6.6 Polynômes irréductibles

6.6.1 Définition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible si et seulement si :

1. $\deg P \geqslant 1$
2. Tout diviseur de P est 1 ou bien est associé à P

Remarque 21 :

1. Autrement dit : $P \in \mathbb{K}[X]$ est irréductible si $\deg P \geqslant 1$ et tout diviseur de P est de la forme λP où $\lambda \in \mathbb{K}^*$
2. On peut remplacer la seconde condition par :

   Il n'existe pas de diviseurs Q de P tels que $0 < \deg Q < \deg P$

   Notons bien que nous écartons les polynômes constants
3. **Vocabulaire** : On dit aussi qu'un polynôme non irréductible est un polynôme réductible ou factorisable.

Exemple 7 :

1. Tout polynôme de degré 1 est irréductible
2. Tout polynôme associé à un polynôme irréductible est lui-même irréductible
3. L'irréductibilité **dépend du corps de base**

   En effet :
   - ▷ Le polynôme X^2+1 est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$
   - ▷ De même,polynôme X^2-2 est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{R}[X]$
4. On voit bien que la réductibilité est liée à l'existence ou non de racine dans le corps $\mathbb{K}$. On peut cependant avoir des polynômes réductibles ou factorisables sans qu'il y ait de racines dans ce corps $\mathbb{K}$

   Exemple : $P(X) = X^4+6X^2+9 = \left(X^2+3\right)^2 = \left(X^2+3\right)\left(X^2+3\right)$ est donc réductible dans $\mathbb{R}$, sans que P admette de racines dans $\mathbb{R}$

6.6.2 Proposition

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Soit $P \in \mathbb{K}[X]$ tel que $\deg P \geqslant 2$

1. Si P est irréductible, alors P n'a pas de racine dans $\mathbb{K}$
2. Si $\deg P = 2$ ou $\deg P = 3$ et si P n'a pas de racine dans $\mathbb{K}$, alors P est irréductible

Démonstration

Comme souvent, cette proposition peut être vue comme un exercice résolu

1. Pour le premier point, nous allons faire une démonstration par contraposée :
   Supposons que P admette une racine $\alpha \in \mathbb{K}$; alors P est divisible par $X-\alpha$ et $P = (X-\alpha)Q$ avec $\deg Q = \deg P - 1$.
   P n'est donc pas irréductible
2. Soit $P \in \mathbb{K}[X]$ tel que $\deg P = 2$ ou $\deg P = 3$ et supposons que P soit réductible, c'est à dire qu'il 2 polynômes $f \in AX$ et $g \in \mathcal{A}[X]$ avec $\deg f \geqslant 1$ et $\deg g \geqslant 1$ tels que $P = fg$.
   De l'identité $\deg P = \deg f + \deg g$, nous obtenons :
   - ▷ Si $\deg P = 2$, alors $\deg f = \deg g = 1$ alors f et g admettent chacun une racine dans $\mathbb{K}$, et donc P admet des racines dans $\mathbb{K}$

▷ Maintenant, si $\deg P = 3$, alors ou bien $\deg f = 1$ et $\deg g = 2$ ou bien $\deg f = 2$ et $\deg g = 1$. Dans chacun des 2 cas cités, il y a un polynôme de degré 1. Supposons, par exemple, que $\deg f = 1$. Alors f admet une racine dans $\mathbb{K}$, et donc P admet une racines dans $\mathbb{K}$

Nous avons donc démontré, toujours par contraposée, le second point

Remarque 22 :

1. Dans $\mathbb{R}[X]$, tous les polynômes de dégré 3 sont réductibles, puisque l'analyse montre qu'ils ont forcément une racine réelle
2. Il n'est pas difficile de démontrer que, dans $\mathbb{Q}[X]$, il existe des polynômes irréductibles de tout degré

6.6.3 Proposition

Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ tels que Q soit un polynôme irréductible.
Alors :
▷ Ou bien Q est premier avec P
▷ Ou bien Q divise P

Démonstration

Soit D le PGCD de P et Q que nous avons choisi unitaire. C'est à dire $D = \text{pgcd}(P, Q)$.
Le polynôme D est donc un polynôme unitaire et il divise Q. Or Q est irréductible et donc, d'après la définition 6.6.1

→ Ou bien D est le polynôme constant égal à 1 et P et Q sont premiers entre eux,
→ Ou bien D est de la forme λQ, où λ est une constante non nulle *(égale à l'inverse du coefficient dominant de Q)*. Alors, dans ce dernier cas, on en déduit que Q divise P.

Ce qui achève la démonstration.

