1.2 Division euclidienne, pgcd de deux polynômes

Un point important qui fait que l'anneau des polynômes à une variable sur un corps $\mathbb{K}$ est très semblable à $\mathbb{Z}$ est l'existence d'une division euclidienne.

Théorème 1.1 *Soient A et B deux polynômes de $\mathbb{K}[X]$, avec B différent du polynôme nul. Alors il existe des polynômes Q (quotient) et R (reste) tels que*

$$A = BQ + R \quad \text{avec } \deg R < \deg B \text{ ou } R = 0 .$$

De plus, le couple (Q, R) vérifiant ces propriétés est unique.

Proposition 1.2 *Le reste de la division euclidienne de P par $X-c$ est $P(c)$. En conséquence, un élément $c \in \mathbb{K}$ est racine de P si et seulement si P est divisible par $X - c$.*

Définition 1.3 *Si A et B sont deux polynômes de $\mathbb{K}[X]$, on dit que* le polynôme D est un plus grand commun diviseur (en abrégé, pgcd) de A et B *quand*

1. *D est un diviseur commun de A et B,*
2. *tout diviseur commun de A et B divise D.*

Autrement dit, l'ensemble des diviseurs de D est égal à celui des diviseurs communs de A et B.

Ceci ne définit pas le pgcd de manière unique, mais à un facteur constant non nul près. L'existence du pgcd est établie, comme pour les entiers, par l'algorithme d'Euclide. Soient A et B deux polynômes. On pose

$$R_0 = A \qquad R_1 = B$$

et, pour $n \geq 1$, tant que R_n est non nul, on définit R_{n+1} comme le reste de la division euclidienne de R_{n-1} par R_n :

$$R_{n-1} = R_n Q_n + R_{n+1} \quad \text{avec } \deg(R_{n+1}) < \deg(R_n) \text{ ou } R_{n+1} = 0 .$$

Comme la suite $\deg R_1,\ \deg R_2, \ldots$ est strictement décroissante, l'algorithme s'arrête au bout d'un nombre fini N d'étapes avec $R_{N+1} = 0$.

Théorème 1.4 *Le polynôme R_N obtenu à la fin de l'algorithme (c'est le dernier reste non nul, si A et B sont différents de 0) est un pgcd de A et B.*

Si A et B sont tous les deux nuls, $\text{pgcd}(A, B) = 0$. Sinon, un pgcd est un polynôme de degré maximal parmi ceux qui divisent à la fois A et B ; on peut rendre le pgcd unique en demandant qu'il soit unitaire (c'est comme cela que le pgcd est quelquefois défini).

Comme pour les entiers, on a :

Théorème 1.5 *Soient A et B deux polynômes, D un pgcd de A et B. Il existe des polynômes U et V tels que $D = UA + VB$.*

Définition 1.6 *Deux polynômes A et B sont dits* premiers entre eux *quand 1 est pgcd de A et B, autrement dit si et seulement si les seuls diviseurs communs de A et B sont les constantes non nulles.*

Théorème 1.7 (Identité de Bezout) *Deux polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que $UA + VB = 1$.*

Corollaire 1.8 *Soit A un polynôme premier avec chacun des polynômes $B_1, \ldots, B_r$. Alors A est premier avec le produit $B_1 \cdots B_r$.*

Théorème 1.9 (Lemme de Gauss) *Soient A, B et C des polynômes tels que A et B soient premiers entre eux et que A divise le produit BC. Alors A divise C.*

Définition 1.10 *Un polynôme M est un* plus petit commun multiple *(ppcm) de deux polynômes A et B si et seulement si*

1. *M est un multiple commun de A et B,*
2. *tout multiple commun de A et B est multiple de M.*

Si A ou B est nul, le ppcm de A et B est 0. Si A et B sont tous les deux non nuls, et si D est un pgcd de A et B, alors AB/D est un ppcm de A et B.

Théorème 1.11 *Soient $A_1, \ldots, A_r$ des polynômes premiers entre eux deux à deux (A_i premier avec A_j si $i \neq j$). Si chaque A_i divise B, alors la produit $A_1 \cdots A_r$ divise B.*

Dans les exercices on dira "le pgcd" ou "le ppcm", et on notera $\operatorname{pgcd}(A, B)$ ou $\operatorname{ppcm}(A, B)$ pour le pgcd ou le ppcm unitaire.

Exercice 1.8

Effectuer les divisions euclidiennes de

$$\begin{aligned} 2X^5 - 5X^3 - 8X \quad &\text{par} \quad X + 3\,, \\ 4X^3 + X^2 \quad &\text{par} \quad X + 1 + i\,, \\ X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5 \quad &\text{par} \quad X^2 + X + 1\,. \end{aligned}$$

En déduire $\operatorname{pgcd}(X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5, X^2 + X + 1)$.

Exercice 1.9

Calculer le reste de la division dans $\mathbb{R}[X]$ de

1. $(\cos a + X \sin a)^n$ par $X^2 + 1$,
2. $(X - 1)^m + X^m - 1$ par $X^2 - X + 1$ selon la valeur de m modulo 6.

Exercice 1.10

Soit $P(X) \in \mathbb{R}[X]$ et a et b deux nombres réels distincts. Calculer le reste $R(X)$ de la division de $P(X)$ par $(X - a)(X - b)$ en fonction de $P(a)$ et $P(b)$.

Exercice 1.11

Soit $P(X) = 3X^3 + 2X^2 + 2$ et $Q(X) = X^2 - 2$.

1. Utiliser l'algorithme d'Euclide pour déterminer le pgcd D de P et Q.
2. En déduire deux polynômes U et V tels que $UP + VQ = D$.

Exercice 1.12

On note $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels et $\deg P$ le degré d'un polynôme P de $\mathbb{R}[X]$. Soit $A(X) = X^3 + 2X^2 - X - 2$ et $B(X) = X^3 - 3X - 2$.

1. Calculer D le pgcd unitaire de A et B.
2. Trouver deux polynômes U_0 et V_0 de $\mathbb{R}[X]$ vérifiant $AU_0 + BV_0 = D$ avec $\deg U_0 < \deg B$ et $\deg V_0 < \deg A$.
3. Trouver le ppcm unitaire de A et B.

Exercice 1.13

On considère les polynômes $A(X) = X^5 - X^4 + 2X^3 + 1$ et $B(X) = X^5 + X^4 + 2X^2 - 1$. Déterminer leur pgcd D et écrire D sous la forme $AU + BV$.

Exercice 1.14

Soient a et b deux entiers strictement positifs. Quel est le pgcd de $X^a - 1$ et $X^b - 1$?

Exercice 1.15

Soit $D = \text{pgcd}(A, B)$ (où A et B ne sont pas nuls tous les deux), et soit (U, V) tels que $AU + BV = D$. Quel est le pgcd de U et V ?

Exercice 1.16

Soient $A(X) = (X-1)^2$ et $B(X) = (X+1)^2$.

1. Calculer le pgcd unitaire D de A et B.
2. Trouver deux polynômes U et V de $\mathbb{R}[X]$ tels que $UA + VB = D$.
3. Déduire une décomposition en éléments simples de $\dfrac{1}{(X^2-1)^2}$.

Exercice 1.17

Soit P et Q dans $\mathbb{K}[X]$ deux polynômes premiers entre eux. Montrer que, si m et n sont des entiers strictement positifs, P^m est premier avec Q^n.

Exercice 1.18

Trouver un polynôme P unitaire de degré ≤ 3, divisible par $X - 1$ et tel que les restes dans la division de P par $X - 2, X - 3$ et $X - 4$ soient égaux.