# Théorèmes de Wantzel et Gauss

**Notations/Définitions :**

- On note $\varphi$ la fonction indicatrice d'Euler
- Si $n \in \mathbb{N}$ on note $F(n) := 2^{2^n} + 1$ le $n$ème nombre de Fermat
- Pour la définition d'un ensemble constructible on se réfère à la définition de Tauvel dans son ouvrage "Corps commutatifs et théorie de Galois", page 196

**Théorème de Wantzel (sens direct):** Soit $z \in \mathbb{C}$. On note $D$ l'ensemble des points $z$ vérifiant la condition suivante :

$(*)$ Il existe des extension $\mathbb{Q} = L_0 \subset ... \subset L_r$ contenues dans $\mathbb{C}$ tels que $z \in L_r$ et $[L_{i+1}L_i] = 2$ pour tout $0 \leq i \leq r-1$.

Alors l'ensemble $C$ des nombres constructibles est inclus dans $D$.

**Théorème de Gauss (sens direct) :** Soit $n \in \mathbb{N} \setminus \{0, 1, 2\}$. Si les sommets du polygone régulier à $n$ côtés sont constructibles, alors $n$ est de la forme

$$n = 2^s F(n_1)...F(n_i)$$

où les $n_i$ sont distincts 2 à 2 et $F(n_i)$ est premier pour tout $i$.

**Lemme 0 :** L'ensemble $C$ des points constructibles de $\mathbb{C}$ est le plus petit sous-corps de $\mathbb{C}$ contenant $\{0, 1\}$ qui est stable par racine carrée et conjugaison.

**Lemme 1 :** Soit $k$ un corps de caractéristique différente de 2 et $k \subset K$ une extension de degré 2. Il existe $x \in K$ tel que $x^2 \in k$ et $K = k(x)$.

**Lemme 2 :** Si $n \in \mathbb{N} \setminus \{0, 1\}$ et $\varphi(n)$ est une puissance de 2 alors le nombre $n$ est de la forme

$$n = 2^s F(n_1)...F(n_i)$$

où les $n_i$ sont distincts 2 à 2 et $F(n_i)$ est premier pour tout $i$.

---

**Preuve du lemme 0 :** Admis. □

**Preuve du lemme 1 :** Soit $y \in K$. On sait que son polynôme annulateur est de degré au plus 2 donc est de degré 2 (sinon $y \in k$) et est de la forme $X^2 + aX + b$. On sait que ses racines sont de la forme $\dfrac{-1 \pm \sqrt{a^2 - 4b}}{2}$

donc $2y = -a \pm x$ en posant $x = \sqrt{a^2 - 4b}$. Finalement, $k(x)$ est un corps compris entre $k$ et $K$ de degré strictement plus grand que 1 (car $x \notin k$, sinon $y$ y serait aussi) donc $k(x) = K$ et $x^2 \in k$. □

**Preuve du théorème de Wantzel (sens direct) :** Grâce au lemme 0 ,comme $\{0, 1\} \subset D$, il suffit de montrer que $D$ est un corps stable par racine carrée et conjugaison. Soit $\alpha$ et $\beta$ deux éléments de $D$. En utilisant la condition $(*)$ et le lemme 1, il existe alors $u_1, ..., u_r$ et $v_1, ..., v_s$ tels que

$$\mathbb{Q} \subset \mathbb{Q}(u_1) \subset ... \subset \mathbb{Q}(u_1, ..., u_r), \alpha \in \mathbb{Q}(u_1, ..., u_r) \text{ avec } [\mathbb{Q}(u_1, ..., u_{i+1}) : \mathbb{Q}(u_1, ..., u_i)] = 2 \text{ pour tout } i$$
$$\mathbb{Q} \subset \mathbb{Q}(v_1) \subset ... \subset \mathbb{Q}(v_1, ..., v_s), \beta \in \mathbb{Q}(v_1, ..., v_s) \text{ avec } [\mathbb{Q}(v_1, ..., v_{i+1}) : \mathbb{Q}(v_1, ..., v_i)] = 2 \text{ pour tout } i$$

