

# Résumé de Cours 1

## Polynômes

Soit  $\mathbb{K}$  un corps commutatif, par exemple,  $\mathbb{K} = \mathbb{C}, \mathbb{R}, \mathbb{Q}$  etc.

Posons

$$\mathbb{K}[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \mid a_i \in \mathbb{K} (0 \leq i \leq n)\}.$$

Pour  $P = a_0 + a_1X + \cdots + a_mX^m$ ,  $Q = b_0 + b_1X + \cdots + b_nX^n \in \mathbb{K}[X]$  et  $\lambda \in \mathbb{K}$ , on définit

$$P + Q := \sum_{k=0}^{\max\{m,n\}} (a_k + b_k)X^{k+l},$$

$$P \cdot Q := \sum_{k=0}^m \sum_{l=0}^n a_k b_l X^{k+l} = \sum_{N=0}^{m+n} \left( \sum_{k+l=N} a_k b_l \right) X^{k+l}.$$

Ici, on pose  $a_{m+1} = a_{m+2} = \cdots = 0$ ,  $b_{n+1} = b_{n+2} = \cdots = 0$ . En particulier,  $X^0 := 1$  et  $X^m = \overbrace{X \cdot X \cdots X}^m$  pour  $m \in \mathbb{N}^*$ . Ces opérations satisfont les propriétés suivantes : pour  $P, Q, R \in \mathbb{K}[X]$ ,

1. (associativité)  $(P + Q) + R = P + (Q + R)$ ,  $(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$ ,
2. (commutativité)  $Q + P = P + Q$ ,  $P \cdot Q = Q \cdot P$ ,
3. (distributivité)  $(P + Q) \cdot R = P \cdot R + Q \cdot R$  (donc,  $P \cdot (Q + R) = P \cdot Q + P \cdot R$ ).

Un **polynôme** en l'indéterminée  $X$  est un élément de  $\mathbb{K}[X]$ .

## Division euclidienne

Soit  $d^0 : \mathbb{K}[X] \rightarrow \mathbb{N} \cup \{-\infty\}$  l'application définie par

$$d^0(P) := \begin{cases} m & \text{si } P = a_0 + a_1X + \cdots + a_mX^m \text{ avec } a_m \neq 0, \\ -\infty & \text{si } P = 0. \end{cases}$$

On appelle  $d^0(P)$  le **degré** du polynôme  $P \in \mathbb{K}[X]$ . (On le note aussi par  $\deg(P)$ .) Voici une propriété :

**Lemme** Soit  $P, Q \in \mathbb{K}[X]$ . Alors,  $d^0(P \cdot Q) = d^0(P) + d^0(Q)$ .  $\square$

**Théorème** (Division euclidienne) Soit  $P, Q \in \mathbb{K}[X]$  avec  $d^0(Q) > 0$ .

Alors, il existe un *unique* couple de polynômes  $(R, S)$  dans  $\mathbb{K}[X]$  tels que

1.  $P = SQ + R$ ,
2.  $d^0(R) < d^0(Q)$ .

Lorsque  $R = 0$ , on dit que le polynôme  $Q$  **divise**  $P$ .  $\square$

Soit  $P, Q \in \mathbb{K}[X] \setminus \{0\}$ . Le **plus grand commun diviseur** de  $P$  et  $Q$ , noté par  $PGCD(P, Q)$ , est un polynôme  $D$  non nul qui divise  $P$  et  $Q$  parmi lesquels le degré  $d^0(D)$  est le plus grand.

Attention ! Le  $PGCD(P, Q)$  est défini à un scalaire près.

**Corollaire** (Identité de Bézout) Soit  $P, Q \in \mathbb{K}[X]$  tels que  $d^0(P), d^0(Q) > 0$ . Alors, il existe un couple de polynômes  $(A, B)$  dans  $\mathbb{K}[X]$  tel que

$$AP + BQ = D,$$

où  $D = PGCD(P, Q)$ .  $\square$