Théorème de Gauss Wantzel

Alexis Guérin

Leçons concernées : 102, 125, 151, 191

Propriété Soient $n \in \mathbb{N}^*$ plus grand que 3 alors un polygone régulier à n côtés est constructible si et seulement si $\zeta_n = e^{\frac{2i\pi}{n}}$ est constructible.

Lemme Soient $n, m \in \mathbb{N}^*$ tel que $n \wedge m = 1$ alors ζ_{nm} est constructible si et seulement si ζ_n et ζ_m le sont.

Théorème de Gauss Wantzel
Les polygones réguliers constructibles sont ceux dont le nombre de côtés n est de la forme 2^α avec $\alpha \geqslant 2$ ou de la forme $2^\alpha p_1 \dots p_r$ avec $\alpha \in \mathbb{N}$ et où les p_i sont des nombres premiers distincts qui sont des nombres de Fermat (de la forme $2^m + 1$).

Preuve On va raisonner par double implication.

• On suppose que $\zeta_n = e^{\frac{2i\pi}{n}}$ est constructible, alors avec le lemme précédent on peut supposer que $n = p^\alpha$ avec p un nombre premier et $\alpha \in \mathbb{N}^*$. Or, si ζ_{p^α} est constructible, alors par le corollaire du théorème de Wantzel $[\mathbb{Q}(\zeta_{p^\alpha}) : \mathbb{Q}] = 2^m$ avec $m \in \mathbb{N}$. D'une autre part, on peut également affirmer que , $[\mathbb{Q}(\zeta_{p^\alpha}) : \mathbb{Q}] = \varphi(p^\alpha)$ (car le polynôme minimal de ζ_{p^α} sur $\mathbb{Q}$ est le n-ème polynôme cyclotomique) et comme $\varphi(p^\alpha) = p^{\alpha-1}(p-1) = 2^m$ on a alors deux possibilités :

$$p^\alpha = 2^{m+1} \quad \textbf{ou} \quad \alpha = 1 \text{ et } \quad p = 2^m + 1$$

Ce qui achève la première implication.

• Pour la seconde implication, on commence par remarquer que les les ζ_{2^m} sont constructible (car on sait construire à la règle et on compas la bissectrice d'un angle). Soit $p = 2^m + 1$, un nombre premier de Fermat. Montrons qu'il est constructible en utilisant le théorème de Wantzel.
On pose $K = \mathbb{Q}(\zeta_p)$. On remarque que $[K : \mathbb{Q}] = p-1$ (car le degré du p-ème polynôme cyclotomique Φ_p est $p-1$) et qu'une $\mathbb{Q}$-base de K est donnée par $\mathcal{B} = \left(\zeta_p, \dots, \zeta_p^{p-1}\right)$. On note $G = Aut_{\mathbb{Q}}(K)$, montrons que G est un groupe cyclique. Pour cela, on va exhiber un isomorphisme de groupe entre G et $(\mathbb{Z}/p\mathbb{Z})^*$.

Soit $g \in G$ alors, par les propriétés des morphismes de corps, g est entièrement déterminé par sa valeur en ζ_p. Or,

$$\Phi_p(g(\zeta_p)) = g(\Phi_p(\zeta_p)) = 0$$

donc $g(\zeta_p)$ est dans l'ensemble des racines de Φ_p qui sont les ζ_p^i avec $i \in [\![1, p-1]\!]$. Réciproquement, on considère le morphisme surjectif

$$\tilde{g}_i : \left| \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{Q}(\zeta_p) \\ P & \longmapsto & P(\zeta_p^i) \end{array} \right.$$

de noyau $Ker(\tilde{g}_i) = \langle \Phi_p \rangle$. Donc $\tilde{g}_i$ induit l'automorphisme de corps $g_i \quad : \quad \mathbb{Q}(\zeta_p) \simeq {}^{\mathbb{Q}[X]}/_{\langle \Phi_p \rangle} \longrightarrow \mathbb{Q}(\zeta_p)$ tel que $g_i(\zeta_p) = \zeta_p^i$. On a donc prouvé que $G \simeq (\mathbb{Z}/p\mathbb{Z})^*$ par l'isomorphisme de groupe

$$\begin{array}{rcl} (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & G \\ i & \longmapsto & g_i \end{array}$$

En particulier, comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$, G l'est aussi. Soit g_0 un générateur de G.

