Chapitre 1

Polynômes à coefficients dans un corps

Dans tout le chapitre, $\mathbb{K}$ désignera l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$.

1.1 L'anneau des polynômes

1.1.1 Notion de corps

$\mathbb{K}$ est muni de deux lois de compositions internes : $+$ et $\times$; la richesse de leurs propriétés lui confère une structure de **corps commutatif** :

- $(\mathbb{K}, +)$ est un **groupe commutatif**, ceci est la conséquence du fait que
  - $+$ est associative : $\forall (a,b,c) \in \mathbb{K}^3,\ (a+b)+c = a+(b+c)$.
  - $+$ est commutative : $\forall (a,b) \in \mathbb{K}^2,\ a+b = b+a$.
  - $+$ admet un élément neutre : 0. On a donc $\forall a \in \mathbb{K},\ a+0 = 0+a = a$.
  - Tout a de $\mathbb{K}$ admet un symétrique (opposé) : $-a$. On a donc $a+(-a) = (-a)+a = 0$.
- $(\mathbb{K}^*, \times)$ est un groupe commutatif (Rappel : $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$). En effet :
  - $\times$ est associative : $\forall (a,b,c) \in (\mathbb{K}^*)^3,\ (a \times b) \times c = a \times (b \times c)$.
  - $\times$ est commutative : $\forall (a,b) \in (\mathbb{K}^*)^2,\ a \times b = b \times a$.
  - $\times$ admet un élément neutre : 1. On a donc $\forall a \in \mathbb{K}^*$, $a \times 1 = 1 \times a = a$.
  - Tout a de $\mathbb{K}^*$ admet un symétrique (inverse) : $\frac{1}{a}$. On a donc $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$.
- $\times$ est distributive à gauche et à droite par rapport à $+$, c'est-à-dire :

$$\forall (a,b,c) \in \mathbb{K}^3,\ a \times (b+c) = a \times b + a \times c \text{ et } (b+c) \times a = b \times a + c \times a$$

Remarques.

1. Dans la pratique et lorsqu'il n'y a pas ambiguïté, on omet le signe $\times$.
2. $\mathbb{R}$ et $\mathbb{C}$ ne sont pas les seuls ensembles ayant une structure de corps (i.e. qui vérifient les propriétés énumérées ci-dessus) : on vérifie sans peine que c'est aussi le cas pour $\mathbb{Q}$. Cela est par contre faux pour $\mathbb{Z}$. On rencontrera dans la suite immédiate du cours sur les polynômes, un corps bien particulier qui entretient avec l'ensemble des polynômes le même rapport que $\mathbb{Q}$ avec $\mathbb{Z}$.

1.1.2 Notion de polynôme - premières opérations

Définition 1.1 *On appelle* ***polynôme*** *à une variable à coefficients dans le corps* $\mathbb{K}$ *toute suite infinie* $\mathrm{A} = (a_0, a_1, a_2, \ldots, a_n, \ldots)$ *d'éléments de* $\mathbb{K}$ *tous nuls à partir d'un certain rang :*

$$\exists \mathrm{N} \in \mathbb{N},\ \forall n \geqslant \mathrm{N},\ a_n = 0$$

Pour tout n *de* $\mathbb{N}$, a_n *est appelé coefficient de rang* n *du polynôme* A.

Remarque. Il ressort de cette définition que deux polynômes sont égaux si et seulement si tous leurs coefficients de rangs correspondants sont égaux : $\mathrm{A} = \mathrm{B} \iff \forall n \in \mathbb{N},\ a_n = b_n$

Exemples.

- $(0, 1, -1, 0, 2, 0, 0, 0, \ldots)$ et $(\pi, e, \sqrt{2}, 0, \ldots)$ sont des polynômes à coefficients dans $\mathbb{R}$.
- Le polynôme $(0, 0, \cdots)$ est appelé ***polynôme nul*** et est noté $0_{\mathbb{K}[\mathrm{X}]}$ ou simplement 0 (les justifications suivent. . .).
- Le polynôme $(1, 0, \cdots)$ est noté $1_{\mathbb{K}[\mathrm{X}]}$ ou simplement 1 (les justifications suivent. . .).
- Un polynôme n'ayant qu'un seul coefficient non nul est appelé ***monôme***.

