Théorème de Kronecker

Référence : [Szp09] p.573.

Théorème 0.1 (de Kronecker) *Soit P_1 un polynôme qui vérifie la propriété K_n : P_1 est unitaire, de degré n, à coefficients entiers, ie $P_1(X) = X^n + a_1X^{n-1} + \ldots + a_n$, les racines de P_1 dans $\mathbb{C}$ sont de module inférieur ou égal à 1 et $a_n \neq 0$. Alors les racines de P_1 sont des racines de l'unité.*

Démonstration On note α_i pour $1 \leq i \leq n$ les racines de P_1 (on sait qu'elles existent car $\mathbb{C}$ est algébriquement clos).
$\rightsquigarrow$ Les relations entre les coefficients $a_1, \ldots, a_n$ et les racines $\alpha_1, \ldots, \alpha_n$ donnent une majoration des coefficients de P_1. En effet, sachant que $\forall 1 \leq i \leq n$, $|\alpha_i| \leq 1$, on a :

$$\frac{|a_k|}{|a_0|} = |a_k| = \left| \sum_{1 \leq i_1 < \ldots < i_k \leq n} \alpha_{i_1} \ldots \alpha_{i_k} \right| \leq C_n^k$$

car on choisit pour la somme k coefficients parmi n.
$\rightsquigarrow$ On pose $R(X) = X^n + b_1X^{n-1} + \ldots + b_n$ un polynôme vérifiant la propriété K_n. On a donc pour tout $1 \leq k \leq n$, $|b_k| \leq C_n^k$.
Par conséquent b_k prend une des $1 + 2C_n^k$ valeurs $-C_n^k, \ldots, -1, 0, 1, \ldots, C_n^k$ (car ses coefficients sont entiers).
Donc le nombre de polynômes vérifiant la propriété K_n est fini puisque majoré par $\prod_{k=1}^{n}(1 + 2C_n^k)$.
$\rightsquigarrow$ On note $P_k(X) = (X - \alpha_1^k) \ldots (X - \alpha_n^k)$ et $Q_k^Y(X) = X^k - Y$ où k est un entier supérieur ou égal à 1.
On considère le résultant $R_k(Y)$ des polynômes, en la variable X, $P_1(X)$ et $Q_k^Y(X)$. Ce polynôme $R_k(Y)$ est égal au déterminant de Sylvester suivant :

$$R_k(Y) = \begin{vmatrix} 1 & & & 1 & & \\ a_1 & \ddots & & 0 & \ddots & \\ \vdots & \ddots & 1 & 0 & & 1 \\ a_n & & a_1 & -Y & & 0 \\ & \ddots & \vdots & & \ddots & 0 \\ & & a_n & & & -Y \end{vmatrix}$$

L'écriture de ce déterminant montre que les coefficients de R_k sont des entiers (en écrivant la formule du déterminant comme somme de permutations).
Par ailleurs, les racines de P_1 sont $\alpha_1, \ldots, \alpha_n$, ainsi le calcul du résultant en fonction des racines de l'un des polynômes nous donne :

$$R_k(Y) = \prod_{i=1}^{n} Q_k^Y(\alpha_i) = \prod_{i=1}^{n} (\alpha_i^k - Y) = (-1)^n P_k(Y)$$

Les polynômes P_k sont donc unitaires et à coefficients entiers. Leurs racines sont de module inférieur ou égal à 1 et non nulle car $0 < |\alpha_i^k| \leq |\alpha_i| \leq 1$ (car un polynôme unitaire à coefficients entiers ne peut pas admettre 0 comme racine). Donc les polynômes P_k vérifient la propriété K_n (ils sont bien de degré n).
$\rightsquigarrow$ Les polynômes qui vérifient ces propriétés sont en nombre fini, il existe donc un entier $k > 1$ tel que $P_k = P_1$. Les racines de P_1 sont $\alpha_1, \ldots \alpha_n$ et celles de P_k sont $\alpha_1^k, \ldots, \alpha_n^k$. Mais P_1 et P_k ont les mêmes racines (avec même multiplicité, puisqu'ils sont égaux). Donc partant d'une racine

α_1 de P_1, on voit donc que $\alpha_1^k, \alpha_1^{k^2}, \alpha_1^{k^3}, \ldots$ sont des racines de P_1 ; il existe donc des entiers p et q tels que $\alpha_1^{k^p} = \alpha_1^{k^q}$, ce qui entraîne que α_1 est une racine de l'unité. Donc les racines de P_1 sont des racines de l'unité.

Lemme utilisé

Lemme 0.1 *Soient* $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \mathbb{K}$ *tels que :*

$$A(X) = a_0(X - \alpha_1) \ldots (X - \alpha_m) \quad \textit{et} \quad B(X) = b_0(X - \beta_1) \ldots (X - \beta_n)$$

ce qui est toujours le cas si $\mathbb{K}$ *est un corps algébriquement clos* ($\mathbb{C}$ *par exemple). Alors :*

$$Res(A, B) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_0^n \prod_{i=1}^{m} B(\alpha_i) = (-1)^{mn} Res(B, A)$$

Références

[Szp09] Aviva Szpirglas. *Mathématiques L3, algèbre.* Pearson education, 2009.