Théorème de Kronecker

Alexis Guérin

Merci à Laurent Montaigu d'avoir trouvé la deuxième partie qui rend ce développement original et surtout m'a permis d'éviter toutes les "applications" de Kronecker, qui, lorsque l'on y réfléchis, n'en sont pas vraiment. Il n'y a pas de référence pour la seconde partie du développement.
Leçons concernées : 102, 144.

Théorème (Théorème de Kronecker)
Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.

Preuve Notons $\Omega_n = \{P \in \mathbb{Z}[X] \text{ tel que } \mathcal{Z}(P) \subset \mathcal{D}(0,1) \text{ et de degré } n\}$. Montrons dans un premier temps que Ω_n est de cardinal fini.
Soit $P = \sum_{i=1}^{n} a_i X^i$ et $z_1, \dots, z_n$ les racines de P. En utilisant les relations coefficients racines de la propriété **??** on peut écrire :

$$|a_{n-i}| = |\Sigma_{i,n}(z_1, \dots, z_n)| \leqslant \sum_{1 \leqslant i_1 < \dots < i_j \leqslant n} 1 = \binom{n}{i}.$$

De plus comme pour tout i, $a_i \in \mathbb{Z}$, cela nous montre qu'il existe un nombre fini de polynômes dans Ω_n.
On note maintenant $P_k = (X - z_1^k) \dots (X - z_n^k) = \sum_{i=0}^{n} c_{j,k} X^{n-i}$. Montrons que pour tout k entier naturel non nul, $P_k \in \Omega_n$.
Par construction des $c_{j,k}$, ce sont des polynômes symétriques à coefficients entiers en les z_i. Ainsi d'après le théorème de structure des polynômes symétriques, il existe $R_{j,k}$, un polynôme à coefficients entiers, tel que

$$c_{j,k} = R_{j,k}(\Sigma_{1,n}(z_1, \dots, z_n), \dots, \Sigma_{n,n}(z_1, \dots, z_n)).$$

Où $\Sigma_{i,j}$ est le j-ème polynôme symétrique élémentaire de degré j. Par conséquent, comme les $\Sigma_{j,n}(z_1, \dots, z_n)$ sont les coefficients de P, ils appartiennent à $\mathbb{Z}$, donc $c_{j,k} \in \mathbb{Z}$. Ainsi on a bien $P_k \in \Omega_n$.
Le cardinal de Ω_n étant fini, l'ensemble des racines des polynômes de Ω_n est donc lui aussi de cardinal fini. Ainsi, pour $i \in [\![1, n]\!]$, si on considère l'application $k \longmapsto z_i^k$, qui va de $\mathbb{N}$ (de cardinal infini) dans l'ensemble des racines des polynômes de Ω_n (de cardinal fini), elle ne peut pas être injective. Donc il existe $k, k' \in \mathbb{N}$ différents l'un de l'autre, tel que $z_i^k = z_i^{k'}$, ce qui s'écrit aussi $z_i^{k-k'} = 1$ avec $k - k' \neq 0$. Donc pour tout i, z_i est une racine de l'unité.

□

Corollaire Soit P un polynôme unitaire de $\mathbb{Z}[X]$ de degré n. On suppose que les racines complexes de P sont non nulles et contenues dans le disque unité de $\mathbb{C}$. Alors P est un produit de polynômes cyclotomiques.
Dans la suite, on notera A_n l'ensemble de ces polynômes.

Preuve Soit P un tel polynôme et Q un facteur irréductible de P dans $\mathbb{Z}[X]$. Alors Q vérifie les hypothèses du théorème de Kronecker et n'admet donc comme racines que des racines de l'unité (0 n'étant pas racine de P par hypothèse). En notant N le ppcm des ordres des racines de Q, il en découle que Q divise $X^N - 1$ dans $\mathbb{Q}[X]$. Or, les polynômes cyclotomiques vérifient la formule suivante,

$$X^N - 1 = \prod_{d|N} \Phi_d,$$

où $\Phi_n \in \mathbb{Q}[X]$ désigne le n-ième polynôme cyclotomique sur $\mathbb{Q}$. Puisque Q est irréductible dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$), ainsi que les Φ_n, il existe $d|N$ tel que $\Phi_d = Q$.

