6.4 Divisibilité des polynômes

6.4.1 Définition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
On dit qu'un polynôme $A \in \mathbb{K}[X]$ est **divisible** par $B \in \mathbb{K}[X]$, ou que B divise A ou que B est un diviseur de A ou que A est **un multiple** de B s'il existe $C \in \mathcal{A}[X]$ tel que $A = BC$
On note $B \div A$

Remarque 10 :

1. L'ensemble $\{BQ \text{ où } Q \in \mathbb{K}[X]\}$ est l'ensemble des multiples de B. On le note $B \times \mathbb{K}[X]$
2. Ainsi, $B \div A \iff A \in B \times \mathbb{K}[X]$

Exemple 2 :

1. Tout polynôme divise 0. En effet, pour tout $P \in \mathbb{K}[X]$, $0 = 0 \times P$; donc $P \div 0$ et 0 ne divise que le polynome nul ; tout ceci présente peu d'intérêt
2. Si $\mathbb{K}$ est un corps et $A \in \mathbb{K}[X]$, alors, tout $\lambda \in \mathbb{K}^*$ divise tout élément $A \in \mathbb{K}[X]$ puisque $A = \lambda \times \left(\frac{1}{\lambda} A\right)$
3. Nous avons $\left(X^2+1\right) \div \left(X^3 - X^2 + X - 1\right)$ puisque $\left(X^3 - X^2 + X - 1\right) = (X-1)\left(X^2+1\right)$

6.4.2 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.

1. La relation de divisibilité est **réflexive**, c'est à dire que pour tout $A \in \mathbb{K}[X]$, $A \div A$
2. La relation de divisibilité est **transitive**, c'est à dire que pour tout $A \in \mathbb{K}[X]$, tout $B \in \mathbb{K}[X]$ et tout $C \in \mathbb{K}[X]$, si $A \div B$ et $B \div C$ alors $A \div C$

Démonstration

La démonstration est simple et laissée au lecteur.

6.4.3 Polynômes associés

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Si $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ se divisent l'un l'autre, c'est à dire si $A \div B$ et $B \div A$ alors $A = \lambda B$ où $\lambda \in \mathbb{K}$.
On dit que A et B sont des polynômes associés

Démonstration

Effectivement, si $A = BC$ et si $B = AC'$, alors $\deg A = \deg B + \deg C$ et $\deg B = \deg A + \deg C'$, c'est à dire que nous avons

$$\deg A = (\deg A + \deg C') + \deg C \iff \deg C' + \deg C = 0$$

Comme nous sommes dans $\mathbb{N}$, alors $\deg C' = \deg C = 0$, c'est à dire que C et C' sont des polynômes constants.

Exemple 3 :

Si $\mathbb{K}$ est un corps, alors, dans $\mathbb{K}[X]$, tout polynôme non nul est associé à un polynôme unitaire et un seul.

En effet, soit $P=\sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$, alors $P = a_n\left(\sum_{k=0}^{n} \frac{a_k}{a_n} X^k\right) = a_n\left(X^n + \sum_{k=0}^{n-1} \frac{a_k}{a_n} X^k\right)$.

En posant $P' = X^n + \sum_{k=0}^{n-1} \frac{a_k}{a_n} X^k$, P' est unitaire et $P = a_n P' \iff P' = \frac{1}{a_n} P$, et P et P' sont associés.

6.4.4 Premières propriétés de la divisibilité

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.

1. Pour tout $A \in \mathbb{K}[X]$, tout $B \in \mathbb{K}[X]$ avec $B \neq 0$, si $B \div A$, alors $\deg B \leqslant \deg A$
2. Pour tout $A \in \mathbb{K}[X]$, tout $B \in \mathbb{K}[X]$ et tout $\lambda \in \mathbb{K}^*$, nous avons :
$$A \div B \iff (\lambda A) \div B$$
3. Pour tout $A \in \mathbb{K}[X]$, tout $B \in \mathbb{K}[X]$ et tout $C \in \mathbb{K}[X]$, $B \div A \Longrightarrow B \div AC$
4. Pour tout $A \in \mathbb{K}[X]$, tout $B \in \mathbb{K}[X]$ et tout $C \in \mathbb{K}[X]$ $(A \div B$ et $A \div C) \Longrightarrow A \div (B+C)$