On va maintenant appliquer le théorème de Wantzel. On commence par remarquer que g_0 est d'ordre $p-1 = 2^m$. On pose alors pour tout $i \in [\![1, m]\!]$, $\tau_i = g^{2^i}$ et $K_i = \{x \in K \text{ tel que } \tau_i(x) = x\}$ qui est un sous corps de K contenant $\mathbb{Q}$. On a de plus $K_0 \subset \ldots \subset K_m$. Verifions que cette chaine d'extension verifie bien les hypothéses du théorème de Wantzel :

$\rightarrow$ Prouvons que $K_0 = \mathbb{Q}$. On a déjà $\mathbb{Q} \subset K_0$. Soit $x \in K_0$ alors comme g_0 est d'ordre $p-1$ pour tous $k, l \in [\![1, p-1]\!]$ avec $k \neq l$ $g_0^k(\zeta_p) \neq g_0^l(\zeta_p)$ (car sinon $g_0^k = g_0^l$ ce qui contredit l'ordre de g_0) donc $\left(g_0^i(\zeta_p)\right)_{1 \leqslant i \leqslant p-1} = \left(\zeta_p^i\right)_{1 \leqslant i \leqslant p-1} = \mathcal{B}$ donc est une base du $\mathbb{Q}$-espace vectoriel K. Ainsi il existe une famille de p éléments de $\mathbb{Q}$ noté $(\lambda_i)_{1 \leqslant i \leqslant p-1}$ tel que

$$x = \sum_{i=1}^{p-1} \lambda_i g_0^i(\zeta_p).$$

Or comme $g_0(x) = x$, on obtient que $\lambda_1 = \ldots = \lambda_{p-1}$, de plus on a la formule

$$\sum_{i=1}^{p-1} g_0^i(\zeta_p) = \sum_{i=1}^{p-1} \zeta_p^i = -1.$$

Donc $x = -\lambda_1 \in \mathbb{Q}$, donc $K_0 = \mathbb{Q}$.

$\rightarrow$ Comme $\tau_m = id_K$ on a immédiatement que $K_m = K$.

$\rightarrow$ Prouvons que $[K_{i+1} : K_i] = 2$. Pour cela on va d'abord montrer que $K_i \subsetneq K_{i+1}$. Soit

$$z = \sum_{h=0}^{2^{m-i-1}-1} g_0^{2^{i+1}h}(\zeta_p).$$

On a alors :

$$g_0^{2^{i+1}}(z) = \sum_{h=0}^{2^{m-i-1}-1} g_0^{2^{i+1}(h+1)}(\zeta_p) = \sum_{h=1}^{2^{m-i-1}-2} g_0^{2^{i+1}h}(\zeta_p) + g_0^{2^{i+1}2^{m-i-1}}(\zeta_p) = z.$$

Donc $z \in K_{i+1}$ et

$$g_0^{2^i}(z) = \sum_{h=0}^{2^{m-i-1}-1} g_0^{2^{i+1}h+2^i}(\zeta_p).$$

Or $0 < 2^{i+1}h + 2^i < 2^m$ pour tout $h \in [\![0, 2^{m-i-1} - 1]\!]$ ainsi, comme $\left(g_0^i(\zeta_p)\right)_{1 \leqslant i \leqslant p-1}$ est une base de K et que les coefficients devant $\zeta_p = g_0^{p-1}(\zeta_p)$ ne sont pas les mêmes pour z et $g_0^{2^i}(z)$ on peut affirmer que $z \notin K_i$. Donc $K_i \subsetneq K_{i+1}$ et en particulier $[K_{i+1} : K_i] > 1$.

Pour finir le théorème de la base télescopique nous permet d'affirmer que

$$\underbrace{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}_{=2^m} = \prod_{i=1}^{m} \underbrace{[K_{i+1} : K_i]}_{>1}.$$

Donc $[K_{i+1} : K_i] = 2$.

Le théorème de Wantzel nous permet de conclure que ζ_p est constructible.

□

Théorème de Wantzel
Soit $z \in \mathbb{C}$, z est constructible si et seulement s'il existe un entier $p \geqslant 1$ et une suite de sous-corps de $\mathbb{C}$, $L_1, L_2, \ldots, L_p$ tels que :

- $L_1 = \mathbb{Q}$
- $\forall 1 \leqslant j \leqslant p-1 \quad L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
- $z \in L_p$