Développement : Théorème de Kronecker

Algèbre & Géométrie

Références : [ENS1] Francinou S., Gianella H., Nicolas S., *Exercices de mathématiques - Oraux X-ENS - Algèbre 1*, Cassini, 2001, p198.
Pour le corollaire : [GX] Gourdon X., *Les maths en tête - Algèbre, 2ème édition*, ellipses, 2009, p89
Pour les leçons :
- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- 105 : Groupe des permutations d'un ensemble fini. Applications.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Le but de ce développement est de prouver le théorème de Kronecker suivant :

Théorème 1. ***Théorème de* Kronecker.**

Soit $P \in \mathbb{Z}[X]$ unitaire non constant dont toutes les racines complexes z vérifient $|z| \leqslant 1$. Si $P(0) \neq 0$, alors toutes les racines de P sont des racines de l'unité.

Preuve : Soit $n \in \mathbb{N}^*$. Soit Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$ de degré n dont les racines complexes sont de module $\leqslant 1$.
⋆ Étape 1 : Montrons que Ω_n est un ensemble fini. Soit $P \in \Omega_n$.
On note $z_1, \dots, z_n$ les racines de P (comptées avec leur multiplicité), avec $n = \deg(P) \geqslant 1$. On note également $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires des z_i, de sorte que :

$$P(X) = X^n + \sum_{i=1}^{n} (-1)^i \sigma_i X^{n-i}.$$

Comme $P \in \mathbb{Z}[X]$, les σ_i sont entiers. Comme, pour tout $i \in [\![1;n]\!]$, on a $|z_i| \leqslant 1$, on a, pour tout $p \in [\![1;n]\!]$:

$$\begin{aligned} |\sigma_p| &= \left| \sum_{I \in \mathcal{P}_p([\![1;n]\!])} \prod_{i \in I} z_i \right| \\ &\leqslant \sum_{I \in \mathcal{P}_p([\![1;n]\!])} 1 \\ &\leqslant |\mathcal{P}_p([\![1;n]\!])| \\ &\leqslant \binom{n}{p}. \end{aligned}$$

Ainsi, on a au plus $\binom{n}{p}$ choix pour le polynôme P. Cela prouve que Ω_n est fini.
⋆ Étape 2 : Soit $P \in \Omega_n$, et on conserve les notations de l'Étape 1. Soit $k \in \mathbb{N}^*$, on pose :

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

Montrons que $P_k \in \Omega_n$. Déjà, P_k a ses racines de module $\leqslant 1$ et est unitaire. Il reste à montrer que $P_k \in \mathbb{Z}[X]$.
Si $r \in [\![1;n]\!]$, le coefficient de X^{n-r} de P_k est $(-1)^r \sigma_r(z_1^k, \dots, z_n^k)$, qui est un polynôme symétrique en les $z_1, \dots, z_n$ à coefficients entiers.
D'après le théorème de Newton pour les polynômes symétriques, il existe $R_{p,k} \in \mathbb{Z}[X_1, \dots, X_n]$ tel que :

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

puisque les $\sigma_i(z_1, \dots, z_n)$ sont entiers (relations coefficients-racines de $P \in \mathbb{Z}[X]$).
Donc $P_k \in \mathbb{Z}[X]$, ce qui prouve que $P_k \in \Omega_n$.

Remarque 2. ***Autre argument pour prouver que $P_k \in \mathbb{Z}[X]$.***

Soit $C(P)$ la matrice compagnon du polynôme P. Cela signifie que le polynôme caractéristique $\chi_{C(P)}$ de $C(P)$ est P.
Comme $P \in \mathbb{Z}[X]$, $C(P) \in \mathcal{M}_n(\mathbb{Z})$. $\chi_P = P$ est scindé dans $\mathbb{C}[X]$, on peut donc trigonaliser $C(P)$ dans $\mathbb{C}$. $C(P)^k$ est donc semblable à une matrice triangulaire supérieure dont les coefficients sont les z_i^k.
Son polynôme caractéristique est donc P_k, dont la matrice compagnon est à coefficients entiers (en tant que puissance d'une matrice de $\mathcal{M}_n(\mathbb{Z})$). Donc $P_k \in \mathbb{Z}[X]$.

⋆ Étape 3 : Concluons.
Comme Ω_n est fini et que chaque élément de Ω_n admet au plus n racines complexes distinctes, l'ensemble des racines des éléments de Ω_n, qu'on note $\mathcal{R}_n$, est fini. En particulier, pour $i \in [\![1;n]\!]$, l'application $\varphi_i : \mathbb{N}^* \to \mathcal{R}_n$ définie par :

$$\forall k \in \mathbb{N}^* \quad \varphi_i(k) = z_i^k$$

n'est pas injective. Il existe donc $k, \ell \in \mathbb{N}^*$ avec $k \neq \ell$ tels que :

$$z_i^k = z_i^\ell.$$

Comme $P(0) \neq 0$, on a $z_i \neq 0$. Cela permet d'écrire $z_i^{k-\ell} = 1$, et z_i est une racine de l'unité.
Cela achève la preuve. □

Corollaire 3.

Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n \geqslant 1$. On suppose que P est irréductible dans $\mathbb{Q}[X]$.
Si toutes les racines de P sont de module $\leqslant 1$, alors $P = X$ ou il existe $d \in \mathbb{N}^*$ tel que $P = \Phi_d$, où Φ_d est le d-ième polynôme cyclotomique.

Preuve : Si $P(0) = 0$, alors X divise P qui est irréductible (et unitaire), donc $P = X$.
Supposons donc que $P(0) \neq 0$. D'après le théorème de Kronecker, les racines de P sont des racines de l'unité.
Si ζ est une racine de P, en notant d son ordre, le d-ième polynôme cyclotomique Φ_d est le polynôme minimal de ζ sur $\mathbb{Q}$. Comme P annule ζ, Φ_d divise P qui est irréductible dans $\mathbb{Q}[X]$.
Finalement, comme Φ_d et P sont unitaires, $P = \Phi_d$. □

Remarque 4.

La preuve du corollaire n'utilise pas ce qui est dans le livre, mais utilise le théorème de Kronecker. J'ai mis la référence du livre pour qu'on retrouve le corollaire, mais le théorème de Kronecker donne le résultat beaucoup plus rapidement.