Théorème de Kronecker

Arnaud Girand

5 juillet 2012

Référence :
- [Szp09], p. 573

Proposition 1
Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$:

$$P =: X^n + \sum_{i=1}^{n} a_i X^{n-i}$$

On fait les hypothèse suivantes :
- *les racines de P sur $\mathbb{C}$ sont de module inférieur ou égal à 1 ;*
- *$a_n \neq 0$ (i.e $X \nmid P$).*

Alors les racines de P sont des racines de l'unité.

Démonstration : Dans toute la suite, on dira qu'un polynôme $R \in \mathbb{Z}[X]$ vérifie la propriété (K_n) si :
- R est unitaire de degré n ;
- les racines de R sur $\mathbb{C}$ sont de module inférieur ou égal à 1 ;
- X ne divise pas R.

Il va sans dire que P vérifie (K_n). Notons $\alpha_1, \ldots, \alpha_n$ les racines de P comptées avec multiplicité ; on a alors, par relations coefficients–racines :

$$\begin{aligned} \forall k \in [n], \quad |a_k| &= \left| \sum_{1 \leq i_1 < \ldots < i_k \leq n} \prod_{j=1}^{k} \alpha_{i_j} \right| \\ &\leq C_n^k \text{ car } \forall \ell \in [n],\ |\alpha_\ell| \leq 1 \end{aligned}$$

Soit $R := X^n + \sum_{i=1}^{n} b_i X^{n-i} \in \mathbb{Z}[X]$ un polynôme vérifiant la propriété (K_n) ; alors on a de même que pour tout $k \in [n]$, $|b_k| \leq C_n^k$ et donc b_k appartient à l'ensemble $\{-C_n^k, \ldots, C_n^k\}$, qui est de cardinal $2C_n^k + 1$. De fait le nombre de polynômes de $\mathbb{Z}[X]$ vérifiant (K_n) est majoré par $\prod_{k=1}^{n}(1 + 2C_n^k)$ donc est fini.

Pour $k \in \mathbb{N}^*$ on pose à présent :

$$P_k := \prod_{i=1}^{n}(X - \alpha_i^k) \text{ et } Q_k := X^k - Y \in \mathbb{Z}[X, Y]$$

On pose ensuite, toujours pour $k \geq 1$: $R_k := \mathrm{Res}_X(P, Q_k)$, i.e :

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

Il est alors clair que $R_k \in \mathbb{Z}[Y]$ et que son coefficient dominant est $(-1)^n Y^n$. De plus on a :

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

Il est de fait immédiat que $P_1 = P$ et que les P_k vérifient (K_n).

Comme les P_k vérifient (K_n), il existe $k > 1$ tel que $P_k = P_1 = P$ et donc P et P_k ont les mêmes racines avec les mêmes multiplicité. De fait, si α est une racine de P, α^k est une racine de P_k donc de P. Mais alors, $(\alpha^k)^k = \alpha^{k^2}$ est une racine de P_k donc de P, ... In fine, tous les éléments de la suite $(\alpha^{k^p})_{p\in\mathbb{N}^*}$ sont des racines de P. P ayant un nombre fini de racines on a alors l'existence de $p, q \geq 1$ avec $p < q$ tels que $\alpha^{k^p} = \alpha^{k^q}$ et donc $\alpha^{k^p - k^q} = 1$: α est bien une racine de l'unité.

Références

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