. Les affirmations suivantes sont équivalentes :

1. D est un pgcd de A et B.
2. $\mathcal{D}(D) = \mathcal{D}(A) \cap \mathcal{D}(B)$.
3. Les diviseurs communs à A et B sont les diviseurs de D.
4. $\forall\, P \in K[X],\ \big(P|A \text{ et } P|B\big) \iff P|D$.
5. $D|A$, $D|B$ et : $\forall\, P \in K[X],\ \big(P|A \text{ et } P|B\big) \implies P|D$.

Remarques.

1. Il faut savoir reconnaître les situations !
2. Cette caractérisation permet de définir $0 \wedge 0$: on a $\mathcal{D}(0) = \mathcal{D}(0) \cap \mathcal{D}(0)$ donc $0 \wedge 0 = 0$. Cela permet d'éviter de toujours devoir supposer qu'un des polynômes est non nul.

Corollaire 1.6 ($A \wedge B$)

Soient $A, B \in K[x]$ avec $A \neq 0$ ou $B \neq 0$. Alors

1. Les pgcd de A et B sont associés.
2. A et B admettent un unique pgcd unitaire, appelé le PGCD de A et B, et noté $A \wedge B$.

Méthode 1.7

Pour déterminer le pgcd de deux polynômes A et B, il suffit de déterminer un polynôme unitaire D qui divise A et B et tel que, si $P|A$ et $P|B$, alors $P|D$.

Proposition 1.8

Soient $A, B, P \in K[X]$. Alors

$$(PA) \wedge (PB) \sim P\,(A \wedge B)\,.$$

1.2 Algorithme d'Euclide

Théorème 1.9 (Algorithme d'Euclide)

Soient $A, B \in K[X]$ deux polynômes non nuls. On construit par récurrence (tant que c'est possible) une suite de polynômes par :

1. $R_{-1} = A$ et $R_0 = B$.
2. Pour $n \geqslant 1$, si $R_n \neq 0$, on définit R_{n+1} comme le reste de la division euclidienne de R_{n-1} par R_n, sinon R_{n+1} n'est pas défini.

Alors :

1. Il existe un entier $p \geqslant 0$ tel que pour tout $n \leqslant p$, R_n est bien défini et non nul, et $R_{p+1} = 0$ (*i.e.* R_p divise R_{p-1}).
2. R_p est un pgcd de A et B, *i.e.* le dernier reste non nul est un pgcd de A et de B.

1.3 Relation de Bézout

Proposition 1.10 (Égalité de Bézout)

Soient $A, B \in K[X]$. Il existe $U, V \in K[X]$ tels que $A \wedge B = AU + BV$.

Méthode 1.11

Voici deux façons de déterminer des coefficients de Bézout. Avec les notations de la proposition 1.9, on note Q_n le quotient de la division euclidienne de R_{n-2} par R_{n-1} ($1 \leqslant n \leqslant p$), et on a

$$R_{n-2} = Q_n R_{n-1} + R_n.$$

1. On utilise l'algorithme donné dans la démonstration. On part de la relation $A \wedge B \sim R_p = R_{p-2} - Q_p R_{p-1}$. On remplace alors R_{p-1} par $R_{p-1} = R_{p-3} - Q_{p-1}R_{p-2}$, donc

$$R_p = R_{p-2} - Q_p(R_{p-3} - Q_{p-1}R_{p-2}) = (1 + Q_pQ_{p-1})R_{p-2} - Q_pR_{p-3}.$$

Puis on remplace R_{p-2} par $R_{p-2} = R_{p-4} - Q_{p-2}R_{p-3}$, et ainsi de suite. Notez qu'on ne remplace qu'un reste à la fois. Lorsqu'il ne reste que R_{-1} et R_0, on a une relation de Bézout : il suffit de diviser R_p par on coefficient dominant.

