# Chapitre 6

# Les polynômes

Jusqu'ici, un polynôme est juste une fonction de la forme

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

L'objet de ce chapitre est de définir les polynômes, non comme une fonction, mais comme une expression formelle qui existe entant que telle
La construction des polynômes prend pour base l'ensemble des suites ; nous nous intéresserons aux suites nulles à partir d'un certain rang

## 6.1 Une construction des polynômes

### 6.1.1 Définition

Soit $\mathcal{A}$ un anneau commutatif et unitaire et on considère $\mathcal{A}^{\mathbb{N}}$ l'ensemble des suites d'éléments de $\mathcal{A}$
On appelle polynôme à une variable *(ou à une idéterminée)*, à coefficents dans $\mathcal{A}$ une suite $(a_n)_{n\in\mathbb{N}} \in \mathcal{A}^{\mathbb{N}}$ d'éléments de $\mathcal{A}$, nulle à partir d'un certain rang

**Remarque 1 :**

Les items de cette remarque, ont, eux aussi, beaucoup d'importance.

1. Dire que la suite $(a_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang, c'est dire qu'il existe $N_a \in \mathbb{N}$ tel que, pour tout $n \in \mathbb{N}$, si $n > N_a$, alors $a_n = 0$
   On peut donc aussi noter cette suite : $(a_0, a_1, \cdots, a_{N_a}, 0, 0, \ldots, 0, \cdots)$
2. Le terme $a_0$ est le terme constant, et les $a_i$ sont les coefficients du polynôme.
3. Un polynôme est donc une application $f : \mathbb{N} \longrightarrow \mathcal{A}$ dont un nombre fini de valeurs sont non nulles
4. De la définition 6.1.1, nous tirons la notion d'égalité de 2 polynômes :
$$((a_0, a_1, \cdots, a_i) = (b_0, b_1, \cdots, b_i)) \Longleftrightarrow ((\forall i \in \mathbb{N})\,(a_i = b_i))$$
5. L'ensemble des polynômes à coefficents dans $\mathcal{A}$ est noté $\mathcal{A}[X]$
6. Dans la plupart des cas, l'anneau $\mathcal{A}$ sera l'anneau des entiers relatifs $\mathbb{Z}$, les corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$

### 6.1.2 Addition de 2 polynômes

1. Soient $P$ et $Q$ 2 polynômes de $\mathcal{A}[X]$.
   Nous avons alors $P=(a_0,a_1,\cdots,a_n,0,0,\ldots,0,\cdots)$ et $Q=(b_0,b_1,\cdots,b_p,0,0,\ldots,0,\cdots)$.
   Nous définissons alors l'addition de $P$ et $Q$ par :
   $$P+Q=(a_0+b_0,a_1+b_1,\cdots,\cdots,0,0,\ldots,0,\cdots)$$
   De manière générale, si $P+Q=(c_0,c_1,\cdots,\cdots,0,0,\ldots,0,\cdots)$, alors $c_i=a_i+b_i$
2. Muni de cette addition, $\mathcal{A}[X]$ est un groupe commutatif
   → L'élément neutre est le polynôme $\mathcal{O}=(0,0,\cdots,\cdots,0,0,\ldots,0,\cdots)$ *(Le polynôme nul)*
   → L'opposé du polynôme $P=(a_0,a_1,\cdots,a_n,0,0,\ldots,0,\cdots)$ est le polynôme $-P=(-a_0,-a_1,\cdots,-a_n,0,0,\ldots,0,\cdots)$

**Démonstration**

La démonstration est simple et laissée au lecteur

### 6.1.3 Multiplication de 2 polynômes

Soient $P$ et $Q$ 2 polynômes de $\mathcal{A}[X]$.
Nous avons alors $P=(a_0,a_1,\cdots,a_n,0,0,\ldots,0,\cdots)$ et $Q=(b_0,b_1,\cdots,b_p,0,0,\ldots,0,\cdots)$.
Nous définissons alors la multiplication de $P$ et $Q$ par :

$$P\times Q=(c_0,c_1,\cdots,c_n,0,0,\ldots,0,\cdots) \text{ où } c_n=\sum_{k=0}^{n}a_kb_{n-k}$$

**Remarque 2 :**

Le produit $c_n=\sum_{k=0}^{n}a_kb_{n-k}$ est aussi appelé **produit de convolution** des suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$