6.6.4 Corollaire

Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ tels que P et Q soient irréductibles. Alors P et Q sont premiers entre eux ou associés

Démonstration

D'après la proposition précédente 6.6.3, ou bien Q est premier avec P ou bien Q divise P.
Si Q divise P, alors, P n'est pas irréductible. Donc, P et Q sont premiers entre eux ou associés, c'est à dire $Q = \lambda P$ où $\lambda \in \mathbb{K}^*$

6.6.5 Polynôme irréductible divisant un produit

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Soient $P \in \mathbb{K}[X]$, $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$, avec P irréductible sur $\mathbb{K}[X]$.
Si le polynôme P divise le produit AB, alors P divise A ou P divise B.
Autrement dit si un polynôme irréductible divise un produit de polynômes, il divise l'un des polynômes.

Démonstration

La démonstration de cette proposition est basée sur le théorème de Gauss 6.5.14.
Soit donc P un polynôme irréductible divisant le produite AB
Supposons que P ne divise pas le polynôme A. Alors d'après la proposition précédente 6.6.3, il est premier avec A.
On peut donc appliquer le théorème de Gauss et conclure que P divise B.

Remarque 23 :

Par récurrence, on peut démontrer que si P irréductible sur $\mathbb{K}[X]$ divise un produit $A_1A_2\cdots A_n$ de polynômes de $\mathbb{K}[X]$, alors, P divise l'un des polynômes A_i

6.6.6 Théorème

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Tout polynôme $P \in \mathbb{K}[X]$ de degré supérieur ou égal à 1 possède un diviseur irréductible.

Démonstration

Soit $P \in \mathbb{K}[X]$ un polynôme non constant, c'est à dire tel que $\deg P \geqslant 1$.
On appelle E l'ensemble des diviseurs non constants de P
E n'est pas vide puisqu'il contient P lui-même.
On en déduit que la partie $\Omega \subset \mathbb{N}$ dont les éléments sont les degrés des éléments de E n'est pas vide.
Toute partie de $\mathbb{N}$ non vide possédant un plus petit élément, Ω, non vide, possède donc un plus petit élément noté n_0. Il existe donc un élément de E, noté P_0 de degré n_0 qui est donc un diviseur non constant de P.
Montrons qu'alors P_0 est irréductible.
En effet, si P_0 n'était pas irréductible, il aurait un diviseur Q, non constant, de degré strictement plus petit. Ce diviseur serait aussi un diviseur de P, et son degré serait donc strictement plus petit que n_0.
Ce qui est en contradiction avec la définition de l'entier n_0

6.6.7 Théorème

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ son anneau de polynômes.
Tout polynôme $P \in \mathbb{K}[X]$ se décompose de manière unique sous la forme

$$P = \lambda \prod_{i=1}^{k} (P_i)^{\alpha_i}$$

Où les P_i sont des polynômes unitaires irréductibles de $\mathbb{K}[X]$, $\lambda \in \mathbb{K}^*$ et $\alpha_i \in \mathbb{N}^*$

Démonstration

La démonstration se fera, par récurrence, sur le degré de P

1. Si $\deg P = 0$, cela veut dire que P est un polynôme constant ; alors $P = \lambda \prod_{i=1}^{k} (P_i)^0 = \lambda$
2. Supposons que, si $\deg P \leqslant n$, alors P se décompose de manière unique sous la forme
$$P = \lambda \prod_{i=1}^{k} (P_i)^{\alpha_i}$$
3. Soit, maintenant, $P \in \mathbb{K}[X]$, réductible, de degré $n+1$.
$\Longrightarrow$ Montrons l'existence
D'après le théorème 6.6.6, P admet au moins un diviseur irréductible ; appelons le P_0. Donc $P = P_0 \times Q$ où $Q \in \mathbb{K}[X]$ et $\deg Q \leqslant n$ puisque $\deg P_0 \geqslant 1$.
D'après l'hypothèse de récurrence, Q se décompose de manière unique sous la forme
$$Q = \lambda \prod_{i=1}^{k} (Q_i)^{\alpha_i}$$
Et donc $P = P_0 \times \left(\lambda \prod_{i=1}^{k} (Q_i)^{\alpha_i}\right) = \lambda \times P_0 \times \left(\prod_{i=1}^{k} (Q_i)^{\alpha_i}\right)$
L'existence est donc prouvée

$\Longrightarrow$ Montrons l'unicité

Supposons donc que P admette 2 décompositions en polynômes irréductibles unitaires

$$P = \lambda \prod_{i=1}^{k} (P_i)^{\alpha_i} = \mu \prod_{i=1}^{k_1} (Q_i)^{\beta_i}$$

