# Théorème de Gauß

**Théorème (Wantzel)**
*Tout nombre constructible (à la règle non graduée et au compas) est un nombre algèbrique sur $\mathbb{Q}$, de degré une puissance de $2$.*

**Lemme —** *Soient $n, m \in \mathbb{N}^*$. Si $n$ et $m$ sont premiers entre eux, l'angle $\widehat{\frac{2\pi}{nm}}$ est constructible si et seulement si $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ le sont.*

**Démonstration**

$\Rightarrow$ Si $\widehat{\frac{2\pi}{nm}}$ est constructible, il est immédiat que

$$\widehat{\frac{2\pi}{n}} = m\widehat{\frac{2\pi}{nm}} \quad \text{et} \quad \widehat{\frac{2\pi}{m}} = n\widehat{\frac{2\pi}{nm}} \quad \text{le sont.}$$

$\Leftarrow$ Comme $n$ et $m$ sont premiers entre eux, par identité de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$un + vm = 1.$$

D'où

$$\widehat{\frac{2\pi}{nm}} = u\widehat{\frac{2\pi}{n}} + v\widehat{\frac{2\pi}{m}}$$

est constructible. $\square$

**Théorème (Gauß)**
*Les polygones réguliers constructibles sont exactement les polygones ayant un nombre de côtés de la forme*

$$2^\alpha p_1 \dots p_r \geqslant 3$$

*où $\alpha \in \mathbb{N}$ et les $p_i$ sont des premiers de Fermat.*

**DÉMONSTRATION**
Soit $n \geqslant 3$. On écrit sa décomposition en facteurs premiers :

$$n = 2^\alpha \prod_{k=1}^{r} p_k^{\beta_k}.$$

Le polygone régulier à $n$ côtés est constructible si et seulement si l'angle $\widehat{\frac{2\pi}{n}}$ est constructible.

Si $n = 2^\alpha$ alors le polygone est bien sûr constructible.

Sinon, comme la bissectrice est toujours constructible, par récurrence immédiate, le polygone régulier à $n$ côtés est constructible si et seulement si celui à $\displaystyle\prod_{k=1}^{r} p_k^{\beta_k}$ est constructible.

D'après le lemme, le polygone régulier à $n$ côté est constructible si et seulement si, pour tout $k \in [\![1; r]\!]$, l'angle $\widehat{\dfrac{2\pi}{p_k^{\beta_k}}}$ est constructible.

$\Leftarrow$ On admettra que si $\beta_k = 1$ et si $p_k$ est un premier de Fermat alors le polygone ayant $p_k^{\beta_k}$ est constructible.

$\Rightarrow$ On suppose que l'angle $\widehat{\frac{2\pi}{p^\beta}}$ est constructible, c'est-à-dire que $\cos\left(\frac{2\pi}{p^\beta}\right)$ est constructible.

D'après le théorème de Wantzel, $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\beta}\right)\right) \; : \; \mathbb{Q}\right] = 2^m$ avec $m \in \mathbb{N}$.
On note $q = p^\beta$ et $\omega = \cos\left(\frac{2\pi}{q}\right) + i\;\sin\left(\frac{2\pi}{q}\right)$.

Comme $\cos\left(\frac{2\pi}{q}\right) = \frac{1}{2}(\omega + \omega^{-1}) \in \mathbb{Q}(\omega)$, d'après le théorème de la base télescopique,

$$[\mathbb{Q}(\omega) \; : \; \mathbb{Q}] = \left[\mathbb{Q}(\omega) \; : \; \mathbb{Q}\left(\cos\left(\frac{2\pi}{q}\right)\right)\right] \cdot \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\beta}\right)\right) \; : \; \mathbb{Q}\right].$$

Comme $\omega$ est une racine primitive $q$-ème de l'unité, le $q$-ème polynôme cyclotomique $\Phi_q$ est le polynôme minimal de $\omega$, soit

$$[\mathbb{Q}(\omega) \; : \; \mathbb{Q}] = \deg \Phi_q = \varphi(q) = (p-1)p^{\beta-1}.$$

où $\varphi$ est l'indicatrice d'Euler car il y a $\varphi(q)$ racines primitives $q$-èmes de l'unité.

De plus comme $\omega \notin \mathbb{R}$ et $\omega^2 - 2\cos\left(\frac{2\pi}{q}\right)\omega + 1 = 0$,

$$\left[\mathbb{Q}(\omega) \ : \ \mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\beta}\right)\right)\right] = 2.$$

Donc

$$(p-1)p^{\beta-1} = 2^{m+1}.$$

Comme $p$ est un premier impair, on en déduit que

$$\beta = 1 \text{ et } p = 2^{m+1} + 1.$$

Comme $p$ est premier, c'est un résultat classique que $m+1$ est une puissance ce $2$, c'est-à-dire que $p$ est un premier de Fermat. $\square$