### 6.1.4 Proposition

Soient $P$ et $Q$ 2 polynômes de $\mathcal{A}[X]$.
Nous avons alors $P=(a_0,a_1,\cdots,a_n,0,0,\ldots,0,\cdots)$ et $Q=(b_0,b_1,\cdots,b_p,0,0,\ldots,0,\cdots)$ 2 polynômes tels que si $i>n$, alors $a_i=0$ et si $j>p$, alors $b_j=0$
Nous appelons toujours $P\times Q=(c_0,c_1,\cdots,c_n,0,0,\ldots,0,\cdots)$
Alors, si $k>n+p$, alors $c_k=0$

**Démonstration**

Soit $k$ entier tel que $k>n+p$. Alors, $c_k=\sum_{i=0}^{k}a_ib_{k-i}$

- ▷ Si $i\leqslant n$, alors $-i\geqslant -n$ et alors $k-i>n+p-n=p$. Comme $k-i>p$, alors $b_{k-i}=0$
- ▷ Si $k-i\leqslant p$, alors $i\geqslant k-p>n+p-p=n$ et donc $a_i=0$

Dans chaque cas, nous avons $c_k=0$

### 6.1.5 Théorème

$\mathcal{A}$ étant un anneau unitaire, $\mathcal{A}[X]$ muni de l'addition et de la multiplication est aussi un anneau unitaire commutatif.

**Démonstration**

1. On sait déjà que $\mathcal{A}[X]$, muni de l'addition est un groupe commutatif
2. L'élément $E = (1, 0, 0, \cdots, 0)$ est l'élément neutre pour la multiplication.
   Pour les calculs, nous notons $E = (e_1, e_2, e_0, \cdots, e_k, \cdots)$ avec $e_1 = 1$ et $e_k = 0$ si $k \geqslant 2$
   En effet, soit $P = (a_0, a_1, \cdots, a_n, 0, 0, \cdots)$ un polynôme de $\mathcal{A}[X]$. Alors, si nous posons $E \times P = (\alpha_0, \alpha_1, \cdots, \alpha_m, 0, 0, \cdots)$ le polynôme produit, nous avons :
   $$\alpha_k = \sum_{i=0}^{k} e_i a_{k-i} = e_0 a_k = a_k$$
   Et nous avons donc bien $E \times P = P$
3. Montrons que la multiplication est associative
   Soient $P = (a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \cdots)$, $Q = (b_0, b_1, \cdots, b_p, 0, 0, \ldots, 0, \cdots)$ et $R = (c_0, c_1, \cdots, c_m, 0, 0, \ldots, 0, \cdots)$ 3 polynômes de $\mathcal{A}[X]$
   Nous écrirons :
   ⋆ $Q \times R = \left([QR]_0, [QR]_1, \cdots, [QR]_q, 0, 0, \ldots, 0, \cdots\right)$ où $[QR]_k = \sum_{i=0}^{k} b_i c_{k-i}$.
   ⋆ Et $P \times Q = \left([PQ]_0, [PQ]_1, \cdots, [PQ]_q, 0, 0, \ldots, 0, \cdots\right)$ où $[PQ]_k = \sum_{i=0}^{k} a_i b_{k-i}$.
   De telle sorte que,$\beta_l$ le terme d'ordre $l$ de $P \times (Q \times R)$, alors
   $$\beta_l = \sum_{j=0}^{l} a_j [QR]_{l-j} = \sum_{j=0}^{l} a_j \left(\sum_{i=0}^{l-j} b_i c_{l-j-i}\right)$$
   Et si $\gamma_l$ le terme d'ordre $l$ de $(P \times Q) \times R$, alors
   $$\gamma_l = \sum_{j=0}^{l} [PQ]_j c_{l-j} = \sum_{j=0}^{l} c_{l-j} \left(\sum_{i=0}^{j} a_i b_{j-i}\right)$$
   Ré-écrivons le terme $\beta_l$ en tableau pour tenter de comprendre :
   $$\begin{array}{ccccccc} a_0b_0c_l+ & a_0b_1c_{l-1}+ & a_0b_2c_{l-2}+ & a_0b_3c_{l-3}+ & \cdots+ & a_0b_lc_0 \\ a_1b_1c_{l-1}+ & a_0b_1c_{l-2}+ & a_1b_2c_{l-3}+ & \cdots & \cdots+ & a_1b_{l-1}c_0 \\ a_2b_0c_{l-2}+ & a_2b_1c_{l-3}+ & \cdots & \cdots & \cdots & \cdots \\ a_3b_0c_{l-3}+ & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{array}$$
   D'où nous pouvons écrire :
   $$\beta_l = \sum_{x=0}^{l} c_{l-x} \left(\sum_{i=0}^{l} a_i b_{x-i}\right) = \sum_{x=0}^{l} [PQ]_x c_{l-x} = \gamma_l$$
   Et donc, nous avons bien $P \times (Q \times R) = (P \times Q) \times R$
   La multiplication est bien associative.
4. La multiplication est commutative
   Avec les mêmes notations que tout à l'heure, nous avons :
   $$[PQ]_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_{k-i} b_i = [QP]_k$$
   Il y a donc commutativité

