# 24. Théorème de Kronecker

[FGN07a, §5.33, p213] [Gou09, §2.5, p89]

## Énoncé

**Théorème. [Théorème de Kronecker]**
*Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes les racines de $P$ sont de module inférieur ou égal à 1 et $P(0) \neq 0$, alors toutes les racines de $P$ sont des racines de l'unité.*

**Corollaire. [Théorème de Kronecker]**
*Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n$ et irréductible sur $\mathbb{Q}$. Si toutes les racines de $P$ sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_n$.*

---

## Développement

1. Soit $\Omega$ l'ensemble des $P \in \mathbb{Z}[X]$ de degré $n$ unitaires tels que toutes les racines de $P$ sont de module inférieur ou égal à 1 et $P(0) \neq 0$.

   Soit $P \in \Omega$. Soient $z_1, \ldots, z_n$ ses racines comptées sans leur multiplicité.
   Pour $r \in [\![1, n]\!]$, on pose $\sigma_r(z_1, \ldots, z_n) = \sum_{I \in \mathcal{P}_r([\![1,n]\!])} \prod_{i \in I} z_i$ le $r$-ième polynôme symétrique élémentaire, de sorte que :

$$P(X) = X^n + \sum_{r=1}^n (-1)^r \sigma_r(z_1, \ldots, z_n) X^{n-r}$$

   On a que les $(\sigma_p(z_1, \ldots, z_n))_p$ sont dans $\mathbb{Z}$. En utilisant que $|z_i| \leq 1$ pour tout $i$, on a :

$$|\sigma_p(z_1, \ldots, z_n)| \leq \sum_{I \in \mathcal{P}_p([\![1,n]\!])} \prod_{i \in I} |z_i| \leq \operatorname{card}(\mathcal{P}_p([\![1, n]\!])) = \binom{n}{p}$$

   Ainsi le nombre de polynômes $P$ satisfaisants est fini !

2. Définissons alors pour $k$ entier non nul le polynôme $P_k = \prod_{1 \leq i \leq n} (X - z_i^k)$.
   On veut montrer que les $(P_k)_{k \in \mathbb{N}^*}$ sont des éléments de $\Omega$.
   Notons déjà qu'ils sont tous de degré $n$, unitaires, et leurs racines sont toutes de module dans $]0, 1]$. Reste donc à vérifier que $P_k \in \mathbb{Z}[X]$.
   Posant $\sigma_r^{(k)} = \sigma_r(z_1^k, \ldots, z_n^k)$, on a pour tout $k$ :

$$P_k = X^n + \sum_{r=1}^n (-1)^r \sigma_r^{(k)} X^{n-r}$$

   Fixons $k \in \mathbb{N}$ et $r \in [\![1, n]\!]$. Alors :

$$\sigma_r^{(k)} = \sum_{I \in \mathcal{P}_r([\![1,n]\!])} \prod_{i \in I} z_i^k = Q_r(z_1, \ldots, z_n) \qquad \text{où } Q_r(X_1, \ldots, X_n) = \sum_{I \in \mathcal{P}_r([\![1,n]\!])} \prod_{i \in I} X_i^k$$

   est un polynôme symétrique. Par le théorème de décomposition en polynômes symétriques, on a que

$$Q_r(X_1, \ldots, X_n) = T_r(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)) = T_r(\sigma_1^{(1)}, \ldots, \sigma_n^{(1)})$$

   pour un certain $T_r$ à coefficients dans $\mathbb{Z}$.

   Comme les $(\sigma_p^{(1)})_{1 \leq p \leq n}$ sont dans $\mathbb{Z}$, on en déduit que $\sigma_r^{(k)} \in \mathbb{Z}$.

   Ceci étant valable pour tout $r \in [\![1, n]\!]$, on a finalement que $P_k \in \mathbb{Z}[X]$.
   On a donc $P_k \in \Omega$.

3. $\Omega$ est fini et donc a fortiori l'ensemble des racines des éléments de $\Omega$ aussi. Par définition il ne contient pas $0$.

   A $i \in [\![1, n]\!]$ fixé, l'ensemble $(z_i^k)_{k \in \mathbb{N}^*}$ est donc nécessairement fini : il existe donc $k_1 < k_2$ tel que $z_i^{k_1} = z_i^{k_2}$, ou encore $z_i^{k_2 - k_1} = 1$ puisque $z_i \neq 0$.
   Donc $z_i$ est une racine de l'unité.

Montrons alors le corollaire. Si $P(0) \neq 0$, on a que chaque $(z_i)_{1 \leq i \leq n}$ est une racine de l'unité.

Par exemple $z_1$ est une racine $k$-ième de l'unité pour un certain $k$. Donc $\Phi_k \mid P$ le polynôme minimal de $z_1$. Comme $P$ et $\Phi_k$ sont irréductibles et unitaires, on a que $P = \Phi_k$.

---

## Commentaires

Bien maitriser le théorème de décompostion en polynômes symétriques élémentaires.