Divisibilité polynomiale et sous-espace vectoriel

Soit $A \in \mathbb{R}[X]$ un polynôme non nul et $F = \{P \in \mathbb{R}[X] \mid A \text{ divise } P\}$.

Définition : "A divise P"

Dire que A **divise** P signifie : $\exists Q \in \mathbb{R}[X]$ tel que $P = AQ$.

Donc on peut réécrire : $F = \{AQ \mid Q \in \mathbb{R}[X]\}$.

On dit aussi que Fest l'ensemble des **multiples** de A.

1. Montrer que F est un sous-espace de $\mathbb{R}[X]$.

Un ensemble $F \subset \mathbb{R}[X]$ est un sous-espace si :

1. $0 \in F$
2. si $P_1, P_2 \in F$ alors $P_1 + P_2 \in F$ (stabilité par addition)
3. si $P \in F$et $\lambda \in \mathbb{R}$ alors $\lambda P \in F$ (stabilité par scalaire)

- Le polynôme nul est $0(X) = 0$.

On a : $0 = A.0$ où 0 à droite est aussi le polynôme nul. Donc $A \mid 0$. Ainsi : $0 \in F$.

- Soient $P_1, P_2 \in F$. Par définition de F, il existe $Q_1, Q_2 \in \mathbb{R}[X]$ tels que : $P_1 = AQ_1, P_2 = AQ_2$.

Alors : $P_1 + P_2 = AQ_1 + AQ_2 = A(Q_1 + Q_2)$.

Or $Q_1 + Q_2 \in \mathbb{R}[X]$, donc $P_1 + P_2$ est encore un multiple de A. Donc : $P_1 + P_2 \in F$.

- Soit $P \in F$et $\lambda \in \mathbb{R}$. Comme $P \in F$, il existe $Q \in \mathbb{R}[X]$ tel que : $P = AQ$.

Alors : $\lambda P = \lambda(AQ) = A(\lambda Q)$. Or $\lambda Q \in \mathbb{R}[X]$, donc λP est un multiple de A, donc : $\lambda P \in F$.

F contient 0, est stable par addition et par multiplication scalaire. Donc : F est un sous-espace vectoriel de $\mathbb{R}[X]$

2. Trouver un supplémentaire (complément) de Fdans $\mathbb{R}[X]$.

On sait :

- $A \in \mathbb{R}[X]$ un polynôme non nul et $F = \{P \in \mathbb{R}[X] \mid A \text{ divise } P\}$.
- F est un sous-espace vectoriel de $\mathbb{R}[X]$.

Objectif : Trouver un sous-espace G tel que : $\mathbb{R}[X] = F \oplus G$.

Cela veut dire deux choses :

1. $\mathbb{R}[X] = F + G$: tout polynôme s'écrit $P = f + g$ avec $f \in F, g \in G$
2. $F \cap G = \{0\}$: cette décomposition est unique

1. Utiliser la division euclidienne par A

Soit $r = \deg(A)$.

Division euclidienne : $\forall P \in \mathbb{R}[X], \exists!\ (P, Q)$ tel que $\boldsymbol{P = AQ + R}$ avec $R = 0$ ou $\deg(R) < \deg(A) = r$

Q s'appelle le quotient et R s'appelle le reste

2. Choisir le candidat G

On prend l'ensemble de tous les "restes possibles" : $G = \{ R \in \mathbb{R}[X] \mid \deg(R) < r \}$.

C'est bien un sous-espace vectoriel : c'est l'ensemble des polynômes de degré $\leq r - 1$.

Il a pour base : $(1, X, X^2, \dots, X^{r-1})$.

3. Montrer que $\mathbb{R}[X] = F + G$

Soit $P \in \mathbb{R}[X]$. Par division euclidienne : $P = AQ + R$.

- $AQ \in F$ car A divise AQ
- $R \in G$ car $\deg(R) < r$

Donc P s'écrit comme somme d'un élément de F et d'un élément de G : $\mathbb{R}[X] \subset F + G$.

L'inclusion inverse $F + G \subset \mathbb{R}[X]$ est évidente (car $F \subset \mathbb{R}[X]$ et $G \subset \mathbb{R}[X]$).

Donc : $\mathbb{R}[X] = F + G$

4. Montrer que $F \cap G = \{0\}$

Soit $P \in F \cap G$.

- Comme $P \in F$, il existe $Q \in \mathbb{R}[X]$ tel que $P = AQ$.
- Comme $P \in G$, on a $\deg(P) < r = \deg(A)$.

Supposons $P \neq 0$. Alors $Q \neq 0$: $\deg(P) = \deg(AQ) = \deg(A) + \deg(Q) \geq \deg(A) = r$.

Donc $\deg(P) \geq r$.

Mais en même temps $P \in G$ impose $\deg(P) < r$. Contradiction.

Donc on ne peut pas avoir $P \neq 0$. Ainsi : $P = 0$.

Donc : $F \cap G = \{0\}$

On a montré :

- $\mathbb{R}[X] = F + G$
- $F \cap G = \{0\}$

Donc : $\mathbb{R}[X] = F \oplus G$

Avec $G = \{R \in \mathbb{R}[X] \mid \deg(R) < \deg(A)\}$ qui est un complément de F dans $\mathbb{R}[X]$.