$\mathcal{A}[X]$ muni de l'addition et de la multiplication est donc un anneau commutatif et unitaire.

### 6.1.6 Proposition

Soit $\mathcal{P}_0$ le sous ensemble de $\mathcal{A}[X]$ des polynômes $(a,0,0,0,0,\cdots,0,0,0,\cdots)$ où $a \in \mathcal{A}$
Alors $\mathcal{A}$ et $\mathcal{P}_0$ sont des anneaux isomorphes et $\mathcal{P}_0$ est un sous anneau de $\mathcal{A}[X]$

**Démonstration**

Pour le démontrer, nous construisons une application $\Phi : \mathcal{A} \longrightarrow \mathcal{P}_0$ naturellement définie par :

$$\begin{cases} \Phi : \mathcal{A} & \longrightarrow & \mathcal{P}_0 \\ a & \longmapsto & \Phi(a) = (a,0,0,0,0,\cdots,0,0,0,\cdots) \end{cases}$$

Clairement :

- ▷ $\Phi$ est bijective
- ▷ Pour tout $a \in \mathcal{A}$ et tout $b \in \mathcal{A}$ :

$$\Phi(ab) = \Phi(a)\Phi(b) \text{ et } \Phi(a+b) = \Phi(a) + \Phi(b)$$

Et donc, $\mathcal{P}_0$ est un sous anneau de $\mathcal{A}[X]$

**Remarque 3 :**

1. On identifie l'élément $a \in \mathcal{A}$ au polynôme $(a,0,0,0,0,\cdots,0,0,0,\cdots) \in \mathcal{A}[X]$
2. Le polynôme nul et le polynôme unité seront donc notés respectivement 1 et 0.
3. Il est possible de définir sur $\mathcal{A}[X]$une multiplication externe :

$$(\forall \lambda \in \mathcal{A})\,(\lambda P = \lambda(a_0,a_1,\cdots,a_n,0,0,\ldots,0,\cdots) = (\lambda a_0,\lambda a_1,\cdots,\lambda a_n,0,0,\ldots,0,\cdots))$$

Nous avons, et cela se vérifie très facilement, pour tout $\lambda \in \mathcal{A}$ et tout $b \in \mathcal{A}$, tout $P \in \mathcal{A}[X]$ et tout $P \in \mathcal{A}[X]$ :

$$\begin{array}{ll} \lambda(\mu P) = (\lambda\mu)P & 1 \times P = P \\ (\lambda+\mu)P = \lambda P + \mu P & \lambda(P+Q) = \lambda P + \lambda Q \end{array}$$

### 6.1.7 Notion d'indéterminée

On note, comme toujours $\delta_{i,j}$ le symbole de Kronecker, c'est à dire le symbole défini par

$$\delta_{i,j} = 0 \text{ si } i \neq j \qquad \delta_{i,i} = 1$$

1. On considère les suites de polynômes $(e_k)_{k\in\mathbb{N}}$ définies par :

   $$e_k = (\delta_{0,k}, \delta_{1,k}, \delta_{2,k}, \cdots, \delta_{k,k}, \cdots) = (\delta_{i,k})_{i\in\mathbb{N}}$$

   C'est à dire des suites nulles partout sauf au rang $k$ qui vaut 1
2. La suite particulière $e_1 = (\delta_{i,1})_{i\in\mathbb{N}} = (0, 1, 0, 0\cdots, 0) = X$ est appelée indéterminée.
3. Pour tout $k \in \mathbb{N}$, nous notons $X^k = \underbrace{X \times X \times X \times \cdots \times X}_{k \text{ fois}}$

