7 Théorème de Gauss (polygones réguliers constructibles)

On admet le théorème de Wantzel, qui donne une condition nécessaire et suffisante pour qu'un point du plan complexe soit constructible à la règle et au compas (sous-entendu, étant donnés les deux points d'affixes respectives 0 et 1) :

Théorème (Wantzel). *Un point d'affixe z est constructible si et seulement si z est dans une extension L de $\mathbb{Q}$ telle qu'il existe une tour d'extensions $\mathbb{Q} = L_0 \subsetneq L_1 \subsetneq ... \subsetneq L_r = L$ avec $[L_i : L_{i-1}] = 2$ $\forall i$.*

On propose de démontrer le théorème suivant :

Théorème (Gauss). *« Le » polygone régulier à n côtés ($n \geqslant 3$) est constructible si et seulement si n est de la forme $2^s p_1 ... p_r$, où les p_i sont des nombres premiers de* Fermat *distincts.*

Pour simplifier, on suppose qu'il s'agit du polygone régulier à n côtés inscrit dans le cercle unité de $\mathbb{C}$, et dont un des sommets est 1 (sinon, il faut supposer que l'on connaît un des côtés).

Rappelons qu'un nombre premier de Fermat est un nombre premier de la forme $2^k + 1$. On montre que k est nécessairement lui-même une puissance de 2.

Preuve.
Commençons par remarquer qu'une condition nécessaire et suffisante pour que le polygone régulier à n sommets soit constructible est que le nombre $\omega_n = e^{2i\pi/n}$ soit constructible.

On commence par supposer que ω_n est constructible, il s'agit de montrer que n est de la forme annoncée.

On écrit *a priori* la décomposition de n en irréductibles : $n = 2^s {p_1}^{\alpha_1} ... {p_r}^{\alpha_r}$, où les p_i sont des nombres premiers $\geqslant 3$ deux à deux distincts et les α_i sont des entiers $\geqslant 1$.

Il est clair que si ω_n est constructible, alors ω_d est constructible si $d|n$ (par exemple, parce que $\omega_d = {\omega_n}^{n/d}$). On en déduit que les $\omega_{{p_i}^{\alpha_i}}$ sont constructibles. Or le polynôme minimal de $\omega_{{p_i}^{\alpha_i}}$ sur $\mathbb{Q}$ est $\phi_{{p_i}^{\alpha_i}}$ (car les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$), qui est de degré $\varphi({p_i}^{\alpha_i}) = {p_i}^{\alpha_i - 1}(p_i - 1)$. On a donc $[\mathbb{Q}(\omega_{{p_i}^{\alpha_i}}) : \mathbb{Q}] = {p_i}^{\alpha_i - 1}(p_i - 1)$, qui doit être une puissance de 2 d'après le théorème de Wantzel. On en déduit que p_i est un nombre de Fermat et $\alpha_i = 1$. n est donc de la forme annoncée.

Réciproquement, soit n un nombre entier $\geqslant 3$ de la forme $2^s p_1 ... p_r$, où les p_i sont des nombres premiers de Fermat distincts, et montrons que ω_n est constructible.

Commençons par remarquer que si deux nombres a et b sont premiers entre eux et tels que ω_a et ω_b sont constructibles, alors ω_{ab} est constructible. En effet, il existe alors deux entiers u et v tels que $au + bv = 1$ (théorème de BEZOUT), il suffit alors d'écrire que $\omega_{ab} = {\omega_a}^u {\omega_b}^v$. Par suite, il nous suffit de montrer que ω_{2^s} et les ω_{p_i} sont constructibles.

Il est clair que ω_{2^s} est constructible, d'après le théorème de WANTZEL : la tour $\mathbb{Q} \subset \mathbb{Q}[\omega_4] \subset ... \subset \mathbb{Q}[\omega_{2^s}]$ convient.

Il nous reste donc à montrer que $\omega = \omega_p$ est constructible si p est un nombre premier de FERMAT.

Le groupe $G = \mathcal{G}al(\mathbb{Q}[\omega]|\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$ par $\sigma \mapsto m$ tel que $\sigma(\omega) = \omega^m$. Ainsi G est cyclique d'ordre $p - 1 = 2^q$.

Soit σ un générateur de G, et posons $L_k = \{z \in \mathbb{Q}(\omega), \sigma^{2^k}(z) = z\}$ pour $0 \leqslant k \leqslant q$. Les L_k sont des sous-corps de $\mathbb{Q}(\omega)$, et on a une tour d'extension $\mathbb{Q} = L_0 \subset ... \subset L_q = \mathbb{Q}(\omega)$.

De plus, $L_{k-1} \subsetneq L_k$. En effet, posons $x = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^k m}(\omega)$. D'une part, il est clair que $x \in L_k$. D'autre part, $x \notin L_{k-1}$, car sinon on aurait $\sum_{m=0}^{2^{q-k}-1} \sigma^{2^{k-1}2m}(\omega) = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^{k-1}(2m+1)}(\omega)$, ce qui est une égalité entre deux combinaisons linéaires différentes des éléments de la base $(1, \omega, ..., \omega^{p-1})$ de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$.

Ainsi, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^q = [L_q : L_{q-1}]...[L_1 : L_0]$ où $[L_k : L_{k-1}] > 1 \ \forall k$. On a donc nécessairement $[L_k : L_{k-1}] = 2 \ \forall k$. Ceci prouve que ω est constructible. □

Signalons que la dernière partie de la démonstration est réduite à presque rien dès lors qu'on connaît le théorème de correspondance de GALOIS.

Leçons possibles
(**109** Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.)
110 Nombres premiers. Applications.
(**112** Corps finis. Applications.)
(**113** Groupe des nombres complexes de module 1. Applications.)
(**116** Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.)
(**118** Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.)
(**120** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications)
(**139** Applications des nombres complexes à la géométrie.)
140 Angles : Définitions et utilisation en géométrie.
(**141** Utilisation des groupes en géométrie.)

143 Constructions à la règle et au compas.
144 Problèmes d'angles et de distances en dimension 2 ou 3.

Références
[CL05]