□

Propriété Pour tout entier $n \geqslant 1$, notons $a_n := \#A_n$. Alors la série entière $\sum_{n\geqslant 1} a_n z^n$ a un rayon de convergence supérieur ou égal à 1 et

$$\sum_{n\geqslant 1} a_n z^n = \prod_{n\geqslant 1} \frac{1}{1 - z^{\varphi(n)}},$$

où φ désigne l'indicatrice d'Euler.

Lemme Pour tout entier $n \geqslant 1$, $\varphi(n) \geqslant \sqrt{\frac{n}{2}}$. En particulier $\lim_{n\to+\infty} \varphi(n) = +\infty$.

Lemme Pour tout complexe z tel que $|z| < 1$, la série $\sum_{n\geqslant 1} a_n z^n$ et le produit infini $\prod_{n\geqslant 1} \frac{1}{1-z^{\varphi(n)}}$ convergent.

Preuve Soit $P \in A_n$ alors, grâce au corollaire du théorème de Kronecker, il existe des entiers naturels non nuls, $k_1, \ldots, k_r$ tels que $P = \prod_r^{i=1} \Phi_{k_i}$, de plus on a l'égalité

$$n = \sum_{i=1}^{r} \deg(\Phi_{k_i}) = \sum_{i=1}^{k} \varphi(k_i).$$

Inversement, si P est un produit de polynôme cyclotomiques alors il est évident que $P \in A_n$. On a donc une bijection entre A_n et l'ensemble

$$C_n = \left\{ (y_k)_k \in \mathbb{N}^{\mathbb{N}} \text{ tel que } \sum_{k=1}^{+\infty} y_k \varphi_k = n \right\}.$$

Ce qui nous permet d'affirmer que $\#C_n = a_n$.
Soient $|z| < 1$ et $n \in \mathbb{N}^*$ on note $f_n(z) = \prod_{k=1}^{n} \frac{1}{1-z^{\varphi(k)}}$ on a alors que :

$$\begin{aligned} f_n(z) = \prod_{i=1}^{n} \frac{1}{1 - z^{\varphi(k)}} &= \prod_{k=1}^{n} \sum_{l=0}^{+\infty} z^{l\varphi(k)} \\ &= \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} z^{i_1\varphi(1)+\ldots+i_n\varphi(n)} \\ &= \sum_{m}^{+\infty} c_{n,m} z^m. \end{aligned}$$

où $c_{n,m} = \#\left\{(y_1, \ldots, y_n) \in \mathbb{N}^n \mid y_1\varphi(1) + \ldots y_n\varphi(n) = m\right\}$.
En remarquant que pour $m \leqslant \varphi(n)$ (ce qui est possible grâce au lemme), $c_{n,m} = \#C_n = a_n$, on a alors :

$$\begin{aligned}\left|\sum_{m=1}^{+\infty} a_m z^m - f_n(z)\right| &\leqslant \sum_{m=1}^{+\infty} |a_m - c_{n,m}||z|^m \\ &\leqslant \sum_{m\leqslant\varphi(n)} |a_m - c_{n,m}||z|^m + \sum_{m\geqslant\varphi(n)} a_m|z|^m \\ &\leqslant \sum_{m\geqslant\varphi(n)} a_m|z|^m \underset{n\to+\infty}{\longrightarrow} 0 \quad \text{(par lemme)}.\end{aligned}$$

L'avant dernière inégalité ayant lieu car $a_m \geqslant c_n, m \geqslant 0$. De plus comme pour $|z| < 1$,

$$f_n(z) \underset{n\to+\infty}{\longrightarrow} \prod_{k=1}^{+\infty} \frac{1}{1 - z^{\varphi(k)}},$$

nous avons donc prouvé le résultat.

□

Le lemme se prouve dans un premier temps pour des puissances de nombres premiers, puis pour le cas général, grâce à un raisonnement par récurrence. Pour la preuve du lemme , la convergence absolue du produit se prouve par un passage au log puis en utilisant un équivalent classique du terme dans la somme obtenue. Pour la convergence de la série entière de coefficient a_n, l'idée est d'utiliser le fait que $a_n = \sum_{m=0}^{\infty} c_{n,m}$ et la convergence du produit pour conclure.