Théorème de Kronecker

Tristan Vaccon

septembre 2012

Le but de ce développement est de démontrer le théorème suivant :

Théorème 1. *Soit $P \in \mathbb{Z}[X]$ unitaire. On suppose que les racines de P dans $\mathbb{C}$ sont toutes dans le disque fermé $D(0,1)$ de centre 0 et de rayon 1. On suppose aussi que $P(0) \neq 0$. Alors, les racines de P sont des racines de l'unité, et sont donc en particulier, dans $S(0,1)$, cercle de centre 0 et de rayon 1.*

Une application directe sera la suivante :

Théorème 2. *Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible. On suppose que P a toutes ses racines dans $D(0,1)$. Alors $P = X$ ou P est un polynôme cyclotomique.*

1 Finitude de l'ensemble des tels polynômes d'un degré donné

Soit un tel P, et soit $z_1, \ldots, z_n$ ses racines : $P = (X - z_1) \ldots (X - z_n)$. Soit $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires en les z_i. On peut écrire $P = \sum_{i=0}^{n} (-1)^{n-i} \sigma_{n-i} X^i$.

Or, $|z_i| \leqslant 1$ si $i \in [\![1, n]\!]$. Pour $p \in [\![1, n]\!]$,

$$|\sigma_p| = |\sum_{I \in P_p([\![1,n]\!])} \prod_{i \ inI} z_i| \leqslant \sum_{I \in P_p([\![1,n]\!])} 1 = card(P_p([\![1,n]\!]) = \binom{n}{p}.$$

On a ici noté $P_p(X)$ pour l'ensemble des parties à p éléments de X.

On en déduit :

Lemme 1.1. *l'ensemble Ω_m des polynômes unitaires de $\mathbb{Z}[X]$, de degré m, dont les racines complexes sont dans $D(0,1)$ est fini.*

2 Construction d'une famille de tels polynômes

Soit $k \in \mathbb{N}$. On pose $P_k = (X - z_1^k)(X - z_2^k) \dots (X - z_n^k)$.

P_k est unitaire, de degré n, avec pour racines les z_i^k, qui sont dans $D(0,1)$. Montrons que $P_k \in \Omega_n$.

Si $r \in [\![1, n]\!]$, le coefficient de X^{n-k} dans P_k est $(-1)^k \sigma_k(z_1^k, \dots, z_n^k)$. Or, $\sigma_k(X_1^k, \dots, X_n^k$ est est un polynôme symétrique en $X_1, \dots, X_n$ à coefficients dans $\mathbb{Z}$, donc (propriété génératrice des polynômes symétriques élémentaires, sur $\mathbb{Z}$), c'est un polynôme à coefficient entier en les $\sigma_i(X_1, \dots X_n)$. Ainsi, $\sigma_k(z_1^k, \dots, z_n^k)$ est un polynôme à coefficients entiers en les $\sigma(z_1, \dots, z_n)$, qui sont dans $\mathbb{Z}$.

On en déduit que pour tout $k \in \mathbb{N}^*$, $P_k \in \mathbb{Z}[X]$, et donc $P_k \in \Omega_n$.

3 Principe des tiroirs de Dirichlet

On a vu que Ω_n est fini, et comme chaque $P \in \Omega_n$ a au plus n racines complexes distinctes, l'ensembles Z_n des racines des éléments de Ω_n est fini. Mais alors, la fonction $\mathbb{N} \to Z_n$, $k \mapsto z_i^k$ est nécessairement non injective.

Ainsi, il existe k, l entiers distincts tels que $z_i^k = z_i^l$, et donc, comme $z_i \neq 0$, z_i *est une racine de l'unité*. Ceci clôt la démonstration du premier théorème.

4 application au second théorème

On prend un polynôme comme dans le premier théorème, et on suppose de plus qu'il est irréductible. Soit z une de ses racines. z est d'ordre finie, et est racine d'un certain polynôme cyclotomique Φ_k. Par action de Galois (P est à coefficient dans $\mathbb{Z}$), on montre facilement que Φ_k divise P. Φ_k et P sont deux polynômes irréductibles de $\mathbb{Z}[X]$, on en déduit que $\Phi_k = P$.

On peut aussi remarquer que, les racines de P sont des racines N-èmes de l'unité pour un N bien choisi, on a $P | X^N - 1$, et $X^N - 1 = \prod_{d|N} \Phi_d(X)$ est sa décomposition en irréductibles sur $\mathbb{Z}$. Comme $P \neq 1$, on en déduit $P = \Phi_k$ pour un certain k.

Maintenant, si P est irréductible et admet 0 comme racine, on a nécessairement $P = X$. Ceci clôt le second théorème. On remarquera que cela permet de voir que tout polynôme de $\mathbb{Z}[X]$ ayant ses racines dans $D(0,1)$ est un produit de puissances de X et de polynômes cyclotomiques.

5 Variante “résultant” de la partie 2

On remarque que si l'on pose $P_k(X) = (X - z_i^k) \dots (X - z_n^k)$ et $Q_k^Y(X) = X^k - Y$, $k \in \mathbb{N}^*$, et si on pose

$$R_k(Y) = Res(P_1(X), Q_k^Y(X)) = \begin{bmatrix} 1 & & & 1 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & 1 & 0 & & 1 \\ a_n & & a_1 & -Y & & 0 \\ & \ddots & \vdots & & \ddots & 0 \\ & & a_n & & & -Y \end{bmatrix} \in \mathbb{Z}[Y].$$

Alors, le terme de plus haut degré de $R_k(Y)$ est $(-1)^n Y^n$ et on a $R_k(Y) = \prod_{i=1}^n Q_k^Y(z_i) = \prod_{i=1}^n (z_i^k - Y) = (-1)^n P_k(Y)$. Ceci permet bien de montrer que $P_k \in \mathbb{Z}[X]$.

Références

[1] Francinou, Gianella, Nicolas Oraux X-ENS, Alg 1

[2] Szpirglas, Aviva Algèbre L3