Polynômes

Dans ce chapitre la lettre $\mathbb{K}$ désignera indifféremment $\mathbb{R}$ ou $\mathbb{C}$. Les lettres n et p désignent des entiers naturels.

Définition

On dit qu'un polynôme de degré n est scindé sur $\mathbb{K}$ s'il admet exactement n racines comptées avec leur multiplicité dans $\mathbb{K}$

Exemple

- Le polynôme $P = X^4 - 1$ est scindé sur $\mathbb{C}$. Il admet $1, -1, i, -i$ comme racines. Il peut donc s'écrire

$$P = (X - 1)(X + 1)(X - i)(X + i)$$

- De manière générale, le polynôme $P = X^n - 1$ s'écrit :

$$P = \prod_{k=0}^{n-1} (X - e^{\frac{i2k\pi}{n}})$$

En effet les n racines de l'unité : $e^{\frac{i2k\pi}{n}}$ avec $k \in \{0, 1, 2, \dots, n-1\}$ sont racines de P .

Théorème

Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Preuve

Par récurrence sur le degré du Polynôme.

Initialisation : $n = 1$. Tout polynôme de degré 1 est scindé.

Hérédité : Supposons que tout polynôme de degré $\leq n$ soit scindé. Soit P un polynôme de degré $n + 1$

Le théorème d'Alembert Gauss nous dit que ce polynôme admet sur $\mathbb{C}$ une racine α .

P peut donc s'écrire $P = (X - \alpha)Q$ avec $\deg(Q) = n$. L'hypothèse de récurrence s'applique donc à Q . Q est scindé donc P est scindé.

Remarque

- Il découle du théorème précédent que les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Le fait que tout polynôme de $\mathbb{C}[X]$ soit scindé implique que tout polynôme de $\mathbb{C}[X]$ peut s'écrire sous la forme $P = K(X - \alpha_1)^{n_1} \dots (X - \alpha_p)^{n_p}$ K étant un complexe, les α_i étant les racines de P , les n_i étant leur multiplicité. Cette décomposition est unique. En effet elle détermine le nombre de racines et leur multiplicité.

Les Propriétés

Soit P et Q deux polynômes. $P|Q$ dans $\mathbb{C}[X]$ ssi les racines de P sont aussi des racines de Q et leurs multiplicités dans P sont inférieures à leurs multiplicités dans Q

Preuve

Soient P et Q deux polynômes dont les racines de P sont aussi des racines de Q et leurs multiplicités dans P sont inférieures à leurs multiplicités dans Q . P et Q sont scindés donc :

Soit $P = K(X - \alpha_1)^{n_1} \dots (X - \alpha_p)^{n_p}$ et $Q = K'(X - \alpha_1)^{m_1} \dots (X - \alpha_p)^{m_p} (X - \beta_1)^{l_1} \dots (X - \beta_r)^{l_r}$ avec K et K' complexes, $m_1 \geq n_1 \dots m_p \geq n_p$ et tous les β_i distincts des α_i Alors nous avons bien $Q = K''P (X - \alpha_1)^{m_1 - n_1} \dots (X - \alpha_p)^{m_p - n_p}$

Avec K'' complexe

P divise bien Q

Réciproquement supposons $P|Q$

Soit α une racine de P de multiplicité n . Nous avons $(X - \alpha)^n | P$ donc $(X - \alpha)^n | Q$ donc α est une racine de Q de multiplicité au moins n

Propriété

Deux polynômes dans $\mathbb{C}[X]$ sont premiers si et seulement si ils n'ont aucune racine commune.

Preuve

Soient P et Q deux polynômes de $\mathbb{C}[X]$ avec $P \wedge Q = 1$. Nous savons d'après le théorème de Bezout que $\exists U$ et V dans $\mathbb{C}[X]$ tels que $PU + VQ = 1$. Supposons que ces deux polynômes aient une racine commune α .

Evaluons l'expression $PU + VQ = 1$ en α

Il vient $P(\alpha)U(\alpha) + V(\alpha)Q(\alpha) = 1 \Rightarrow 0 = 1$. Nous sommes donc bien arrivés à une contradiction. P et Q n'ont pas de racine commune.

Réciproquement. Supposons que P et Q soient deux polynômes sans racine commune. Soit R un diviseur commun de P et Q . D'après la propriété précédente toute racine de R soit aussi être racine de P et de Q . Nous en déduisons que R n'admet pas de racine. Sur $\mathbb{C}[X]$ cela implique $\deg(R) = 0$. Nous avons bien $P \wedge Q = 1$.

Propriété

Tout polynôme de $\mathbb{R}[X]$ peut s'écrire comme produit de polynômes du premier degré et de polynômes du second degré dont le discriminant est négatif.

Preuve

Soit P un polynôme de $\mathbb{R}[X]$. Il peut se décomposer dans $\mathbb{C}$ sous la forme

$$P = (X - \alpha_1)^{n_1} \dots (X - \alpha_p)^{n_p} (X - \beta_1)^{l_1} \dots (X - \beta_r)^{l_r}$$

En supposant les α_i réels et les β_j complexes.

Nous avons déjà démontré dans le chapitre sur les racines de polynôme que si β était une racine d'un polynôme de $\mathbb{R}[X]$ de multiplicité l alors $\bar{\beta}$ est aussi une racine de P de multiplicité l

P peut donc s'écrire $P = (X - \alpha_1)^{n_1} \dots (X - \alpha_p)^{n_p} (X - \beta_1)^{m_1} (X - \bar{\beta}_1)^{m_1} \dots (X - \beta_s)^{m_s} (X - \bar{\beta}_s)^{m_s}$

Or $(X - \beta_s)(X - \bar{\beta}_s) = X^2 - (\beta_s + \bar{\beta}_s)X + \beta_s\bar{\beta}_s$. C'est donc un polynôme du second degré à coefficients réels.

Son discriminant est strictement négatif. Sinon cela signifierait qu'il possède une racine réelle, or toutes les racines réelles ont déjà été comptabilisées dans les α_i .

Nous avons donc $P = (X - \alpha_1)^{n_1} \dots (X - \alpha_p)^{n_p} Q_1^{m_1} \dots Q_s^{m_s}$ avec les Q_i qui sont des polynômes du second degré à coefficients réels dont le discriminant est strictement négatif.

Remarques	<ul style="list-style-type: none"> • La décomposition dans $\mathbb{R}[X]$ est issue de celle dans $\mathbb{C}[X]$. La décomposition dans $\mathbb{C}[X]$ est unique. Celle dans $\mathbb{R}[X]$ aussi. • Ces décompositions permettent de présenter un polynôme sous la forme d'un produit d'éléments premiers. (c'est l'équivalent dans $\mathbb{R}$ de la décomposition d'un nombre en facteurs premiers). Ces polynômes sont dits des polynômes premiers. Ils ne sont divisibles que par eux même ou par un polynôme scalaire. • Ces décompositions permettent aussi de déterminer très facilement PGCD et PPCM d'un couple de polynômes.
Exemple	Si dans $\mathbb{C}[X]$, $P = (X - i)^2(X + i)$ et $Q = (X - i)(X + i)^2$ alors $P \wedge Q = (X - i)(X + i)$ et $P \vee Q = (X - i)^2(X + i)^2$