   Alors $X^k = e_k$ ; en particulier $X^0 = e_0 = 1$
4. Tout polynôme $P = (a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \cdots)$ peut s'écrire

   $$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k$$

5. Pour tout entier naturel $n \in \mathbb{N}$ et tout nombre $a_k \in \mathcal{A}$ $(k \leqslant n)$, la relation

   $$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k = 0$$

   Entraîne, pour tout $k \leqslant n$, $a_k = 0$
6. Tout polynôme $P \in \mathcal{A}[X]$ s'écrit de manière unique $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k$

**Démonstration**

1. Il est évident que tout polynôme $P = (a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \cdots)$ de $\mathcal{A}[X]$ peut s'écrire

   $$P = a_0 + a_1e_1 + a_2e_2 + \cdots + a_ne_n = \sum_{k=0}^{n} a_ke_k$$

2. Nous allons démontrer par récurrence que, pour tout $k \in \mathbb{N}$, alors $X^k = e_k$
   - ▷ C'est vrai pour $k = 0$ et $k = 1$
   - ▷ Supposons maintenant que $X^k = e_k$
   - ▷ Démontrons maintenant que $X^{k+1} = e_{k+1}$

   Par définition, $X^{k+1} = X^k \times X$ et si $X^{k+1} = (\alpha_0, \alpha_1, \cdots, \alpha_p, 0, 0, \ldots, 0, \cdots)$, nous avons :

   $$\alpha_p = \sum_{i=0}^{p} \delta_{i,k}\delta_{p-i,1}$$

   D'après 6.1.4, si $p > k+1 \iff p \geqslant k+2$, alors $\alpha_p = 0$
   Si $p < k$, alors, comme $i \leqslant p < k$, $\delta_{i,k} = 0$ et $\alpha_p = 0$
   Si $p = k$, alors $\alpha_k = \sum_{i=0}^{k} \delta_{i,k}\delta_{k-i,1} = \delta_{k,k}\delta_{0,1} = 0$

   Et, si $p = k+1$, alors $\alpha_{k+1} = \sum_{i=0}^{k+1} \delta_{i,k}\delta_{k+1-i,1} = \delta_{k,k}\delta_{1,1} = 1$

   Et nous avons bien $X^{k+1} = e_{k+1}$

   Ainsi, pour tout $k \in \mathbb{N}$, alors $X^k = e_k$

3. Et donc, d'après le point 1, l'identité

$$P = a_0 + a_1 e_1 + a_2 e_2 + \cdots + a_n e_n = \sum_{k=0}^{n} a_k e_k$$

peut aussi s'écrire

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k$$

4. Supposons, maintenant, que $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k = 0$.

Si nous revenons à la définition, ceci signifie que nous avons :

$$(a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \cdots) = (0, 0, \cdots, 0, 0, 0, \ldots, 0, \cdots)$$

qui est vraie, si et seulement si, pour tout $k \leqslant n$, $a_k = 0$

5. Supposons, maintenant, qu'il y ait 2 écritures de $P$ :

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = b_0 + b_1 X + b_2 X^2 + \cdots + b_n X^n$$

Alors :

$$\begin{gathered} P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = b_0 + b_1 X + b_2 X^2 + \cdots + b_n X^n \\ \Longleftrightarrow \\ (a_0 - b_0) + (a_1 - b_1) X + (a_2 - b_2) X^2 + \cdots + (a_n - b_n) X^n = 0 \end{gathered}$$

D'où nous déduisons $a_0 = b_0, a_1 = b_1, \cdots a_n = b_n$.
Il y a donc unicité de l'écriture d'un polynôme

**Remarque 4 :**

1. $X$ est une idéterminée ; on aurait pu choisir $Y$ comme nom de l'indéterminée !!

   Pour « pousser un peu », nous aurions très bien pu choisir comme indéterminée $\heartsuit$, $\looparrowright$ ou encore $Jules$ et nous aurions alors écrit $\mathcal{A}[\heartsuit]$, $\mathcal{A}[\looparrowright]$ ou encore $\mathcal{A}[Jules]$.
   Ainsi, le même polynôme $P$ sécrit dans $\mathbb{Z}[X]$ $P = X^2 + X + 1$ et dans $\mathbb{Z}[\heartsuit]$, $P = \heartsuit^2 + \heartsuit + 1$
   L'usage veut que nous utilisions $X$ comme indéterminée [1]

   L'anneau des polynômes à coefficients dans $\mathcal{A}$ est noté $\mathcal{A}[X]$. D'après la remarque précédente, on voit que $\mathcal{A}[X]$ et $\mathcal{A}[Y]$ sont isomorphes.