Addition

Définition 1.2 *Soient* $\mathrm{A} = (a_0, a_1, \cdots)$ *et* $\mathrm{B} = (b_0, b_1, \cdots)$ *deux polynômes à une variable à coefficients dans le corps* $\mathbb{K}$. *On appelle* ***somme*** *des polynômes* A *et* B *et on note* $\mathrm{A} + \mathrm{B}$ *le polynôme* $(a_0 + b_0, a_1 + b_1, \cdots)$ *(Le lecteur vérifiera qu'il s'agit bien d'un polynôme).*

Exemple. Si $\mathrm{A} = (0, \sqrt{2}, 2, 3, 0, \cdots)$ et $\mathrm{B} = (-1, 0, -2, 0, \cdots)$ alors $\mathrm{A}+\mathrm{B} = (-1, \sqrt{2}, 0, 3, 0, \cdots)$.

Propriétés. L'addition des polynômes hérite des propriétés de l'addition dans $\mathbb{K}$: elle est associative, commutative, possède un élément neutre (le polynôme nul, ce qui justifie sa notation) et tout polynôme $\mathrm{A} = (a_0, a_1, \cdots)$ a un opposé $-\mathrm{A} = (-a_0, -a_1, \cdots)$. Muni de l'addition, l'ensemble des polynômes à une variable à coefficients dans le corps $\mathbb{K}$ est donc un groupe commutatif.

Exercice 1.1 Démontrer ces propriétés.

Multiplication

Définition 1.3 *Soient* $\mathrm{A} = (a_0, a_1, \cdots)$ *et* $\mathrm{B} = (b_0, b_1, \cdots)$ *deux polynômes à une variable à coefficients dans le corps* $\mathbb{K}$. *On appelle* ***produit*** *des polynômes* A *et* B *et on note* $\mathrm{A.B}$ *(ou plus simplement* AB*) le polynôme* $(c_0, c_1, \cdots)$ *défini par :*

$$\forall n \in \mathbb{N} \quad c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}$$

Remarque. Les coefficients c_n sont bien tous nuls à partir d'un certain rang.

Exemple. Si $\mathrm{A} = (1, 2, 0, \cdots)$ et $\mathrm{B} = (0, 1, 1, 0, \cdots)$ alors $\mathrm{AB} = (0, 1, 3, 2, 0, \cdots)$.

Propriétés. La multiplication des polynômes est associative, commutative, possède un élément neutre (le polynôme $(1, 0, 0, \cdots)$, ce qui justifie sa notation) et elle est distributive par rapport à l'addition.

Démonstration : Vérifions par exemple l'associativité (le reste est laissé en exercice).
Soient $\mathrm{A} = (a_0, a_1, \cdots)$, $\mathrm{B} = (b_0, b_1, \cdots)$ et $\mathrm{C} = (c_0, c_1, \cdots)$ trois polynômes. Soit $n \in \mathbb{N}$.

Le coefficient de rang n de A(BC) est $\displaystyle\sum_{k=0}^{n} a_k \left(\sum_{j=0}^{n-k} b_j c_{n-k-j}\right) = \sum_{k=0}^{n}\sum_{j=0}^{n-k} a_k b_j c_{n-k-j} = \sum_{\substack{i\in\mathbb{N},\, j\in\mathbb{N},\, k\in\mathbb{N}\\ i+j+k=n}} a_i b_j c_k$

