Théorèmes de Wantzel et de Gauss

Achille Méthivier

Théorème 1 (Théorème de Wantzel)**.** *Soit S une partie de $\mathbb{C}$ contenant 0 et 1, L le sous-corps de $\mathbb{C}$ engendré par S et $\bar{S}$ et $z \in \mathbb{C}$. Les conditions suivantes sont équivalentes.*

1. *z est constructible à partir de S,*
2. *Il existe des extensions $L = L_0 \subset L_1 \subset \cdots \subset L_r \subset \mathbb{C}$ telles que $z \in L_r$ et $[L_{i+1} : L_i] = 2$.*

Lemme 2 (Admis)**.** *L'ensemble des nombres constructibles à partir de S est le plus petit sous-corps de $\mathbb{C}$ contenant S, stable par conjugaison et par racine carré.*

Démonstration du théorème. On va seulement montrer que $(1) \implies (2)$ (le sens qui nous intéresse). Notons D l'ensemble des complexes qui vérifient la condition (2) et montrons que $C(S) \subset D$. Soient $\alpha, \beta \in D$. Il existe $u_1, \ldots, u_r, v_1, \ldots, v_s \in \mathbb{C}$ vérifiant :

$$u_1^2 \in L, \quad u_2^2 \in L(u_1), \ \ldots \ , u_r^2 \in L(u_1, \ldots, u_{r-1}), \ \alpha \in L(u_1, \ldots, u_r),$$
$$v_1^2 \in L, \quad v_2^2 \in L(v_1), \ \ldots \ , v_s^2 \in L(v_1, \ldots, v_{s-1}), \ \beta \in L(v_1, \ldots, v_s).$$

Alors

$$u_1^2 \in L, \quad u_2^2 \in L(u_1), \ \ldots \ , u_r^2 \in L(u_1, \ldots, u_{r-1}), \ \alpha \in L(u_1, \ldots, u_r),$$
$$v_1^2 \in L(u_1, \ldots, u_r), \quad v_2^2 \in L(u_1, \ldots, u_r, v_1), \ \ldots \ , v_s^2 \in L(u_1, \ldots, u_r, v_1, \ldots, v_{s-1}),$$
$$\alpha, \beta \in L(v_1, \ldots, v_s, u_1, \ldots, u_r).$$

Finalement, $\alpha + \beta \in D$, $\alpha\beta \in D$ et si $\alpha \neq 0$, $\alpha^{-1} \in D$. Donc D est un sous-corps de $\mathbb{C}$ stable par racine carré. Et comme L est stable par conjugaison, il vient que $L = \bar{L}$ et donc $\overline{L(u_1, \ldots, u_{r-1})} = L(\overline{u_1}, \ldots, \overline{u_{r-1}})$. D'après le lemme précédent, $C(S) \subset D$. □

Théorème 3 (Théorème de Gauss)**.** *Soit $n \in \mathbb{N}\backslash\{0, 1, 2\}$. Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est de la forme $n = 2^s F(n_1) \cdots F(n_r)$, où $F(k) = 2^{2^k} + 1$, le k-ième nombre de Fermat, avec les $F(n_i)$ premiers entre eux.*

Lemme 4. *Soit $m \in \mathbb{N}^*$. Si l'entier $2^m + 1$ est premier, m est une puissance de 2.*

Démonstration. On peut toujours écrire $m = 2^q(2r + 1)$. Supposons que m n'est pas une puissance de 2, c'est-à-dire $r \geq 1$. En posant $s = 2^{2^q}$, il vient que

$$2^m + 1 = s^{2r+1} + 1 = (s + 1) \sum_{i=1}^{2r} (-1)^i s^{2r-i}.$$

Comme $2 \leq s + 1 < 2^m + 1$ car $r \geq 1$. Ainsi, $2^m + 1$ n'est pas premier. □

Lemme 5. *Soit $n \in N\backslash\{0, 1\}$. Les conditions suivantes sont équivalentes.*

1. *$\varphi(n)$ est une puissance de 2.*
2. *On a $n = 2^s p_1 \cdots p_r$ avec $p_1, \ldots, p_r$ premiers impairs, distincts deux à deux et tels que $p_i - 1$ soit une puissance de 2.*

Démonstration. Écrivons la décomposition en facteurs premiers de n

$$n = 2^s p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

On a donc l'expression de $\varphi(n)$

$$\varphi(n) = 2^{s-1} p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1} (p_1 - 1) \cdots (p_r - 1).$$

Le résultat en découle immédiatement car si $\alpha_i - 1 \leq 1$, alors $p_i | \varphi(n)$. □

Démonstration du théorème. On démontre uniquement le sens direct. Soit $n \in \mathbb{N}\backslash\{0, 1, 2\}$. Polygone régulier à n côtés est constructible si et seulement si ses sommets le sont. Or, $\zeta = \mathrm{e}^{2i\pi/n}$, racine n-ième primitive de l'unité, est un des sommets du polygones, les autres étant donnés par les ζ^k, $1 \leq k \leq n - 1$. Comme l'ensemble des nombre constructibles est un corps, il suffit de montrer que ζ est constructible. Par définition, ζ est racine du polynôme cyclotomique Φ_n

$$\Phi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} (X - \zeta^k).$$

On a donc $\deg(\Phi_n) = \varphi(n)$. Or, Φ_n est unitaire, irréductible et à coefficients rationnels (et même entiers), donc c'est le polynôme minimal de ζ sur $\mathbb{Q}$ et on a

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

De plus, d'après le théorème de Wantzel, il existe $\mathbb{Q} \subset L_1 \subset \cdots \subset L_r \subset \mathbb{C}$, suite d'extensions telles que $[L_{i+1} : L_i] = 2$ et $\zeta \in L_r$. Par définition, $\mathbb{Q}(\zeta) \subset L_r$ et par multiplicativité des degrés,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] \ \Big| \ [L_r : \mathbb{Q}] = 2^q.$$

Donc $\varphi(n)$ divise 2^q, c'est une puissance de 2 et on conclut grâce au lemme. □

I Références

1. Corps commutatifs et théorie de Galois, Patrice Tauvel (page 205)