2. $\mathcal{A}$ peut très bien être un corps $\mathbb{K}$, car un corps est un anneau particulier.

   **Exemples :**
   - $P = X^2 + X + 1$ est dans $\mathbb{Z}[X]$, mais aussi dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$ ou encore $\mathbb{C}[X]$
   - $Q = (1+i) X^3 - 2iX + 1$ est dans $\mathbb{C}[X]$, mais pas dans $\mathbb{R}[X]$, $\mathbb{Q}[X]$ ou $\mathbb{Z}[X]$
   - $R = X^4 + 1$ est aussi dans $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ ou $\mathbb{C}[X]$

3. $\mathcal{A}[X]$ étant un anneau, il nous est possible de considérer $\mathcal{A}[X][Y]$ polynôme d'indéterminée $Y$ et de coefficients dans $\mathcal{A}[X]$. Nous notons $\mathcal{A}[X][Y] = \mathcal{A}[X, Y]$

1. Et ce n'est pas plus mal, bien au contraire !!

### 6.1.8 Nombre algébrique, nombre transcendant

Soit $\mathcal{A}$ un anneau unitaire et commutatif et $\mathcal{L}$ un anneau commutatif et unitaire tel que $\mathcal{A} \subset \mathcal{L}$
Soit $\alpha \in \mathcal{L} \setminus \mathcal{A}$, c'est à dire tel que $\alpha \in \mathcal{L}$ et $\alpha \notin \mathcal{A}$
Nous appelons $\mathcal{A}[\alpha]$ l'ensemble des éléments de $\mathcal{L}$ définis par :

$$\mathcal{A}[\alpha] = \left\{ y \in \mathcal{L} \text{ tels que } y = \sum_{k=0}^{n} a_k \alpha^k \text{ où } a_k \in \mathcal{A} \text{ pour } k = 0, \dots n \right\}$$

$\mathcal{A}[\alpha]$ est aussi un anneau commutatif et unitaire.

1. S'il existe une relation $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$, avec, pour tout $k = 0, \cdots, n$, $a_k \in \mathcal{A}$, on dit que $\alpha$ est algébrique sur $\mathcal{A}$
2. Si, pour tout $n \in \mathbb{N}$, pour tout $n$-uplet $(a_0, a_1, \cdots, a_n) \in \mathcal{A}^n$, l'égalité $a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n = 0$ entraîne $a_0 = a_1 = a_2 = \cdots = a_n = 0$, on dit que $\alpha$ est transcendant sur $\mathcal{A}$

**Remarque 5 :**

1. Si $\mathcal{A}$ est un anneau et $\mathcal{L}$ un anneau tel que $\mathcal{A} \subset \mathcal{L}$, on dit que $\mathcal{L}$ est un **sur-anneau** de $\mathcal{A}$
2. Il n'est pas nécessaire que $\mathcal{L}$ soit un anneau commutatif et unitaire ; il suffit juste que $\alpha$ commute avec avec tous les éléments de $\mathcal{A}$. Si je l'ai écrit dans la définition, c'est que ce sera le cas le plus fréquent.
3. La démonstration du fait que $\mathcal{A}[\alpha]$ est aussi un anneau commutatif et unitaire est élémentaire.
4. Si $\alpha$ est transcendant, alors les anneaux $\mathcal{A}[\alpha]$ et $\mathcal{A}[X]$ sont isomorphes

**Exemple 1 :**

1. Le nombre $\sqrt{2}$ est algébrique sur $\mathbb{Z}$ et $\mathbb{Q}$, puisque si $\alpha = \sqrt{2}$, alors $\alpha^2 - 2 = 0$ et le polynôme $P = X^2 - 2$ est un polynôme de $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$
2. De même le nombre complexe $i$ est algébrique sur $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$, puisque si $\alpha = i$, alors $\alpha^2 + 1 = 0$ et le polynôme $Q = X^2 + 1$ est un polynôme de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ et $\mathbb{R}[X]$