2. Voici un algorithme plus efficace pour une programmation. On détermine par récurrence des polynômes $U_n, V_n \in K[X]$ pour $-1 \leqslant n \leqslant p$ tels que

$$U_nA + V_nB = R_n.$$

Pour $n = p$, on a $R_p \sim A \wedge B$, ce qui donne des coefficients de Bézout en divisant par le coefficient dominant de R_p.

On pose $U_{-1} = 1$ et $V_{-1} = 0$ (car $R_{-1} = a$) et $U_0 = 0$, $V_0 = 1$ (car $R_0 = b$). Si pour $0 \leqslant n < p$ $U_{n-1}, V_{n-1}, U_n, V_n$ sont construits, on a

$$R_{n+1} = R_{n-1} - Q_{n+1}R_n = (U_{n-1} - Q_{n+1}U_n)A + (V_{n-1} - Q_{n+1}U_n)B,$$

et on pose

$$U_{n+1} = U_{n-1} - Q_{n+1}U_n \quad \text{et} \quad V_{n+1} = V_{n-1} - Q_{n+1}U_n.$$

Cet algorithme a l'avantage de prendre moins de place mémoire.

Pour les deux algorithmes, il est intéressant d'obtenir les coefficients de Bézout formellement en fonction des différents Q_n, R_n (ou U_n et V_n le cas échéant), et de faire les calculs explicites une fois pour toute à la fin. En effet, les coefficients sont, en fonction de Q_n, R_n, (ou U_n et V_n), toujours les mêmes, donc on "s'habitue" au calcul. De plus, certains produits se répètent, ce que l'on ne remarque pas en effectuant les calculs au fur et à mesure. Enfin, quand on remplace au fur et à mesure, on ne reconnaît plus les R_n à remplacer, et on est vite perdu !

2 Polynômes premiers entre eux et théorème de Bézout

2.1 Polynômes premiers entre eux

Définition 2.1

Deux polynômes A et B sont *premiers entre eux* si $A \wedge B = 1$.

Proposition 2.2

Soient $A, B \in K[X]$. Il existe $A_1, B_1 \in K[X]$ premiers entre eux tels que

$$A = (A \wedge B)A_1, \qquad B = (A \wedge B)B_1.$$

2.2 Théorème de Bézout

Théorème 2.3 (Théorème de Bézout)

Deux polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que

$$AU + BV = 1.$$

Remarque.

Attention, s'il existe U et V tel que

$$AU + BV = D,$$

on n'a pas nécessairement $D \sim A \wedge B$, puisque par exemple si

$$AU' + BV' = A \wedge B \quad \text{alors} \quad A(CU') + B(CV') = C(A \wedge B)$$

pour tout polynôme C. Par exemple, on a

3 PPCM

Définition 3.1 (PPCM)

Soient $A, B \in K[X]$ deux polynômes non nul. Un ppcm de A et B est un multiple non nul commun à A et B de degré minimal, *i.e.* un polynôme $M \neq 0$ tel que

1. A et B divisent M.

2. Si A et B divisent P, alors $\deg(M) \leqslant \deg(P)$.

Remarque.
Si $A = 0$ ou $B = 0$, seul 0 est un multiple commun à A et B, qu'on peut définir comme ppcm.

Proposition 3.2 (PPCM et polynômes associés)

Soient $A, B, C, D, P, Q \in K[X]$, avec A, B, C, D non nuls.

1. Si $A \sim C$ et $B \sim D$, les ppcm de A et B sont les mêmes que ceux de C et D.
2. Si $P \sim Q$, alors P est un ppcm de A et B si et seulement si Q en est un.

Théorème 3.3 (Caractérisation du ppcm)

Soient $A, B, M \in K[X]$ des polynômes non nuls. Les affirmations suivantes sont équivalentes.

1. M est un ppcm de A et B.
2. L'ensemble des multiples communs à A et B est l'ensemble des multiples de M.
3. $\forall\, P \in K[X],\ \big(A|P \text{ et } B|P\big) \iff M|P$.
4. $A|M$, $B|M$ et $\forall\, P \in K[X],\ \big(A|P \text{ et } B|P\big) \implies M|P$.