Le coefficient de rang n de (AB)C est $\displaystyle\sum_{k=0}^{n}\left(\sum_{j=0}^{k} a_j b_{k-j}\right) c_{n-k} = \sum_{k=0}^{n}\sum_{j=0}^{k} a_j b_{k-j} c_{n-k}$ soit encore $\displaystyle\sum_{\substack{i\in\mathbb{N},\, j\in\mathbb{N},\, k\in\mathbb{N}\\ i+j+k=n}} a_i b_j c_k$. (On peut, pour s'en convaincre, regrouper dans cette deuxième expression les termes contenant a_0, ceux contenant a_1, ... et retrouver ainsi la première expression.) □

Conséquence. Compte tenu des propriétés mises en évidence, muni de l'addition et de la multiplication ainsi définies, l'ensemble des polynômes à une variable à coefficients dans le corps $\mathbb{K}$ est ce que l'on appelle un **anneau commutatif (unitaire)**.

Remarque. Cet ensemble n'est pas un corps : tous les polynômes non nuls n'ont pas nécessairement un inverse. En fait, comme on le verra, très peu en ont...

Remarque. Par convention, pour tout polynôme A, $\mathrm{A}^0 = 1$. On définit alors par récurrence la puissance n-ième du polynôme A en posant : $\forall n \in \mathbb{N},\ \mathrm{A}^{n+1} = \mathrm{A}.\mathrm{A}^n$.

Exercice 1.2 Démontrer la formule du binôme : pour tous polynômes A et B et pour tout entier naturel n,

$$(\mathrm{A}+\mathrm{B})^n = \sum_{k=0}^{n} \binom{n}{k} \mathrm{A}^k \mathrm{B}^{n-k}$$

1.1.3 Polynômes constants - Notation définitive des polynômes

Définition 1.4 *On appelle* ***polynôme constant*** *ou plus simplement* ***constante*** *tout polynôme de la forme* $(\lambda, 0, 0, \cdots)$ *où* $\lambda \in \mathbb{K}$.
Un tel polynôme sera identifié à la constante λ *(voir la proposition 1.6).*

Conséquence. ***(Multiplication par un scalaire)*** Pour tout polynôme $\mathrm{A} = (a_0, a_1, \cdots)$ et tout λ dans $\mathbb{K}$ on a : $\lambda.\mathrm{A} = (\lambda, 0, 0, \cdots).(a_0, a_1, \cdots) = (\lambda a_0, \lambda a_1, \cdots)$.

Remarque. L'addition et la multiplication par les constantes munissent l'ensemble des polynômes à une variable d'une structure que l'on nomme ***espace vectoriel sur le corps*** $\mathbb{K}$.

Définition 1.5 *On appelle* ***indéterminée*** *ou encore* ***variable*** *le polynôme* $\mathrm{X} = (0, 1, 0, 0, \cdots)$.

Propriété. On vérifie alors que : $\mathrm{X}^2 = \mathrm{X}.\mathrm{X} = (0, 0, 1, 0, 0, \ldots)$, $\mathrm{X}^3 = \mathrm{X}.\mathrm{X}^2 = (0, 0, 0, 1, 0, \ldots)$ et ainsi de suite ...
On conviendra dorénavant que $\mathrm{X}^0 = (1, 0, 0, \ldots) = 1$.

Conséquence. Tout polynôme $\mathrm{A} = (a_0, a_1, \ldots, a_n, 0, \ldots)$ peut s'écrire :

$$\mathrm{A} = a_0 + a_1\mathrm{X} + a_2\mathrm{X}^2 + \ldots + a_n\mathrm{X}^n = \sum_{i=0}^{n} a_i \mathrm{X}^i$$

Notation. Puisque les scalaires (i.e. les éléments de $\mathbb{K}$) et l'indéterminée suffisent pour écrire tous les polynômes, on notera dorénavant $\mathbb{K}[\mathrm{X}]$ leur ensemble.

Remarque. L'indéterminée X n'est pas un élément de $\mathbb{K}$. En particulier, l'équation polynomiale $\mathrm{X}^2 - 1 = 0$ n'a pas de solution (écrire $\mathrm{X} = 1$ ou $\mathrm{X} = -1$ n'aurait pas de sens).

