

# Théorème de Kronecker.

2013 – 2014

Référence : Serge Francinou, Hervé Gianella, Serge Nicolas, *Oraux X-ENS Algèbre 1*, Cassini, 2008, p.213.

## Théorème.

On définit

$$\Omega_n := \{P \in \mathbb{Z}[X] \mid P \text{ unitaire, } \deg P = n \text{ et } z \in Z(P) \Rightarrow 0 < |z| \leq 1\}$$

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.

*Démonstration.* Montrons dans un premier temps que  $\Omega_n$  est fini.

On note  $z_1, \dots, z_n$  les racines de  $P$  et  $\sigma_1, \dots, \sigma_n$  les fonctions symétriques élémentaires de  $P$  évaluées en  $(z_1, \dots, z_n)$ .

Alors

$$P = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$$

et  $\sigma_i \in \mathbb{Z}$ .

Or  $|z_i| \leq 1$  donc, pour  $1 \leq p \leq n$ ,

$$|\sigma_p| = \left| \sum_{1 \leq i_1 < \dots < i_p \leq n} z_{i_1} \cdots z_{i_p} \right| \leq \sum_{1 \leq i_1 < \dots < i_p \leq n} 1 = \binom{n}{p}.$$

On en déduit que  $\Omega_n$  est fini.

On considère désormais

$$P_k := \prod_{i=1}^n (X - z_i^k)$$

et montrons que  $P_k \in \Omega_n$ .

Afin de montrer que  $P_k \in \mathbb{Z}[X]$ , introduisons le polynôme  $Q_k := X - Y^k \in \mathbb{Z}[X, Y]$  et considérons  $R_k(X) := \text{Res}_Y(P(Y), Q_k(X, Y))$ .  $P \in \mathbb{Z}[X]$  et  $Q_k \in \mathbb{Z}[X, Y]$  donc  $R_k \in \mathbb{Z}[X]$ . Par ailleurs,

$$R_k(X) = \prod_{i=1}^n Q_k(X, z_i) = \prod_{i=1}^n (X - z_i^k) = P_k(X)$$

donc  $P_k \in \mathbb{Z}[X]$ . De plus,  $P_k$  est unitaire et ses racines sont les  $z_i^k$  qui vérifient  $0 < |z_i^k| \leq 1$ . Par conséquent,  $P_k \in \Omega_n$ .

Or  $\Omega_n$  est fini donc l'ensemble des racines des éléments de  $\Omega_n$  est fini donc, pour  $i \in \{1, \dots, n\}$ , l'application

$$\begin{aligned} \mathbb{N}^* &\longrightarrow \mathbb{C} \\ k &\longmapsto z_i^k \end{aligned}$$

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.  $\square$

**Corollaire.**

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.

*Démonstration.* 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) et donc  $P \mid X^N - 1$  pour un certain  $N$ . Or

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

avec  $\Phi_d$  irréductible sur  $\mathbb{Z}$ .

$P \neq 1$  donc  $P = \Phi_k$  pour un certain  $k$ .  $\square$

**Corollaire.**

< 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.

**Détails supplémentaires**

Autre rédaction possible pour montrer que  $P_k \in \mathbb{Z}[X]$  :

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

$$\sigma_r(X_1^k, \dots, X_n^k) = Q_r(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)).$$

On en déduit, étant donné que  $\sigma_i(z_1, \dots, z_n) \in \mathbb{Z}$ ,

$$\sigma_r(z_1^k, \dots, z_n^k) = Q_r(\sigma_1(z_1, \dots, z_n), \dots, \sigma_n(z_1, \dots, z_n)) \in \mathbb{Z}.$$