Démonstration

La démonstration est simple et peut être vue comme un exercice corrigé

1. Si B divise A et si $B \neq 0$, alors $A = BC$ et, parce que $\mathbb{K}$ est intègre, $\deg A = \deg B + \deg C$ et donc $\deg B \leqslant \deg A$
2. Supposons $A \div B$.
   Il existe donc $Q \in \mathbb{K}[X]$ tel que $B = AQ$ et donc, pour tout $\lambda \in \mathbb{K}^*$, nous avons $B = (\lambda A)\left(\frac{1}{\lambda} Q\right)$.
   Nous avons bien $(\lambda A) \div B$
3. Si $B \div A$, il existe alors $Q \in \mathbb{K}[X]$ tel que $A = BQ$ et donc, pour tout $C \in \mathbb{K}[X]$, $AC = BQC \iff AC = B(QC)$, et donc $B \div AC$
4. Si $A \div B$ et $A \div C$, alors il existe $Q_1 \in \mathbb{K}[X]$ et $Q_2 \in \mathbb{K}[X]$ tels que $B = Q_1 A$ et $C = Q_2 A$ et donc $B + C = Q_1 A + Q_2 A = A(Q_1 + Q_2)$ et donc $A \div (B+C)$

Remarque 11 :

On ne peut que constater une analogie avec la division dans l'ensemble $\mathbb{Z}$

6.4.5 Définition

Soit $\mathcal{A}$ un anneau commutatif unitaire et $P \in \mathcal{A}[X]$
Un élément $c \in \mathcal{A}$ est appelé zéro ou racine du polynôme P si et seulement si $\widetilde{P}(c) = 0$

Remarque 12 :

1. La fonction polynôme $\widetilde{P}$ a été définie en 6.2.4
2. Pour plus de généralité, la définition a été donnée dans un anneau $\mathcal{A}$ et son anneau de polynôme $\mathcal{A}[X]$.
3. Soit $\mathbb{L}$ un corps tel que $\mathbb{K} \subset \mathbb{L}$.
   Si $P \in \mathbb{K}[X]$, alors, nous avons aussi $P \in \mathbb{L}[X]$, et si $\alpha \in \mathbb{L}$, nous pouvons avoir $P(\alpha) = 0$
   Exemple :
   Le polynôme $X^2 - 2$ n'a aucune racine dans $\mathbb{Q}$, mais en a 2 dans $\mathbb{R}$
   De même, le polynôme $X^2 + 1$ n'a aucune racine dans $\mathbb{R}$, mais en a 2 dans $\mathbb{C}$

Exercice 6 :

Soit $\mathcal{A}$ un anneau commutatif unitaire intègre et $P \in \mathcal{A}[X]$. Soient $f \in \mathcal{A}[X]$ et $g \in \mathcal{A}[X]$ tels que $P = fg$, c'est à dire tels que P soit le produit des 2 polynômes f et g. Démontrer que $\alpha \in \mathcal{A}$ est une racine de P si et seulement si α est une racine de f ou de g *Cet exercice ne fait pas l'objet d'une correction*

6.4.6 Théorème

Soit $\mathcal{A}$ un anneau commutatif unitaire
$P \in \mathcal{A}[X]$ est divisible par le polynôme unitaire du premier degré $(X - c)$ si et seulement si, c est une racine *(ou zéro)* de P

Démonstration

1. Supposons que c soit un zéro de P et faisons la division euclidienne de P par $(X - c)$. Nous avons alors :
$$P(X) = Q(X)(X - c) + R(X) \text{ avec } \deg R < 1$$
C'est à dire $\deg R = 0$ et donc R est constant. Alors $P(c) = R = 0$, ce qui veut dire que $P(X) = Q(X)(X - c)$ et donc P est divisible par $(X - c)$
2. Réciproquement, il est bien sûr évident que si P est divisible par $(X - c)$, alors $P(c) = 0$

Remarque 13 :

1. Remarquons que nous venons de faire un abus de langage en identifiant $P(c)$ et $\widetilde{P}(c)$, ce que nous ferons volontiers dorénavant.
2. Si $P \in \mathbb{K}[X]$ a une racine dans $\mathbb{K}$, alors P est réductible dans $\mathbb{K}[X]$, mais la réciproque est fausse :
Exemple :
Le polynôme $Q(X) = \left(X^2 + 1\right)^2$ est réductible dans $\mathbb{R}[X]$, puisque $Q(X) = \left(X^2 + 1\right)\left(X^2 + 1\right)$, mais n'a aucune racine dans $\mathbb{R}$

Exercice 7 :

Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$.
Soient
- $A = X^2 - 2X\cos\theta + 1$,
- $P_n = X^n \sin\theta - X \sin n\theta + \sin(n-1)\theta$
- $Q_n = X^{n+1}\cos(n-1)\theta - X^n \cos n\theta - X\cos\theta + 1$

Démontrer que A divise P_n et que A divise Q_n

Exercice 8 :

1. Soient $A \in \mathbb{K}[X]$ et $A \in \mathbb{K}[X]$. Nous désignons par Q et R le quotient et le reste de la division euclidienne de A par B.
Montrer que les racines communes à A et B sont les racines communes à B et R
2. Résoudre les équations $A(x) = 0$ et $B(x) = 0$ avec
$$A(X) = X^4 - 3X^3 - 7X^2 + 27X - 18 \text{ et } B(X) = X^3 - 12X^2 + 47X - 60$$
sachant que A et B ont des racines communes

