

Théorème de Kronecker

Francinou oraux X-ENS
(p. 257)
+ CVA pour l'application

Recasages: 102, 144

Théorème: Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.

Preuve: Notons $z_1, \dots, z_m$ les racines de P comptées avec multiplicité. $n \geq 1$ est le degré de P ; et $\sigma_1, \dots, \sigma_m$ les fonctions symétriques élémentaires des z_i . On a donc

$$P(X) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n, \quad k \in [1; n], \sigma_k \in \mathbb{Z}$$

Posons $\Omega_n = \{P \in \mathbb{Z}[X], \deg(P) = n, \text{dom}(P) \leq 1, Z(P) \subset \overline{D(0, 1)}\}$.

Montrons que Ω_n est fini:

$\forall k \in [1; n], |z_i| \leq 1$ donc pour tout $p \in [1; n]$,

$$|a_p| = \left| \sum_{\substack{I \subset [1; n] \\ \#I = p}} \prod_{i \in I} z_i \right| \leq \sum_{\substack{I \subset [1; n] \\ \#I = p}} 1 = \# \{I \subset [1; n] \mid \#I = p\} = \binom{n}{p}$$

Donc Ω_n est fini.

• On considère, pour tout $k \in \mathbb{N}^*$, $P_k(X) = (X - z_1^k) \dots (X - z_m^k)$. $\overset{H_2}{P_k \in \Omega_n}$
Les (P_k) sont des polynômes unitaires de degré n dont les racines sont de module inférieur ou égal à 1.

Le coefficient de X^{n-k} dans P_k est $(-1)^k \sigma_k(z_1^k, \dots, z_m^k)$. C'est un polynôme symétrique en $z_1, \dots, z_m$ à coefficients dans $\mathbb{Z}$. Par le théorème de structure, il est égal à un polynôme de $\mathbb{Z}[X]$ en les fonctions symétriques élémentaires des z_i qui sont elles-mêmes dans $\mathbb{Z}$ (car $P \in \mathbb{Z}[X]$). Ainsi, pour tout $k \in \mathbb{N}^*$, $P_k \in \mathbb{Z}[X]$, donc $P_k \in \Omega_n$.

• Comme Ω_n est fini, et que chaque élément de Ω_n admet au plus n racines, l'ensemble des racines des éléments de Ω_n est aussi fini.

En particulier, $k \mapsto z_i^k$ n'est pas injective.

Il existe donc deux entiers $k \neq l$ tels que $z_i^k = z_i^l$
 Comme $z_i \neq 0$, il s'agit d'une racine de l'unité.

Application: Soit G un sous-groupe fini de $GL_n(\mathbb{Z})$. Alors le morphisme $\pi: G \rightarrow GL_n(\mathbb{Z}/3\mathbb{Z})$
 $A = (a_{ij}) \mapsto (\bar{a}_{ij})$ est bien défini et injectif.

Preuve: Comme $A \in GL_n(\mathbb{Z})$, il existe $A' \in M_n(\mathbb{Z})$ tel que $AA' = I_n$
 En prenant le déterminant, on a $\det(A) \det(A') = 1$ donc $\det(A) \in \{1, -1\}$. Or, on a la formule:

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{j=1}^n a_{\sigma(j), j}$$

Donc $\det(\bar{A}) = \overline{\det(A)} = \pm 1$.

Ainsi, on a bien $\bar{A} \in GL_n(\mathbb{Z}/3\mathbb{Z})$. De plus, $\pi(AB) = \pi(A)\pi(B)$ et $\pi(I_n) = I_n$.
 D'où un morphisme de $GL_n(\mathbb{Z})$ dans $GL_n(\mathbb{Z}/3\mathbb{Z})$.

Montrons qu'il est injectif. Soit $A \in GL_n(\mathbb{Z})$ tel que $\pi(A) = \bar{I}_n$ i.e.
 $A = I_n + 3B$, $B \in M_n(\mathbb{Z})$. Comme G est fini, il existe $d > 0$, tel que
 $A^d = I_n$ donc $X^d - 1$ annule A et donc A est diagonalisable sur $\mathbb{C}$. De plus, toute valeur propre de A est une racine d -ième de l'unité.
 $\rightarrow B$ trigonalisable dans $\mathbb{C}$.

D'autre part, si P est une matrice de passage telle que PBP^{-1} est triangulaire, alors $PAP^{-1} = I_n + 3PBP^{-1}$ triangulaire, et donc, pour toute valeur propre α de A , $\beta = \frac{\alpha-1}{3}$ est une valeur propre de B . Ainsi, $\rightarrow$ en diagonalisant PAP^{-1} .

$$|\beta| = \frac{|\alpha-1|}{3} \leq \frac{|\alpha|+1}{3} \leq \frac{2}{3} < 1$$

Donc, $X^d - 1$ unitaire à coeff dans $\mathbb{Z}$, a la que des racines de module $|\beta| < 1$. Par le théorème de Kronecker, elles sont toutes nulles. Les valeurs propres de A sont donc toutes égales à 1 et comme A est diagonalisable, il en résulte que $A = I_n$.

Soit $z_i = 0$, soit z_i est une racine de l'unité

$|\beta| < 1$ donc pas une racine de l'unité