Proposition 1.6
L'application $\varphi : \begin{array}{l} \mathbb{K} \longrightarrow \mathbb{K}[X] \\ \lambda \longmapsto (\lambda, 0, \ldots) \end{array}$ *vérifie :*

- $\forall (\lambda, \mu) \in \mathbb{K}^2$, $\varphi(\lambda + \mu) = \varphi(\lambda) + \varphi(\mu)$ *et* $\varphi(\lambda\mu) = \varphi(\lambda).\varphi(\mu)$
- $\varphi(1) = 1_{\mathbb{K}[X]}$

On dit que φ *est un* ***morphisme d'anneaux (unitaires)****. L'application* φ *est de plus injective (ce qui justifie l'identification du scalaire* λ *et du polynôme* $(\lambda, 0, \ldots)$*).*

Démonstration : Cela résulte de manière immédiate des définitions des opérations (addition et multiplication) dans $\mathbb{K}[X]$. □

1.2 Degré et valuation d'un polynôme

1.2.1 Degré d'un polynôme

Définition 1.7 *Soit* A *un polynôme non nul. Le* ***degré*** *de* A *(noté* $\deg A$*) est le* *plus grand* *entier* n *tel que le coefficient* a_n *de* X^n *dans* A *soit non nul. Ce coefficient* a_n *s'appelle alors le coefficient dominant et est noté* coefdom(A)*.*
On dit que A *est* ***unitaire*** *ou encore* ***normalisé*** *si son coefficient dominant est 1.*
Par convention, $\deg 0 = -\infty$*.*

Exemple. $A = -2X^3 + X^2 + 2X^5 + X^4$ est un polynôme de degré 5 et de coefficient dominant 2.

Proposition 1.8 *Pour* *tous* *polynômes* A *et* B*, avec les conventions* $\max(-\infty, d) = d$ *et* $-\infty + d = -\infty$ *pour tout* d *de* $\mathbb{N} \cup \{-\infty\}$*, on a :*

- $\deg(A + B) \leqslant \max\{\deg A, \deg B\}$
  L'inégalité stricte a lieu si et seulement si A *et* B *sont non nuls,* $\deg A = \deg B$ *et* $\mathrm{coefdom}(A) + \mathrm{coefdom}(B) = 0$*.*
- $\deg(AB) = \deg A + \deg B$.
  Si A *et* B *sont non nuls, on a de plus* $\mathrm{coefdom}(AB) = \mathrm{coefdom}(A).\mathrm{coefdom}(B)$*.*

Démonstration : Montrons le résultat pour le produit (celui pour la somme est laissé à titre d'exercice). C'est clair si A ou B est nul. Dans le cas contraire, notons p le degré de A et q celui de B et posons $C = AB$. Avec les notations habituelles, on a : $\forall n \in \mathbb{N} \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Comme $\forall k > p$, $a_k = 0$ et $\forall k > q$, $b_q = 0$, on a immédiatement $\forall n > p + q$, $c_n = 0$ et aussi $c_{p+q} = a_p b_q$. Les conclusions en découlent. □

Proposition 1.9 *Soient* A *et* B *deux polynômes de* $\mathbb{K}[X]$*.*

$$\textit{Si } AB = 0 \textit{ alors } A = 0 \textit{ ou } B = 0$$

En termes plus savants, l'anneau $\mathbb{K}[X]$ *est* ***intègre****.*

Démonstration : Supposons $AB = 0$ et $A \neq 0$. L'égalité $\deg(AB) = \deg A + \deg B$ entraîne alors $\deg B = -\infty$ et donc $B = 0$. □

Exercice 1.3 Montrer que les seuls éléments inversibles (pour la multiplication) de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Remarque. Pour tout entier naturel n, il est d'usage de noter $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré au plus n. Cet ensemble a une structure d'espace vectoriel sur $\mathbb{K}$ (voir feuille d'exercices).

