Chapitre 4

Introduction aux polynômes

Dans ce chapitre, nous proposons un brève introduction aux polynômes et à la division polynomiale.

4.1 Anneau de polynômes

Définition 3.

(*a*) Soit A un anneau commutatif (unitaire), $a_0, \cdots, a_n \in A$ et $n \in \mathbb{N}$ avec $a_n \neq 0$. Une expression de la forme

$$a_n x^n + \cdots + a_1 x + a_0$$

est dite *polynôme* à coefficient dans A. L'entier n est dit *degré* du polynôme et a_n est dit *coefficient de plus haut degré*. On conviendra qu'un polynôme de nul est de degré $-\infty$.

(*b*) Un polynôme de la forme $a_n x^n$ est dit *monôme*.

(*c*) L'ensemble $A[x] = \{a_n x^n + \cdots + a_0$ avec $a_i \in A$ et $n \in \mathbb{N}\}$ est dit *anneau des polynômes* à coefficients dans A.

Remarque 3. On confondra un polynôme $p = a_n x^n + \cdots + a_1 x + a_0$ à coefficients dans un anneau A avec la fonction polynomiale de A dans A qui à $k \in A$ associe $a_n k^n + \cdots a_1 k + a_0$; dans ce cas, l'image de $u \in A$ sera noté $p(u)$.

Exemple 4.

- $p_1 = 1$ et $p_2 = x^2 + 17$ sont des polynômes à coefficients dans $\mathbb{Z}$, de degrés respectifs 0 et 2.
- $p_1' = x^3 + i$ et $p_2' = x^5 + ix + 3$ sont des polynômes à coefficients dans $\mathbb{C}$, de degrés respectifs 3 et 5.

Définition 4. Soit A un anneau commutatif, $p_1 = a_n x^n + \cdots + a_0$ et $p_2 = b_m x^m + \cdots + b_0$ deux éléments de $A[x]$.

– On définit la somme de p_1 et p_2 par

$$p_1 + p_2 = (a_s + b_s)x^s + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

où $s = \max(m, n)$ et $a_i = 0$ si $s \geqslant i > n$ et $b_i = 0$ si $s \geqslant i > m$.

– Le produit de p_1 et p_2 est défini par

$$p_1 p_2 = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \cdots + c_1 x + c_0$$

où pour $k \in \{0, \cdots m+n\}$ $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k = \sum_{\substack{i+j=k \\ i,j \in \{0,\cdots,k\}}} a_i b_j$.

Exemple 5. Soient $p_1 = 2x^3 + x^2 + 2x + 2, p_2 = 2x^2 + 2x + 1 \in \mathbb{Z}/3\mathbb{Z}[x]$. On a alors $p_1 + p_2 = 2x^3 + x$ et $p_1 p_2 = x^5 + 2x^3 + 2$.

La preuve du premier item de la proposition suivante est laissée en exercice.

Proposition 5.
- Si A est un anneau commutatif, alors $A[x]$ l'est aussi ; de plus l'élément unité de $A[x]$ est 1_A.
- Si A est un anneau intègre, alors $A[x]$ l'est aussi.

Preuve. Du premier item, nous savons que si A est intègre (donc commutatif), alors $A[x]$ est commutatif. Il suffit donc de montrer que $A[x]$ n'admet pas de diviseurs de zéro. Soient $p_1 = a_n x^n + \cdots + a_0$ et $p_2 = b_m x^m + \cdots + b_0$ deux polynômes non nuls de $A[x]$. On a alors $p_1 p_2 = b_m a_n x^{m+n} + \cdots$. Puisque A est intègre, $b_m a_n \neq 0$; on a ainsi $p_1 p_2 \neq 0$. L'anneau commutatif $A[x]$ n'admet donc pas de diviseur de zéro, il est intègre. □

4.2 Division polynômiale

Dans le cas où l'anneau A est un corps, on obtient dans $A[x]$ un algorithme analogue à celui de la division des entiers.