Corollaire 3.4

Soient $A, B \in K[X]$ avec $A \neq 0$ et $B \neq 0$. Alors :

1. Les ppcm de A et B sont associés.
2. A et B admettent un unique ppcm unitaire, appelé le PPCM de A et B, et noté $A \vee B$.

Remarque.
Le théorème reste vrai même si $A = 0$ ou $B = 0$.

Méthode 3.5

Pour déterminer le ppcm de a et b, on exhibe un multiple M commun à A et B tel que, pour tout $P \in K[X]$, $\big(A|P \text{ et } B|P\big) \implies M|P$.

Proposition 3.6

Soient $A, B, P \in K[X]$. Alors

$$(PA) \vee (PB) \sim P\,(A \vee B)\,.$$

4 Lemme de Gauss

4.1 Lemme de Gauss

Théorème 4.1 (Lemme de Gauss)

Soient $A, B, C \in K[X]$. Si A divise BC et si A et B sont premiers entre eux, alors A divise C.

Corollaire 4.2

Soient A et B deux polynômes premiers entre eux. Alors

$$A \vee B \sim AB.$$

Proposition 4.3

Soient $A, B \in K[X]$. Alors

$$AB \sim (A \wedge B)(A \vee B).$$

4.2 Polynômes premiers avec un produit

À partir d'ici, tous les polynômes sont non nuls.

Proposition 4.4

Soient $A, B, C \in K[X]$.

1. A est premier avec BC si et seulement si A est premier avec B et C.
2. Si A et B divisent C et si A et B sont premiers entre eux, alors AB divise C.

Proposition 4.5

1. Un polynôme est premier avec un produit si et seulement s'il est premier avec chacun de ses facteurs.
2. Si des polynômes deux à deux premiers entre eux divisent un polynôme P, alors leur produit divise P.

5 PGCD d'un nombre fini de polynômes

5.1 Cas de trois polynômes

Proposition 5.1

Soient $A, B, C \in K[X]$ des polynômes non nuls. Alors

$$\mathcal{D}(A) \cap \mathcal{D}(B) \cap \mathcal{D}(C) = \mathcal{D}(A \wedge B) \cap \mathcal{D}(C) = \mathcal{D}(A) \cap \mathcal{D}(B \wedge C) = \mathcal{D}(A \wedge C) \cap \mathcal{D}(B).$$

Proposition 5.2

Soient $A, B, C \in K[X]$ des plynômes non nuls. Alors

$$A \wedge (B \wedge C) = (A \wedge B) \wedge C.$$

Définition 5.3 (PGCD de trois polynômes)

Soient $A, B, C \in K[X]$ des polynômes non nuls. Le pgcd $A \wedge B \wedge C$ de A, B et C est défini par

$$A \wedge B \wedge C = A \wedge (B \wedge C) = (A \wedge B) \wedge C.$$

Proposition 5.4

Soient $A, B, C \in K[X]$ des polynômes non nuls. Le pgcd de A, B et C est l'unique diviseur unitaire de degré maximal commun à A, B et C.

Proposition 5.5

Soient $A, B, C \in K[X]$. Un polynôme P divise A, B et C si et seulement s'il divise $A \wedge B \wedge C$.

5.2 Généralisation

Voici les résultats pour un nombre quelconque de polynômes.

Définition 5.6 (PGCD de n polynômes)

Soient $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in (\mathbb{N}^*)^n$. Le pgcd des A_k est l'unique diviseur unitaire de degré maximal commun aux A_k. On le note $A_1 \wedge \cdots \wedge A_n$.

