Chapitre 17 : Polynômes
Partie B : Arithmétique dans $\mathbb{K}[X]$

I) Divisibilité dans $\mathbb{K}[X]$

a) Aux polynômes rien de nouveaux

Définition : Soit $(P, Q) \in (\mathbb{K}[X])^2$. On dit que P divise Q si et seulement s'il existe $R \in \mathbb{K}[X]$ tel que $Q = P \times R$:

$$P|Q \iff \exists R \in \mathbb{K}[X], Q = P \times R$$

Exemple I.a.1 : Déterminer deux polynômes non constants qui divisent $X^2 - 1$ sur $\mathbb{R}[X]$.

Application I.a.2 : Déterminer tous les polynômes unitaires de degré 1 qui divise $X^6 - 1$ sur $\mathbb{C}[X]$.

b) Propriétés

Propriété I.b.1 : Soit $(P, Q, R) \in (\mathbb{K}[X])^3$. Si R divise P et R divise Q alors R divise toute combinaison linéaire de P et de Q :

$$\begin{cases} R|P \\ R|Q \end{cases} \Longrightarrow R|PA + QB, \forall (A, B) \in (\mathbb{K}[X])^2$$

Propriété I.b.2 : Soit $(A, B) \in (\mathbb{K}[X])^2$. Alors :

$$A|B \text{ et } B|A \iff \exists \lambda \in \mathbb{K}^*, A = \lambda B \iff A\mathbb{K}[X] = B\mathbb{K}[X]$$

On dit que A et B sont des polynômes associés.

c) Division euclidienne dans $\mathbb{K}[X]$

Propriété I.c.1 : Soit $(A, B) \in (\mathbb{K}[X])^2$ tels que $B \neq 0$. Alors, il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Les polynômes Q et R seront alors appelés le quotient et le reste dans la division euclidienne de A par B.

Exemple I.c.2 : Déterminer le quotient et le reste de la division euclidienne de :
$P(X) = X^3 + 2X^2 + X + 1$ par $B(X) = X^2 + 1$

Remarque : Il est parfois utile de seulement déterminer le reste de la division euclidienne.

Application I.c.3 : On pose : $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$. Calculer $A^2 - 5A + 4I_3$ puis en déduire A^n.

Application I.c.4 : Déterminer le reste de la division euclidienne de X^n par $X^2 - 2\cos(\theta) X + 1$.

Remarque : On a bien entendu $A|B$ si et seulement si le reste de la division euclidienne de A par B est nul.

II) Dérivation sur $\mathbb{K}[X]$

a) Cela tombe sous le sens !

Définition : Soit $P(X) = a_0 + a_1X + \cdots + a_nX^n$. On définit P′ la dérivée formelle de P par :

$$P'(X) = a_1 + 2a_2X + 3a_3X^3 + \cdots + na_nX^{n-1}$$

$$P(X) = \sum_{k=0}^{n} a_kX^k \Longrightarrow P'(X) = \sum_{k=1}^{n} ka_kX^{k-1}$$

Exemple II.a.1 : Déterminer la dérivée de $P(X) = X^5 + 4X^3 + 5X^2 + 1$

b) Propriétés

Propriété II.b.1 : Soient $(P, Q) \in (\mathbb{K}[X])^2$. On a :
(1) On a $P' = 0 \Leftrightarrow P$ est constant.
(2) Si $\deg(P) \geq 1$, on a $\deg(P') = \deg(P) - 1$.
(3) La dérivation est linéaire : $\forall(\lambda, \mu) \in \mathbb{K}^2, (\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
(4) $(P \times Q)' = P' \times Q + P \times Q'$.
(5) $(P o Q)' = Q' \times (P' o Q)$.

Définition (Dérivée n-ième) : Soit $P \in \mathbb{K}[X]$. On définit le polynôme $P^{(n)}$ comme étant l'itération n fois de la dérivation. On note $P^{(0)} = P$ par convention.