Proposition 6. Soit K un corps, $p_1, p_2 \in K[x]$ tels que $p_2 \neq 0$. Il existe un unique couple (q, r) d'éléments de $K[x]$ tels que

$$p_1 = p_2 q + r \quad \text{et} \quad \deg r < \deg p_2;$$

q et r sont dits respectivement *quotient* et *reste* de la division de p_1 par p_2.

Preuve. Montrons l'existence de q et r. Si $p_1 = 0$ ou si $\deg p_1 < \deg p_2$, il suffit de prendre $q = 0$ et $r = p_1$. On peut donc supposer $\deg p_1 \geqslant \deg p_2$. Posons $p_1 = a_n x^n + \cdots + a_0$ et $p_2 = b_m x^m + \cdots + b_0$. Supposons la propriété vérifiée pour tous les polynômes de degré strictement inférieur à n et montrons qu'elle l'est pour p_1. Soit $p_1' = p_1 - a_n b_m^{-1} x^{n-m} p_2$; on a alors $\deg p_1' < \deg p_1$. Ainsi, d'après l'hypothèse de récurrence, il existe $q_1, r_1 \in K[x]$ tels que

$$p_1' = p_2 q_1 + r_1 \quad \text{avec} \quad \deg r_1 < \deg p_2.$$

De la relation $p_1' = p_1 - a_n b_m^{-1} x^{n-m} p_2$, on obtient

$$p_1 = (q_1 + a_n b_m^{-1} x^{n-m}) p_2 + r_1.$$

On posant $q = q_1 + a_n b_m^{-1} x^{n-m}$ et $r = r_1$, on obtient un couple d'éléments de $K[x]$ avec les propriétés désirées.

Montrons l'unicité du couple (q, r). Soient (q', r') un couple d'éléments de $K[x]$ tel que $p_1 = q' p_2 + r'$ avec $\deg r' < \deg p_2$. On a alors

$$q p_2 + r = q' p_2 + r';$$

ou encore

$$r' - r = (q - q')p_2.$$

Puisque $\deg r < \deg p_2$ et $\deg r' < \deg p_2$ et que si $q - q' \neq 0$, alors $\deg(q - q')p_2 \geqslant \deg p_2$, on a nécessairement $r' - r = 0$ et $q - q' = 0$. Ainsi, $r' = r$ et $q = q'$; d'où l'unicité du couple (q, r). □

Exemple 6. Considérons $K = \mathbb{Z}/5\mathbb{Z}$ et $p_1 = 3x^4 + x^3 + 2x^2 + 1$, $p_2 = x^2 + 4x + 2$ deux polynômes à coefficients dans K. Calculons le quotient et le reste de la division de p_1 par p_2.

p_1	$3x^4 + x^3 + 2x^2 + 1$	$x^2 + 4x + 2$	p_2
$3x^2 p_2$	$3x^4 + 2x^3 + x^2$	$3x^2 + 4x$	
$p_1' = p_1 - 3x^2 p_2$	$4x^3 + x^2 + 1$		
$4x p_2$	$4x^3 + x^2 + 3x$		
$p_1' - 4x p_2$	$2x + 1$		

On obtient $p_1 = (3x^2 + 4x)p_2 + 2x + 1$.

Définition 5. Soient K un corps et $p_1 \in K[x]$.

- On dit que $p_2 \in K[x]$ divise p_1 et non note $p_2 \mid p_1$ s'il existe $q \in K[x]$ tel que $p_1 = p_2 q$. Si p_2 ne divise pas p_1, on note $p_2 \nmid p_1$.
- Un scalaire $a \in K$ est dit *zéro* ou *racine* de p_1 de multiplicité $k \geqslant 1$ si $(x-a)^k \mid p_1$ et $(x - a)^{k+1} \nmid p_1$.

Corollaire 2. Soient K un corps, $p \in K[x]$ et $a \in A$; $p(a)$ est le reste de la division de p par $(x - a)$.

Preuve. D'après la proposition 6, il existe q, r tels que $p = (x-a)q + r$ avec $\deg r < 1$. Ainsi, r est une constante et donc $f(a) = r$. □

Corollaire 3. Soient K un corps et $p \in K[x]$. Si p est de degré n, alors il admet au plus n racines dans K (en comptant la multiplicité des racines).

