Polygones réguliers constructibles

Théorème 1 (Gauss-Wantzel)**.** Soit p un nombre premier impair. Soit $\alpha \in \mathbb{N}^*$. L'angle $\frac{2\pi}{p^\alpha}$ est constructible si et seulement si $\alpha = 1$ et $p = 1 + 2^{2^\beta}$.

Démonstration. $\boxed{\Rightarrow}$ Notons $\omega = \exp\left(\frac{2i\pi}{q}\right)$ avec $q = p^\alpha$. Par le théorème de Wantzel, puisque $\cos\left(\frac{2\pi}{q}\right)$ est constructible, il existe un entier m tel que :

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

De plus, ϕ_q étant le polynôme minimal de ω, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \phi_q = p^{\alpha-1}(p-1)$. D'autre part, on a aussi :

$$\omega^2 - 2\omega\cos\frac{2\pi}{q} + 1 = 0 \ \text{ donc } \ \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\pi}{q}\right)\right] = 2.$$

Par multiplicativité, il vient $p^{\alpha-1}(p-1) = 2^{m+1}$. Puisque p est premier impair, $\alpha = 1$. Écrivons $m+1 = \lambda 2^\beta$ avec λ impair, de sorte que $p = 1 + 2^{\lambda 2^\beta}$.

$$X^\lambda + 1 = (X+1)\sum_{k=0}^{\lambda-1}(-1)^k X^{\lambda-1-k} \ \text{ donc } \ X+1 | X^\lambda + 1.$$

En particulier, $1 + 2^{2^\beta} | p$, ce qui entraîne $p = 1 + 2^{2^\beta}$.

$\boxed{\Leftarrow}$ Notons $n = 2^\beta$, $p = 1 + 2^n$ et $\omega = \exp\left(\frac{2i\pi}{q}\right)$. Toujours : $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. Soit $G = \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\omega)$.
Un élément $g \in G$ est entièrement déterminé par $g(\omega)$. L'un des deux arguments suivants donne $g(\omega) \in \{\omega, \dots, \omega^{p-1}\}$:

— soit $1 = g(\omega^p) = g(\omega)^p$ et $g(\omega) \neq 1$ car g est injectif, donc $g(\omega) \in \{\omega, \dots, \omega^{p-1}\}$.

— soit $0 = g(\phi_p(\omega)) = \phi_p(g(\omega))$ donc $g(\omega) \in \{\omega, \dots, \omega^{p-1}\}$.

Ainsi, le groupe G se réécrit :

$$G = \left\{g_k : \omega \mapsto \omega^k,\, k \in \{1, \dots, n\}\right\} \simeq (\mathbb{F}_p)^\times = \mathbb{Z}/(p-1)\mathbb{Z}.$$

Soit G générateur de G. Posons $K_i = \{x \in \mathbb{Q}(\omega),\ g^{2^i}(x) = x\}$, qui définit une famille croissante de sous-corps de $\mathbb{Q}(\omega)$. Par définition d'un générateur, $\left(g^k(\omega)\right)_{0 \leq k \leq p-2}$ forme une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$.

Lemme 2. La famille de sous-corps construite ci-dessus vérifie : $K_0 = \mathbb{Q}$ et pour tout $i \in \{0, \dots, n-1\}$, $K_i \neq K_{i+1}$.

Démonstration. Soit $z = \sum_{k=0}^{p-2} \lambda_k g^k(\omega) \in K_0$.

$$g(z) = \sum_{k=0}^{p-2} \lambda_k g^{k+1}(\omega) = \lambda_{p-2} w + \sum_{k=1}^{p-2} \lambda_{k-1} g^k(\omega).$$

Donc tous les scalaires λ_k sont égaux, ce qui donne $z = -\lambda_0 \in \mathbb{Q}$. Ainsi $K_0 = \mathbb{Q}$.

Montrons que $z = \sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega) \in K_i \backslash K_{i-1}$. En exploitant encore l'unicité de la décomposition dans la $\mathbb{Q}$-base :

$$g^{2^{i-1}}(z) = \sum_{k=0}^{2^{n-i}-1} g^{k2^i + 2^{i-1}}(\omega) \neq z \ \text{ et } \ g^{2^i}(z) = \sum_{k=0}^{2^{n-i}-1} g^{(k+1)2^i}(\omega) = \omega + \sum_{k=1}^{2^{n-i}-1} g^{k2^i}(\omega) = z.$$

□

Or par multiplicativité :

$$2^n = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=0}^{n-1}[K_{i+1} : K_i] \geq 2^n \ \text{ donc } \ [K_{i+1} : K_i] = 2.$$

Par théorème de Wantzel, tout $x \in \mathbb{Q}(\omega)$ est constructible, donc $\cos\frac{2\pi}{q}$ aussi. □