On a alors

$$\alpha, \beta \in K := \mathbb{Q}(u_1, ..., u_r, v_1, ..., v_s).$$

Quitte à enlever les $v_i$ tels que $v_i \in \mathbb{Q}(u_1, ..., u_r, v_1, ..., v_{i-1})$, on peut supposer que la concaténation de nos extensions forme une tour d'extensions de degré 2. Comme $K$ est un corps, $\alpha\beta$, $\alpha + \beta$, $\alpha^{-1}$ (si $\alpha \neq 0$) $\in K$ donc $D$ est un sous-corps de $\mathbb{C}$.

Si $z^2 \in D$, il existe $u_1, ..., u_r$ tels que

$$\mathbb{Q} \subset \mathbb{Q}(u_1) \subset ... \subset \mathbb{Q}(u_1, ..., u_r), \alpha \in \mathbb{Q}(u_1, ..., u_r) \text{ avec } [\mathbb{Q}(u_1, ..., u_{i+1}) : \mathbb{Q}(u_1, ..., u_i)] = 2 \text{ pour tout } i.$$

On sait alors que $z \in \mathbb{Q}(u_1, ..., u_r, z)$ et que cette extension est au plus de degré 2 car $X^2 - z^2$ annule $z$. Donc $z \in D$ et $D$ est stable par racine carrée.

Comme $\mathbb{Q}$ est stable par conjugaison, $\overline{\mathbb{Q}(u_1, ..., u_r)} = \mathbb{Q}(\overline{u_1}, ..., \overline{u_r})$ donc $D$ est bien stable par conjugaison.

Finalement, $D$ est comme voulu, d'où le résultat. □

**Preuve du lemme 2 :** On peut écrire la décomposition en facteurs premiers de $n = 2^s p_1^{\alpha_1} ... p_r^{\alpha_r}$. On sait que l'indicatrice d'Euler est multiplicative donc

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

Pour que $\varphi(n)$ soit une puissance de 2 il faut que en particulier que les $p_i - 1$ soit une puissance de 2 et donc il existe $m_i$ tels que $p_i = 2_i^m + 1$. Soit $m$ un des $m_i$ et montrons que c'est une puissance de 2. On peut toujours écrire un nombre sous la forme $m = 2^q(2r + 1)$. Supposons par l'absurde que $r \geq 1$. En posant $s = 2^{2^q}$ il vient

$$2^m + 1 = s^{2r+1} + 1 = (s + 1) \sum_{i=0}^{2r} (-1)^i s^{2r-i}.$$

Comme on a $2 \leq s + 1 < 2^m + 1$, le nombre $2^m + 1$ admet un diviseur différent de 1 ou lui-même et n'est donc pas premier, ce qui est absurde, d'où le résultat. □

**Preuve du théorème de Gauss (sens direct) :** Si les sommets du $n$-polygone régulier sont constructible, le nombre $\zeta := e^{\frac{2i\pi}{n}}$ est constructible. Par définition il est annulé par le polynôme cyclotomique $\phi_n$ qui est irréductible, unitaire et à coefficients entiers. C'est donc le polynôme minimal de $\zeta$ sur $\mathbb{Q}$. On sait aussi que $\deg(\phi_n) = \varphi(n)$ et donc

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

Par le théorème de Wantzel on sait qu'il existe une extension $L$ de $\mathbb{Q}$ de degré $2^q$ avec $q$ entier qui contient $\zeta$. On a alors la suite d'extension $\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset L$. On a alors par multiplicativité des degrés

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^q$$

et donc par lemme 2 on a le résultat voulu ! □

**Remarques importantes :**

- Attention, développement compliqué, potentiellement bancal à présenter !
- Je pense que c'est bien d'avoir une idée (même très très vague) de la démonstration des résultats admis.
- C'est aussi bien d'avoir un peu en tête les méthodes concrètes pour construire des nombres constructibles (le symétrique par rapport à un point etc.)