Exemple II.b.2 : On pose $P(X) = X^n$. Déterminer $P^{(k)}$ pour tout k entier naturel.

Propriété II.b.3 : Soit $P \in \mathbb{K}[X]$. On a :
(1) $P^{(k)} = 0$ dès que $\deg(P) < k$.
(2) $\forall(\lambda, \mu) \in \mathbb{R}^2$ et $n \in \mathbb{N}, (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$

Propriété II.b.4 (Formule de Leibniz) :

$$\forall(P, Q) \in (\mathbb{K}[X])^2, (P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$$

Application II.b.5 : $\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, f_n(x) = x^n(1 + x)^n$
1) Déterminer de deux manières différentes le terme dominant de $f_n^{(n)}$.
2) En déduire la valeur de :

$$S_n = \sum_{k=0}^{n} \binom{n}{k}^2$$

Propriété II.b.6 (Formule de Taylor) :

$$\forall P \in \mathbb{K}[X], P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(x - a)^k$$

III) Racine d'un polynôme

a) $P(a) = 0$

Définition : Soit $P \in \mathbb{K}[X]$. On dit que $a \in \mathbb{K}$ est une racine de P si et seulement si $P(a) = 0$.

Exemple III.a.1 : Déterminer les racines de $P(X) = X^3 - 1$ dans $\mathbb{C}$.

Application III.a.2 : Montrer qu'un polynôme de $\mathbb{R}[X]$ qui admet une racine complexe z_0 admet aussi comme racine son conjugué $\overline{z_0}$.

b) Propriétés

Propriété III.b.1 : a est racine d'un polynôme P si et seulement si $(X - a)$ divise P :

$$P(a) = 0 \Leftrightarrow (X - a)|P$$

Application III.b.2 : Déterminer les racines de $P(X) = X^3 - X + 6$.

Propriété III.b.3 : $a_1, \dots, a_n$ sont racines d'un polynôme P si et seulement si $(X - a_1) \dots (X - a_n)$ divise P :

$$\forall i \in [\![1, n]\!], P(a_i) = 0 \Leftrightarrow \prod_{i=1}^{n} (X - a_i) \mid P$$

Propriété III.b.4 : Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines distinctes.
Seul le polynôme nul admet une infinité de racine.

Application III.b.5 : Soit $(P, Q) \in (\mathbb{K}[X])^2$. Montrer que :

$$\forall n \in \mathbb{N}, P(2^n) = Q(2^n) \Longrightarrow P = Q$$

c) Multiplicité d'une racine

Propriété III.c.1 : Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On a :

$$(X - a)^r \mid P \iff P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$$

On dit alors que a est racine de P d'ordre de multiplicité au moins r.

Exemple III.c.2 : On pose : $P(X) = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$
Montrer que 1 est racine de P d'ordre de multiplicité au moins 3.

Propriété III.c.3 : Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On a équivalence entre :
$(1) \exists Q \in \mathbb{K}[X], P(X) = (X - a)^r Q(a)$ avec $Q(a) \neq 0$
(2) $(X - a)^r \mid P(X)$ et $(X - a)^{r+1} \nmid P(X)$
$(3) P(a) = P'(a) = P''(a) = \cdots = P^{(r-1)}(a) = 0$ et $P^{(r)}(a) \neq 0$

Application III.c.4 : Déterminer les racines de $P(X) = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$.

Propriété III.c.5 : Soient $P \in \mathbb{K}[X]$, $(a_1; \dots; a_n) \in \mathbb{K}^n$ et $(r_1; \dots; r_n) \in \mathbb{N}^n$. On a alors :
$\forall i \in [\![1; n]\!], a_i$ est racine de P de multiplicité au moins $r_i \iff (X - a_1)^{r_1} \dots (X - a_n)^{r_n} \mid P$

Remarque : On a ainsi le résultat suivant :
Un polynôme de degré n admet au plus n racines comptées avec leurs ordres de multiplicité.