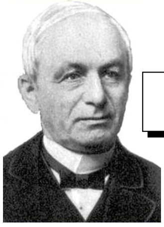

Théorème de Kronecker

Référence : FGNal1 : p. 213 + Szpirglas Mathématiques L3 Algèbre p. 573

Théorème

On définit
$$\Omega_n := \{P \in \mathbb{Z}[X] \mid P \text{ unitaire}, \deg P = n \text{ et } z \in Z(P) \Rightarrow 0 < |z| \leqslant 1\}$$
où $Z(P)$ désigne les racines complexes de P. Si $P \in \Omega_n$, alors les racines de P sont des racines de l'unité.

Preuve :

Montrons dans un premier temps que Ω_n est fini.
Soit $P \in \Omega_n$. On note $z_1, \ldots, z_n$ les racines de P et $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires de P évaluées en $(z_1, \ldots, z_n)$. On a $\sigma_p = \displaystyle\sum_{1 \leqslant i_1 < \cdots < i_p \leqslant n} z_{i_1} \ldots z_{i_p}$

Notons $P = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n = (X - z_1) \ldots (X - z_n)$.
A noter que $a_n \neq 0$ et $0 < \alpha_i \leqslant 1$. On peut alors utiliser la relation coefficient-racines (se démontre facilement par récurrence sur n) : $a_p = (-1)^p \sigma_p(z_1 \ldots z_n)$
$$P = X^n - \sigma_1 X^{n-1} + \ldots + (-1)^n \sigma_n$$
et $\sigma_i \in \mathbb{Z}$.
Or $|z_i| \leqslant 1$ donc, pour $1 \leqslant p \leqslant n$,
$$|\sigma_p| = \left| \sum_{1 \leqslant i_1 < \ldots < i_p \leqslant n} z_{i_1} \cdots z_{i_n} \right| \leqslant \sum_{1 \leqslant i_1 < \ldots < i_p \leqslant n} 1 = \binom{n}{p}.$$ [1]

On en déduit que Ω_n est fini.
On considère désormais
$$P_k := \prod_{i=1}^{n} (X - z_i^k)$$
et montrons que $P_k \in \Omega_n$.

Le coefficient de X^{n-r} dans P_k est $(-1)^r \sigma_r(z_1^k, \ldots, z_n^k)$. Or $\sigma_r(X_1^k, \ldots, X_n^k)$ est un polynôme symétrique à coefficients dans $\mathbb{Z}$, donc par le théorème de structure des polynômes symétriques il existe $Q_r \in \mathbb{Z}[X_1, \ldots, X_n]$ tel que
$$\sigma_r(X_1^k, \ldots, X_n^k) = Q_r(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)).$$
On en déduit, étant donné que $\sigma_i(z_1, \ldots, z_n) \in \mathbb{Z}$,
$$\sigma_r(z_1^k, \ldots, z_n^k) = Q_r(\sigma_1(z_1, \ldots, z_n), \ldots, \sigma_n(z_1, \ldots, z_n)) \in \mathbb{Z}.$$

De plus, P_k est unitaire et ses racines sont les z_i^k qui vérifient $0 < |z_i^k| \leqslant 1$. Par conséquent, $P_k \in \Omega_n$.
Or Ω_n est fini donc l'ensemble Z_n des racines des éléments de Ω_n est fini donc, pour $i \in \{1, \ldots, n\}$, l'application
$$\begin{aligned} \mathbb{N}^* &\longrightarrow Z_n \\ k &\longmapsto z_i^k \end{aligned}$$
n'est pas injective. On en déduit qu'il existe $k \neq l$ tels que $z_i^k = z_i^l$ et $z_i \neq 0$ donc $z_i^{k-l} = 1$ et z_i est une racine de l'unité. ■

1. cardinal des parties à p éléments de $[\![1, n]\!]$

Corollaire 1

Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible tel que $Z(P) \subset D(0,1)$, où $Z(P)$ désigne les racines de P.
Alors $P = X$ ou P est un polynôme cyclotomique.

Preuve :
(Gourdon Algèbre p.89 ? ?) Supposons $P \neq X$. Alors P est irréductible donc 0 n'est pas racine de P et, d'après le théorème de Kronecker, ses racines sont des racines de l'unité. De plus, les racines de P sont simples car P est irréductible (sinon il serait divisible par $P \wedge P'$ non trivial). Donc il existe un entier N tel que pour toute racine z de P, $z^N = 1$ et donc $P \mid X^N - 1$.
Or

$$X^N - 1 = \prod_{d \mid N} \Phi_d$$

avec Φ_d irréductible sur $\mathbb{Z}$.
$P \neq 1$ donc $P = \Phi_k$ pour un certain k. ■

Corollaire 2

Tout polynôme de $\mathbb{Z}[X]$ unitaire ayant ses racines dans $D(0,1)$ est un produit de puissances de X et de polynômes cyclotomiques.

Version résultant pour montrer que $P_k \in \mathbb{Z}[X]$ (paragraphe décalé)

On va introduire,pour $\lambda \in \mathbb{C}$, $Q_k^\lambda = X^k - \lambda$ et, pour finir, le résultant suivant (de taille $k+n$) :

$$R_k(\lambda) = \mathrm{Res}(P, Q_k^\lambda) = \begin{vmatrix} 1 & & & & 1 & & \\ a_1 & \ddots & & & 0 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & 1 \\ a_n & & \ddots & 1 & 0 & & 0 \\ & \ddots & & a_1 & -\lambda & \ddots & \vdots \\ & & \ddots & \vdots & & \ddots & 0 \\ & & & a_n & & & -\lambda \end{vmatrix}$$

On voit bien que R_k est polynomial en λ (si l'on préfère, il est assez aisé de raisonner dans $\mathbb{Z}[\lambda]$) et que ses coefficients sont entiers (les a_p étant entiers). Pour conclure, on va exprimer le résultant en fonction des racines des polynômes (on rappelle que P est unitaire et que ses racines sont les z_i) :

$$R_k(\lambda) = \mathrm{Res}(P, Q_k^\lambda) = \prod_{i=1}^{n} Q_k^\lambda(z_i) = \prod_{i=1}^{n} (z_i^k - \lambda) = (-1)^n P_k(\lambda)$$

Les coefficients de R_k sont entiers, donc ceux de P_k le sont aussi.

Notes :

✓ **A l'oral**, 7'45 sauf la partie qui change. 2'27 version polynome symétrique. 2' version résultant. Il faut vraiment prendre son temps à fond !
✓ On a par exemple $\sigma_1 = z_1 + z_2 + \cdots + z_n$ et $\sigma_n = z_1.z_2 \ldots z_n$.
♣ Leopold Kronecker (1823 - 1891) est un mathématicien et logicien allemand. Persuadé que l'arithmétique et l'analyse doivent être fondées sur les “nombres entiers”, il est célèbre pour la citation suivante : “Dieu a fait les nombres entiers, tout le reste est l'oeuvre de l'homme. ”. Cela le met en opposition avec certains développements mathématiques de Cantor, l'un de ses étudiants. Son point de vue sera repris par Weyl au siècle suivant. En analyse, Kronecker rejette la formulation d'une fonction continue partout mais nulle part dérivable de son collègue Weierstrass.