1.2.2 Valuation d'un polynôme

Définition 1.10 *La* ***valuation*** *du polynôme* $\mathrm{A} = \sum_{k=0}^{\infty} a_k \mathrm{X}^k$ *(notée* $\operatorname{val} \mathrm{A}$*) est, si le polynôme est non nul, le* <u>*plus petit*</u> *indice* m *tel que* $a_m \neq 0$*, sinon elle est égale à* $+\infty$ *(convention).*

Proposition 1.11 *Pour tous polynômes* A *et* B*, , avec les conventions* $\min(+\infty, d) = d$ *et* $+\infty + d = +\infty$ *pour tout* d *de* $\mathbb{N} \cup \{+\infty\}$*, on a :*

$$\operatorname{val}(\mathrm{A}+\mathrm{B}) \geqslant \min\{\operatorname{val} \mathrm{A}, \operatorname{val} \mathrm{B}\} \qquad \textit{et} \qquad \operatorname{val}(\mathrm{A}.\mathrm{B}) = \operatorname{val} \mathrm{A} + \operatorname{val} \mathrm{B}$$

Exercice 1.4 Démontrer cette proposition.

1.3 Autres opérations sur les polynômes

1.3.1 Substitution

On peut substituer un polynôme B à la variable X dans un autre polynôme A pour obtenir un nouveau polynôme A(B) (parfois noté aussi $\mathrm{A} \circ \mathrm{B}$) : si $\mathrm{A} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$, alors $\mathrm{A}(\mathrm{B}) = a_0 + a_1\mathrm{B} + \cdots + a_n\mathrm{B}^n$.

Exemple. Si $\mathrm{A} = \mathrm{X}^3 - 2\mathrm{X} + 5$ alors $\mathrm{A}(\mathrm{X}^2-1) = (\mathrm{X}^2-1)^3 - 2(\mathrm{X}^2-1) + 5 = \mathrm{X}^6 - 3\mathrm{X}^4 + \mathrm{X}^2 + 6$.

Remarques.
- Lorsque $\mathrm{B} = \mathrm{X}$, $\mathrm{A} \circ \mathrm{B} = \mathrm{A}(\mathrm{X}) = \mathrm{A}$. Le polynôme A peut donc aussi être noté A(X).
- Lorsque $\mathrm{B} = 0$, $\mathrm{A} \circ \mathrm{B} = \mathrm{A}(0) = a_0$. Lorsque $\mathrm{A} = 0$, $\mathrm{A} \circ \mathrm{B} = 0(\mathrm{B}) = 0$.

Proposition 1.12 *Soient* A *et* B *deux polynômes* <u>*non nuls*</u> *de* $\mathbb{K}[\mathrm{X}]$*. Alors :*

$$\deg(\mathrm{A} \circ \mathrm{B}) = \deg(\mathrm{A}).\deg(\mathrm{B})$$

Proposition 1.13 *Soit* $(\mathrm{A}_1, \mathrm{A}_2, \mathrm{B}) \in (\mathbb{K}[\mathrm{X}])^3$*. Alors :*
- $(\mathrm{A}_1 + \mathrm{A}_2)(\mathrm{B}) = \mathrm{A}_1(\mathrm{B}) + \mathrm{A}_2(\mathrm{B})$
- $(\mathrm{A}_1\mathrm{A}_2)(\mathrm{B}) = \mathrm{A}_1(\mathrm{B}).\mathrm{A}_2(\mathrm{B})$

Exercice 1.5 Démontrer ces deux propositions.

1.3.2 Dérivation des polynômes

Définition 1.14 *Soit* $\mathrm{A} = a_0 + a_1\mathrm{X} + \cdots + a_n\mathrm{X}^n$ *un polynôme de* $\mathbb{K}[\mathrm{X}]$*. On appelle polynôme* ***dérivé*** *de* A *et on note* A' *le polynôme noté* A' *défini par* $\mathrm{A}' = a_1 + 2a_2\mathrm{X} + \cdots + na_n\mathrm{X}^{n-1}$ *si* $n \in \mathbb{N}^*$ *et* $\mathrm{A}' = 0$ *si* $n = 0$*.*

Remarque. Cette définition est purement algébrique et ne fait aucunement appel à la notion analytique de limite.