Preuve. Procédons par récurrence sur n. On sait qu'un polynôme de degré 0 (constant non nul) n'admet pas de racine. Supposons que tout polynôme de degré $n' < n$ admette au plus n' racines. Soit p un polynôme de degré n. Si p n'a aucune racine dans K, la propriété est vérifiée. Sinon, soit a une racine de p de multiplicité $k \leqslant n$. On a alors

$$p = (x - a)^k q \text{ avec } q(a) \neq 0 \text{ et } \deg q = n - k.$$

Si p n'a pas d'autre racine que a, alors la propriété est vérifiée. Sinon, soit $b \neq a$ une autre racine de de p. On a alors

$$p(b) = (b-a)^k q(b) = 0.$$

Ainsi, b est aussi une racine de q avec la même multiplicité que pour p. Ainsi, toute racine de p autre que a est aussi racine de q avec la même multiplicité et réciproquement. Or d'après l'hypothèse de récurrence, q qui a pour degré $n-k<n$ admet au plus $n-k$ racines. On déduit que p admet au plus n racines. □

Remarque 4. Le résultat ci dessus n'est pas vérifié pour un anneau de polynômes quelconque. Le lecteur vérifiera que dans $\mathbb{Z}/6\mathbb{Z}[x]$, le polynôme x^2+3x+2 admet quatre racines que sont $1, 2, 4$ et 5.

Définition 6. Soit A un anneau intègre et $p \in A[x]$. Le polynôme p est dit irréductible sur A s'il est non–nul et non–inversible et si pour tous $p_1, p_2 \in A[x]$, si $p = p_1 p_2$ alors p_1 ou p_2 est inversible dans $A[x]$.

Exemple 7.

- $p = 2x^2+4$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{Z}$, car dans $\mathbb{Z}[x]$, $p = 2(x^2+2)$ et 2 n'est pas inversible
- $p' = x^2 - 3$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{R}$.
- $p'' = x^2+1$ est irréductible sur $\mathbb{Z}/3\mathbb{Z}$ mais réductible sur $\mathbb{Z}/5\mathbb{Z}$; dans $\mathbb{Z}/5\mathbb{Z}[x]$, $p'' = (x-2)(x-3)$.

Définition 7. Soit K un corps.

- On appelle *fraction rationnelle à une indéterminée* tout couple (p, q) tel que $p \in K[x]$ et $q \in K[x] \setminus \{0\}$. Une fraction rationnelle (p, q) sera notée $\dfrac{p}{q}$.
- Si $\dfrac{p}{q}$ et $\dfrac{r}{s}$ sont deux fractions rationnelles telles que $ps = rq$, elles seront considérées comme identiques.
- L'ensemble des fractions rationnelles est noté $K(x)$.

Exercices

Exercice 4.1. Montrer que si A est un anneau intègre et si p_1 et p_2 sont deux éléments de $A[x]$, alors $\deg p_1 p_2 = \deg p_1 + \deg p_2$ et $\deg p_1 + p_2 \leqslant \max(\deg p_1, \deg p_2)$.

Exercice 4.2. Montrer que si K est un corps, alors $K[x]$ est un anneau principal.

Exercice 4.3. Montrer que si K est un corps, alors $K(x)$ muni de l'addition

$$\frac{p}{q} + \frac{r}{s} \mapsto \frac{ps + qr}{qs}$$

et de la multiplication

$$\frac{p}{q} + \frac{r}{s} \mapsto \frac{pr}{qs}$$

est un corps.

Exercice 4.4. Soient $p_1 = x^3 + 3x^2 + 2x + 1$ et $p_2 = x^2 + 1$ deux polynômes de $\mathbb{Z}[x]$. Effectuer la division de p_1 par p_2. Effectuer la division dans $\mathbb{C}[x]$ de p_1 par $x - i$.

Exercice 4.5. Soit $p = 1 - x^8$; Factoriser p dans $\mathbb{C}[x]$, dans $\mathbb{R}[x]$, et dans $\mathbb{Q}[x]$.