Polygones réguliers constructibles

2012-2013

Référence : Jean-Claude Carrega, *Théorie des corps : la règle et le compas*, Hermann, 1989, p.48-52 et 214-219.

Lemme.
Soit m et n deux entiers premiers entre eux. Alors :

$$\text{l'angle } \widehat{\frac{2\pi}{mn}} \text{ est constructible} \iff \text{les angles } \widehat{\frac{2\pi}{m}} \text{ et } \widehat{\frac{2\pi}{n}} \text{ sont constructibles.}$$

Démonstration.
$\Rightarrow$: Chaque angle est un multiple de $\widehat{\frac{2\pi}{mn}}$.
$\Leftarrow$: $n \wedge m = 1$ donc par Bezout, il existe $a, b \in \mathbb{Z}$ tels que $an + bm = 1$. D'où :

$$\widehat{\frac{2\pi}{mn}} = a\widehat{\frac{2\pi}{m}} + b\widehat{\frac{2\pi}{n}}$$

donc $\widehat{\frac{2\pi}{mn}}$ est constructible. □

Corollaire.
Soit $n \geq 3$ et

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

sa décomposition en produit de facteurs premiers.

Alors :

$$\textit{le polygone régulier à } n \textit{ côtés est constructible} \iff \textit{les angles } \widehat{\frac{2\pi}{p_i^{\alpha_i}}} \textit{ le sont.}$$

Théorème (Gauss-Wantzel)**.**
Soit $\alpha \in \mathbb{N}^*$.
Alors :

(i) Les angles $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles.

(ii) Soit p un nombre premier impair, alors :

$$\textit{l'angle } \widehat{\frac{2\pi}{p^\alpha}} \textit{ est constructible} \iff \alpha = 1 \textit{ et } p = 1 + 2^{2^\beta} \textit{ où } \beta \in \mathbb{N}.$$

Démonstration.

(i) Cela revient à construire des bissectrices.

(ii) $\Rightarrow$: On pose $q := p^\alpha$ et $\omega := e^{2i\pi/q}$. On a donc supposé ω constructible.
Par le théorème de Wantzel, on a alors :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m \text{ où } m \in \mathbb{N}.$$

Or ω est une racine primitive q-ième de l'unité, donc son polynôme minimal sur $\mathbb{Q}$ est le polynôme cyclotomique Φ_q, de degré $\varphi(q) = p^{\alpha-1}(p-1)$.
D'où :

$$2^m = [\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1)$$

Or p est premier impair donc $\alpha = 1$ et on obtient $p = 2^m + 1$.
On écrit maintenant $m = \lambda 2^\beta$ avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair.
Puisque -1 est racine de $1 + X^\lambda$, on a $1 + X \mid 1 + X^\lambda$, donc :

$$1 + 2^{2^\beta} \mid 1 + (2^{2^\beta})^\lambda = p$$

et p étant premier, on a :

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

$\Leftarrow$: On pose $n := 2^\beta$, $p = 1 + 2^n$ et $\omega := e^{2i\pi/p}$.

Alors puisque le polynôme minimal de ω est Φ_p, on a :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$$

Soit G le groupe d'automorphismes sur $\mathbb{Q}$ de $\mathbb{Q}(\omega)$ (*i.e.* le groupe des automorphismes de corps de $\mathbb{Q}(\omega)$ fixant $\mathbb{Q}$). Alors tout $g \in G$ est entièrement déterminé par $g(\omega)$. De plus,

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

Ainsi $g(\omega)$ est une racine de Φ_p donc est une puissance de ω.
Réciproquement, le morphisme qui est l'identité sur $\mathbb{Q}$ et qui envoie ω sur ω^k appartient à G.
Donc

$$G = \{\omega \mapsto \omega^k \mid k \in \{1, \ldots, p-1\}\}$$

et donc G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. G est ainsi engendré par un certain g d'ordre $p - 1 = 2^n$.
On pose, pour $0 \leq i \leq n$,

$$\mathbb{K}_i := \left\{z \in \mathbb{Q}(\omega) \mid g^{2^i}(z) = z\right\}$$

Alors on a les inclusions :

$$\mathbb{Q} \subset \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega)$$

Montrons que $\mathbb{Q} = \mathbb{K}_0$ et que toutes les extensions sont quadratiques.
La famille $(\omega, g(\omega), \ldots, g^{p-2}(\omega))$ est une base de $\mathbb{Q}(\omega)$ donc pour $z \in \mathbb{K}_0$, il existe $\lambda_0, \ldots, \lambda_{p-2}$ tels que :

$$z = \lambda_0\omega + \cdots + \lambda_{p-2}g^{p-2}(\omega)$$

Donc en appliquant g, on a :

$$z = g(z) = \lambda_0 g(\omega) + \cdots + \lambda_{p-2} g^{p-1}(\omega)$$

avec $g^{p-1} = \mathrm{id}$, donc par identification, on a $\lambda_0 = \cdots = \lambda_{p-2}$.
On a alors :

$$\begin{aligned} z &= \lambda_0(\omega + g(\omega) + \cdots + g^{p-2}(\omega)) \\ &= \lambda_0(\omega + \omega^2 + \cdots + \omega^{p-1}) \\ &= -\lambda_0 \end{aligned}$$

Par conséquent, $z \in \mathbb{Q}$ donc $\mathbb{K}_0 = \mathbb{Q}$.
De plus,

$$\sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega) \in \mathbb{K}_i \setminus \mathbb{K}_{i-1}$$

donc les extensions $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega)$ sont strictes et $[\mathbb{K}_n : \mathbb{Q}] = 2^n$. Toutes les extensions sont donc de degré 2 car il y en a n.
Finalement, par le théorème de Wantzel, ω est constructible à la règle et au compas.

$\square$

En combinant le théorème et le corollaire du lemme, on obtient que le polygone régulier à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et d'un nombre fini de nombres de Fermat premiers distincts.