Les P_i et les Q_i étant unitaires, λ et μ représentent le coefficient du terme de plus haut de degré de P et donc $\lambda = \mu$, ce qui nous permet de simplifier et donc d'écrire

$$\prod_{i=1}^{k} (P_i)^{\alpha_i} = \prod_{i=1}^{k_1} (Q_i)^{\beta_i}$$

Et, en ne tenant pas compte de leur multiplicité :

$$P_1 \times P_2 \times \cdots \times P_r = Q_1 \times Q_2 \times \cdots \times Q_s \Longleftrightarrow P_1 \times (P_2 \times \cdots \times P_r) = Q_1 \times Q_2 \times \cdots \times Q_s$$

P_1, irréductible, divise le produit $Q_1 \times Q_2 \times \cdots \times Q_s$ et donc, d'après 6.6.5, divise l'un des Q_i.
Quitte à ré-arranger les polynômes, on peut supposer que P_1 divise Q_1.
Q_1 étant irréductible, nous en déduisons qu'ils sont associés ; mais comme P_1 et Q_1 sont unitaires, nous avons $P_1 = Q_1$.
Nous pouvons, alors, dans l'expression $P_1 \times P_2 \times \cdots \times P_r = Q_1 \times Q_2 \times \cdots \times Q_s$, simplifier par P_1 et nous obtenons $P_2 \times \cdots \times P_r = Q_2 \times \cdots \times Q_s$
En posant $g = P_2 \times \cdots \times P_r = Q_2 \times \cdots \times Q_s$, nous avons 2 décompositions en polynômes irréductibles d'un polynôme g tel que $\deg g \leqslant n$.
D'après l'hypothèse de récurrence, cette décomposition est unique.

Nous venons donc de montrer que tout polynôme $P \in \mathbb{K}[X]$ se décompose de manière unique sous la forme $P = \lambda P_1 \times P_2 \times \cdots \times P_r$ où les P_i sont des polynômes unitaires irréductibles de $\mathbb{K}[X]$, $\lambda \in \mathbb{K}^*$.

6.6.8 Proposition

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

Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ 2 polynômes tels que $P = \lambda \prod_{i=1}^{k} (P_i)^{\alpha_i}$ et $Q = \mu \prod_{i=1}^{k} (P_i)^{\beta_i}$ *(On peut avoir* $\alpha_i = 0$ *ou* $\beta_i = 0$*)* avec $\lambda \in \mathbb{K}^*$ et $\mu \in \mathbb{K}^*$

Alors, pour que P divise Q, il faut et il suffit que $\alpha_i \leqslant \beta_i$ pour tout i

Démonstration

1. Supposons que $\alpha_i \leqslant \beta_i$ pour tout i.
   Alors,
   $$\begin{aligned} Q = & \mu \prod_{i=1}^{k} (P_i)^{\beta_i} = \mu \prod_{i=1}^{k} (P_i)^{\beta_i - \alpha_i + \alpha_i} = \lambda \prod_{i=1}^{k} (P_i)^{\alpha_i} \times \frac{\mu}{\lambda} \prod_{i=1}^{k} (P_i)^{\beta_i - \alpha_i} \\ = & P \times R \end{aligned}$$
   Et donc, P divise bien Q
2. Réciproquement, supposons que P divise Q.
   Il existe alors $R \in \mathbb{K}[X]$ tel que $Q = P \times R$ et $R = \frac{\mu}{\lambda} \prod_{i=1}^{k} (P_i)^{\gamma_i}$, avec éventuellement $\gamma_i = 0$.
   Alors, $P \times R = \mu \prod_{i=1}^{k} (P_i)^{\alpha_i + \gamma_i}$ et donc $\alpha_i + \gamma_i = \beta_i$ d'où $\alpha_i \leqslant \beta_i$
   Ce que nous voulions

6.6.9 Corollaire

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

Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ 2 polynômes unitaires tels que $P = \prod_{i=1}^{k} (P_i)^{\alpha_i}$ et $Q = \prod_{i=1}^{k} (P_i)^{\beta_i}$ *(On peut avoir $\alpha_i = 0$ ou $\beta_i = 0$)*

Alors :

1. $D = \text{pgcd}(P, Q) = \prod_{i=1}^{k} (P_i)^{\inf(\alpha_i, \beta_i)}$
2. $M = \text{ppcm}(P, Q) = \prod_{i=1}^{k} (P_i)^{\sup(\alpha_i, \beta_i)}$

Remarque 24 :

Soient $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ sont des polynômes unitaires.
Si $D = \text{pgcd}(P, Q)$ et $M = \text{ppcm}(P, Q)$, alors $DM = PQ$