6.4.7 Théorème

Soit $\mathcal{A}$ un anneau commutatif unitaire
Soient $P \in \mathcal{A}[X]$, $\alpha \in \mathcal{A}$ et $n \in \mathbb{N}$. Les conditions suivantes sont équivalentes :
1. P est divisible par $(X - \alpha)^n$, mais pas par $(X - \alpha)^{n+1}$
2. $P(X) = (X - \alpha)^n Q(X)$ où $Q \in \mathcal{A}[X]$ est un polynôme tel que $Q(\alpha) \neq 0$

On dit alors que α est une racine d'ordre n ou de multiplicité n

Démonstration

1. Supposons P est divisible par $(X-\alpha)^n$, mais pas par $(X-\alpha)^{n+1}$
   Alors, $P(X) = (X-\alpha)^n Q(X)$.
   Si $Q(\alpha) = 0$, alors Q est divisible par $(X-\alpha)$ et alors $Q(X) = (X-\alpha) Q_1(X)$, ce qui veut dire que $P(X) = (X-\alpha)^{n+1} Q_1(X)$.
   Il y a donc contradiction et $Q(\alpha) \neq 0$
2. Supposons $P(X) = (X-\alpha)^n Q(X)$ où $Q \in \mathcal{A}[X]$ est un polynôme tel que $Q(\alpha) \neq 0$
   Nous allons démontrer que P n'est pas divisible par $(X-\alpha)^{n+1}$.
   Supposons le contraire, c'est à dire que $P(X) = (X-\alpha)^{n+1} Q_1(X)$; alors, nous avons $Q(X) = (X-\alpha) Q_1(X)$ et donc $Q(\alpha) = 0$, ce qui est contraire à l'hypothèse.

6.4.8 Corollaire

Soit $\mathcal{A}$ un anneau commutatif unitaire et $P \in \mathcal{A}[X]$
Soient $x_1, x_2, \ldots, x_p$ p racines distinctes de P d'ordre respectif $n_1, \ldots, n_p$.
Alors, $P(X) = (X-\alpha_1)^{n_1} (X-\alpha_2)^{n_2} \cdots (X-\alpha_p)^{n_p} Q(X)$ où $Q \in \mathcal{A}[X]$ est un polynôme n'addmettant pas pour racines $x_1, x_2, \ldots, x_p$

Démonstration

Elle est évidente

Exercice 9 :

Trouver $a \in \mathbb{C}$ pour que $P(X) = X^5 + aX^4 + aX + 1$ admette 1 comme racine double

6.4.9 Corollaire

Soit $\mathcal{A}$ un anneau commutatif unitaire et intègre
Alors un polynôme $P \in \mathcal{A}[X]$ de degré n a au plus n racines dans $\mathcal{A}$

Démonstration

Nous allons faire cette démonstration de deux façons.

1. Pour la première démonstration, nous supposons que P admette $(n+1)$ racines $x_1, x_2, \ldots, x_n, x_{n+1}$.
   Alors $P(X) = (X-x_1)(X-x_2)\cdots(X-x_n)(X-x_{n+1}) Q(X)$, et donc, $\deg P \geqslant n+1$; il y a une contradiction et donc P admet au plus n racines dans $\mathcal{A}$
2. Nous faisons la seconde démonstration par récurrence sur le degré de P.
   (a) Si le degré de P est 1, c'est à dire si $P(X) = aX + b$
   - ▷ Si a n'est pas inversible dans $\mathcal{A}$, alors P n'a pas de racine dans $\mathcal{A}$
   - ▷ Si a est inversible dans $\mathcal{A}$, alors $c = -a^{-1}b$ est une racine de P, et P n'a que cette racine dans $\mathcal{A}$

   Ainsi, si $\deg P = 1$, P a au plus 1 racine dans $\mathcal{A}$
   (b) Supposons que $P \in \mathcal{A}[X]$ de degré n a au plus n racines dans $\mathcal{A}$
   (c) Soit $P \in \mathcal{A}[X]$ de degré $n+1$
   - ▷ P peut n'avoir aucune racine dans $\mathcal{A}$; il a donc 0 racine.
   - ▷ Supposons que P admette une racine $c \in \mathcal{A}$.
     Alors, P est divisible par $(X-c)$ et nous avons $P(X) = Q(X)(X-c)$.
     $\mathcal{A}$ étant un anneau intègre, nous avons $\deg P = \deg Q + 1 \iff \deg Q = n$ et donc, comme $\deg Q = n$,d'après l'hypothèse de récurrence, Q admet au plus n racines dans $\mathcal{A}$, et ainsi P admet au plus $n+1$ racines dans $\mathcal{A}$

   Le théorème est ainsi démontré.