Proposition 5.7

Soient $n \in \mathbb{N}$, $n \geqslant 2$, et $(A_1, \dots, A_n) \in (\mathbb{N}^*)^n$. Alors

$$A_1 \wedge \cdots \wedge A_n = (A_1 \wedge \cdots \wedge A_{n-1}) \wedge A_n = A_1 \wedge (A_2 \wedge \cdots \wedge A_n).$$

Remarque.

Le pgcd de n polynômes est caractérisé comme étant le seul polynôme dont l'ensemble des diviseurs est l'ensemble des diviseurs communs aux n polynômes.

Proposition 5.8 (Relation de Bézout)

Soient $n \in \mathbb{N}$, $n \geqslant 2$, et $(A_1, \dots, A_n) \in (K[X])^n$. Il existe $(U_1, \dots, U_n) \in (K[X])^n$ tel que

$$U_1 A_1 + \cdots + U_n A_n = A_1 \wedge \cdots \wedge A_n.$$

Définition 5.9 (Polynômes premiers entre eux dans leur ensemble)

Soient $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in (K[X])^n$. Les polynômes A_k sont premiers entre eux dans leur ensemble si $A_1 \wedge \cdots \wedge A_n = 1$.

Définition 5.10 (Polynômes premiers entre eux deux à deux)

Soient $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in (K[X])^n$ des polynômes non nuls. Les polynômes A_k sont premiers entre eux deux à deux si

$$\forall\, (i,j) \in [\![1, n]\!],\ i \neq j \Longrightarrow A_i \wedge A_j = 1.$$

Remarque.

Attention à ne pas confondre ces deux notions. Par exemple, 6,10 et 15 sont premiers entre eux dans leur ensemble, mais pas deux à deux (et pris deux à deux, ils ne sont pas premiers entre eux !).

Proposition 5.11

Soient $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in (K[X])^n$ des polynômes non nuls premiers entre eux deux à deux. Alors ils sont premiers entre eux dans leur ensemble.

6 Polynômes irréductibles

6.1 Définition

Définition 6.1 (Polynôme irréductible)

Un polynôme P est *irréductible* s'il n'est pas constant et si

$$A|P \Longrightarrow \Big(\deg(A) = 0 \quad \text{ou} \quad A \sim P\Big),$$

ou de manière équivalente s'il n'est pas constant et si pour tous $A, B \in K[X]$,

$$P = AB \Longrightarrow \Big(\deg(A) = 0 \quad \text{ou} \quad \deg(B) = 0\Big).$$

Dans le cas contraire, il est réductible.

Proposition 6.2 (Cas particuliers pour tout K)

Soit $P \in K[X]$

1. Si $\deg(P) = 1$, alors P est irréductible.
2. Si $\deg(P) \geqslant 2$ et P a une racine, alors P est réductible.
3. Si P est irréductible et a moins une racine, alors $\deg(P) = 1$.
4. Si P est de degré 2 ou 3, et si P n'a pas de racine, il est irréductible.

Remarque.

Attention, ce résultat est faux si $\deg(P) \geqslant 4$, comme le prouve l'exemple de $(X^2+1)^2$ dans $\mathbb{R}[X]$, qui n'a pas de racine réelle, mais est réductible.

Remarque.

L'irréductibilité dépend du corps de base K.

Proposition 6.3

Un polynôme irréductible est premier avec tout polynôme qu'il ne divise pas.

Corollaire 6.4

Un polynôme irréductible divise un produit si et seulement s'il divise un des facteurs.

6.2 Décomposition en produit d'irréductibles

Théorème 6.5 (Polynômes irréductibles à coefficients complexes)

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Théorème 6.6 (Polynômes irréductibles à coefficients réels)

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Remarque.

On retrouve la décomposition 5.13 vue dans le chapitre 17 : tout polynôme non constant à coefficients complexes est scindé, et tout polynôme non constant à coefficients réels est le produit de polynômes de degré 1 et de polynômes de degré 2 sans racine réelle : c'est la décomposition enproduit d'irréductibles, similaire à la décomposition en facteurs premiers pour les entiers.