Proposition 1.15 *Soient* A *et* B *dans* $\mathbb{K}[\mathrm{X}]$ *et* $\lambda \in \mathbb{K}$*.*
- $(\mathrm{A}+\mathrm{B})' = \mathrm{A}' + \mathrm{B}'$ *et* $(\lambda\mathrm{A})' = \lambda\mathrm{A}'$ *: on dit que l'application* $\mathrm{P} \longmapsto \mathrm{P}'$ *est linéaire.*
- $(\mathrm{AB})' = \mathrm{A}'\mathrm{B} + \mathrm{AB}'$
- $(\mathrm{A} \circ \mathrm{B})' = \mathrm{B}'.\,\mathrm{A}' \circ \mathrm{B}$

Démonstration : Montrons par exemple la formule sur le produit.
Pour montrer que $(\mathrm{AB})' = \mathrm{A}'\mathrm{B} + \mathrm{AB}'$, on montre que ces deux polynômes ont les mêmes coefficients. En notant $\mathrm{A} = (a_0, a_1, \cdots)$ et $\mathrm{B} = (b_0, b_1, \cdots)$, on a $\mathrm{AB} = (c_0, c_1, \cdots)$ avec $\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Pour tout n de $\mathbb{N}$, le coefficient de rang n dans le polynôme

- $(\mathrm{AB})'$ est $(n+1)c_{n+1} = (n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k}$,
- $\mathrm{A}'\mathrm{B} + \mathrm{AB}'$ est $\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k} + \sum_{k=0}^{n} a_k(n-k+1)b_{n-k+1}$ soit, en changeant k en $k-1$ dans la première somme, $\sum_{k=1}^{n+1} k a_k b_{n+1-k} + \sum_{k=0}^{n} a_k(n-k+1)b_{n-k+1}$. Ce coefficient vaut donc
$$(n+1)a_{n+1}b_0 + \sum_{k=1}^{n} a_k(n-k+1+k)b_{n-k+1} + a_0(n+1)b_{n+1} = (n+1)\sum_{k=0}^{n+1} a_k b_{n+1-k}.$$

On a donc bien $(\mathrm{AB}') = \mathrm{A}'\mathrm{B} + \mathrm{AB}'$. □

Dérivation d'ordre supérieur.

On définit par récurrence les dérivées successives d'un polynôme A en posant : $\mathrm{A}^{(0)} = \mathrm{A}$ et, pour tout n de $\mathbb{N}$, $\mathrm{A}^{(n+1)} = \left(\mathrm{A}^{(n)}\right)'$. $\mathrm{A}^{(n)}$ est appelé polynôme dérivé d'ordre n de A.

Exemple. Soit $\mathrm{A} = 2 + \mathrm{X} + 3\mathrm{X}^2 + \mathrm{X}^4$. Alors $\mathrm{A}' = 1 + 6\mathrm{X} + 4\mathrm{X}^3$, $\mathrm{A}'' = \mathrm{A}^{(2)} = 6 + 12\mathrm{X}^2$, $\mathrm{A}^{(3)} = 24\mathrm{X}$, $\mathrm{A}^{(4)} = 24$ et $\mathrm{A}^{(5)} = 0$

Exercice 1.6 Démontrer la formule de Leibniz : pour tous polynômes A et B et pour tout entier naturel non nul n,
$$(\mathrm{AB})^{(n)} = \sum_{k=0}^{n} \binom{n}{k} \mathrm{A}^{(k)}\mathrm{B}^{(n-k)}$$

Remarque. Si A est un polynôme non constant alors on a $\deg \mathrm{A}' = \deg \mathrm{A} - 1$. En particulier, si A est degré n alors on a $\forall k > n,\ \mathrm{A}^{(k)} = 0$.