THÉORÈME DE KRONECKER

Théorème : Soit $P \in \mathbb{Z}[X]$ avec $P(0) \neq 0$ et unitaire, et de degré n. Si toutes les racines de P ont module inférieur à 1, alors ce sont des racines de l'unité.

Preuve : Prenons $\mathcal{A}_n := \{$polynômes vérifiant les hypothèses du théorème$\}$

→ Etape 1 : $\forall n$, $\mathcal{A}_n$ est fini.

Soit $\sigma_j \in \mathbb{Z}[T_1, \dots, T_n]$ le j-ième polynôme élémentaire symétrique, de sorte que pour $Q \in \mathcal{A}_n$, et pour $z_1, \dots, z_n$ ses racines,

$$Q(X) = \prod_{k=1}^{n} (X - z_k) = \sum_{j=0}^{n} \underbrace{(-1)^n \sigma_j(z_1, \dots, z_n)}_{:= c_j} X^{n-j}$$

Or, comme $Q \in \mathbb{Z}[X]$, $c_j \in \mathbb{Z}$. De plus, par les relations coefficients-racines :

$$|c_j| \leq |\sigma_j(z_1, \dots, z_n)| \leq \sum_{1 \leq k_1 < \dots < k_j \leq n} \prod_{\ell=1}^{j} |\lambda_{k_j}|$$

$$\leq \sum_{1 \leq k_1 < \dots < k_j \leq n} 1 = \binom{n}{j}$$

Ainsi, les c_j ont tous un nombre fini de possibilités, donc puisque Q est entièrement déterminé par ses coefficients, $\mathcal{A}_n$ est fini.

→ Etape 2 : Soit $P \in \mathcal{A}_n$ et $z_1, \dots, z_n$ ses racines. On note $P_k := \prod_{j=1}^{n} (X - z_k^j) \in \mathbb{C}[X]$. On va montrer que $\forall k \geq 1$, $P_k \in \mathcal{A}_n$.

Considérons M la matrice compagnon de P. Alors, $M \in \mathcal{M}_n(\mathbb{Z})$ car $P \in \mathbb{Z}[X]$. Dans $\mathbb{C}$, M se trigonalise, et on a l'existence de $Q \in \mathcal{M}_n(\mathbb{C})$ tq.

$$M = Q \begin{bmatrix} z_1 & & * \\ & \ddots & \\ (0) & & z_n \end{bmatrix} Q^{-1}$$

$$\forall k \geq 1, \quad M^k = Q \begin{bmatrix} z_1^k & & * \\ & \ddots & \\ (0) & & z_n^k \end{bmatrix} Q^{-1}.$$

On remarque alors que P_k est le polynôme caractéristique de $M^k \in \mathcal{M}_n(\mathbb{Z})$.

Donc, $P_k \in \mathbb{Z}[X]$.

De plus, P_k est de degré n, n'a pas 0 pour racines et puisque $\forall n \geq 1$, $|z_n| \leq 1$, alors, $\forall k \geq 1$, $\forall n \geq 1$, $|z_n^k| \leq 1$. D'où, $P_k \in A_n$.

→ Etape 3 : Conclusion.

$\# A_n < +\infty$ et pour chaque polynôme de A_n, le nombre de racines est fini. Ainsi, le nombre de racines d'éléments de A_n est fini.

Soit $P \in A_n$ et z une de ses racines. $\forall k \in \mathbb{N}^*$, $P_k \in A_n$ et z^k est une de ses racines.

infini !

Donc $\exists k \neq l$ tq. $z^k = z^l$ par le principe des tiroirs.

Comme $z \neq 0$, $z^{|k-l|} = 1$ et z est une racine de l'unité.

Application: Si de plus, P est irréductible, alors, P est un polynôme cyclotomique.

Preuve: Par le théorème précédent, toutes les racines de P sont des racines de l'unité. En notant alors N le produit des ordres des racines de P, on a :

$$P \mid (X^N - 1)^n .$$

Or, la décomposition en irréductible de $X^N - 1$ est :

$$X^N - 1 = \prod_{d \mid N} \Phi_d .$$

Par unicité de la décomposition en facteurs premiers de $(X^N - 1)^n$, il existe $d \mid N$ tq. $P = \Phi_d$

Remarques:

- Développement très classique, mais qui est sympa et qui passe bien dans le temps imparti sans se presser.
- Pour l'étape 2, il y a d'autres versions: par les polynômes élémentaires, ou encore le résultant. La preuve que j'ai choisie ne nécessite pas de théorème exotique, je trouve que c'est la plus simple.
- Bien savoir montrer (ou à défaut, expliquer) les relations coefficients-racines.