Polygones réguliers constructibles

Arnaud Girand

5 juillet 2012

Référence :
- [Car89], p. 48–52 et 214–219

Prérequis :
- théorème de Wantzel.

Lemme 1
Soit m et n deux entiers premiers entre eux.
Alors :

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

Démonstration :

($\Rightarrow$) Immédiat car ces angles sont des multiples de $\widehat{\frac{2\pi}{mn}}$; il suffit alors de reporter avec un compas le bon nombre de fois la corde formée par ce dernier angle sur le cercle unité.

($\Leftarrow$) Par théorème de Bézout, il existe $a, b \in \mathbb{N}$ tels que $an + bm = 1$; de fait :

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

$\widehat{\frac{2\pi}{mn}}$ est alors une combinaison entière d'angles constructibles, donc l'est.

Lemme 2
Soit $n \geq 3$ de décomposition en produit de facteurs premiers :

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

Alors :

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

Démonstration : Découle par récurrence du lemme 1.

Proposition 1 (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 :

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

Ainsi on obtient (en combinant ce résultat avec le lemme 2) que :

le polygone régulier à n côtés est constructible
$\Leftrightarrow$
n est le produit d'une puissance de 2 (éventuellement égale à 1) et d'un nombre fini (éventuellement nul) de nombres de Fermat premiers distincts

Démonstration :

(i) On se ramène à la construction de bissectrices via une récurrence sur α.

(ii) ($\Rightarrow$) Si on suppose $\widehat{\frac{2\pi}{p^\alpha}}$ constructible alors $\cos\left(\frac{2\pi}{p^\alpha}\right)$ l'est également et donc par théorème de Wantzel :

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right):\mathbb{Q}\right] = 2^m \text{ avec } m \in \mathbb{N} \tag{1}$$

Posons $q := p^\alpha$ et $\omega := e^{2i\pi/q}$. Alors ω est algébrique sur $\mathbb{Q}$ et son polynôme minimal est le polynôme cyclotomique ϕ_q (il est annulateur irréductible unitaire), qui est de degré $\phi(q) = p^{\alpha-1}(p-1)$, donc :

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

Comme $\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{p^\alpha}\right)$ on a $\cos\left(\frac{2\pi}{p^\alpha}\right) \in \mathbb{Q}(\omega)$ et $\omega^2 - 2\omega\cos\left(\frac{2\pi}{p^\alpha}\right) + 1 = 0$ ergo :

$$\left[\mathbb{Q}(\omega):\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)\right] = 2 \tag{3}$$

Or :

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

Et donc par (2) , (3) et (1) on a :

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

Donc, comme p est un nombre premier impair on a nécessairement $\alpha = 1$ et $p = 2^{m+1}+1$. Par décomposition en produits de facteurs premiers, $m+1 = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair. De fait $p = 1 + (2^{2^\beta})^\lambda$.

Comme λ est impair, $1 + X | 1 + X^\lambda$ et donc $1 + 2^{2^\beta} | p$ donc, par primalité, $p = 1 + 2^{2^\beta}$ est un nombre de Fermat.

($\Leftarrow$) Posons $n = 2^\beta$, de telle sorte que $p = 1 + 2^n$, et $\omega := e^{2i\pi/p}$. De fait on a, comme le polynôme minimal de ω est ϕ_p, que :

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

Soit $g \in G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)$; alors comme $g(\mathbb{Q}) = \mathbb{Q}$ g est entièrement déterminé par $g(\omega)$. De plus on a :

$$0 = g(0) = g(\phi_p(\omega)) = \phi_p(g(\omega)) = \sum_{i=0}^{p-1} g(\omega)^i$$

Ainsi $g(\omega) \in \mathrm{Rac}_{\mathbb{C}}(\phi_p) = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$ et donc on a :

$$G = \{g_k : \omega \mapsto \omega^k \mid k \in [p-1]\}$$

En particulier, $|G| = p-1$ et donc l'application surjective suivante est un isomorphisme :

$$\begin{aligned} \psi : G &\to (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \\ g_k &\mapsto \bar{k} \end{aligned}$$

Ainsi G contient un élément g_0 d'ordre $p-1 = 2^n$ et donc si pose, pour $0 \leq i \leq n$ $\mathbb{K}_i := \{z \in \mathbb{Q}(\omega) \mid g_0^{2^i}(z) = z\}$. Il est clair que les $\mathbb{K}_i$ sont des sous–corps de $\mathbb{Q}(\omega)$ ($\mathbb{K}_i = \ker(g^{2^i} - \mathrm{id})$). De plus, $\mathbb{Q} \subset \mathbb{K}_0$ et si $z \in \mathbb{K}_0$ alors comme $(g_0(\omega)^i)_{0\leq i\leq p-2}$ forme une base de $\mathbb{Q}(\omega)/\mathbb{Q}$ (image d'une base par un isomorphisme) on a l'existence de $\lambda_0, \ldots, \lambda_{p-2} \in \mathbb{Q}$ tels que $z = \lambda_0\omega + \ldots + \lambda_{p-2}g_0^{p-2}(\omega)$ et donc :

$$\sum_{i=0}^{p-2} \lambda_i g_0^i(\omega) = z = g_0(z) = \sum_{i=0}^{p-2} \lambda_i g_0^{i+1}(\omega)$$

Par identification tous les λ_i sont égaux et donc $z = \lambda_0 g_0(\omega + \ldots + \omega^{p-1}) = -\lambda_0 \in \mathbb{Q}$. On a donc une tour d'extensions :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega) \tag{4}$$

Les inclusions sont de plus strictes car pour tout i, l'élément suivant appartient à $\mathbb{K}_{i+1} \setminus \mathbb{K}_i$:

$$\sum_{k=0}^{2^{n-i-1}-1} g_0^{2^{i+1}k}(\omega)$$

Posons $f := g_0^{2^{n-1}}$ et $\omega^\lambda := f(\omega)$. $f^2 = \mathrm{id}$ donc :

$$\omega = f^2(\omega) = \omega^{\lambda^2}$$

De fait $\omega^{\lambda^2-1} = 1$ et donc $p|\lambda^2 - 1$, i.e $\overline{\lambda^2 - 1} = \bar{0}$ dans $\mathbb{F}_p$ et donc $\overline{\lambda} = \pm\bar{1}$. Comme $f \neq \mathrm{id}$ on a alors nécessairement $\overline{\lambda} = -\bar{1}$, i.e $f(\omega) = \omega^{-1}$.

Remarquons ensuite que $f\left(\cos\left(\frac{2\pi}{p}\right)\right) = \frac{1}{2}(f(\omega) + f(\omega^1)) = \cos\left(\frac{2\pi}{p}\right)$ et donc $\cos\left(\frac{2\pi}{p}\right) \in \mathbb{K}_{n-1}$. On a donc :

$$\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset \mathbb{K}_{n-1} \subsetneq \mathbb{K}_n = \mathbb{Q}(\omega)$$

D'où :

$$1 < [\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] \leq \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] \tag{5}$$

De plus, on montre de la même façon qu'en (i) (en substituant p à q) que :

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2 \tag{6}$$

Et donc au final :

$$[\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] = 2 \text{ ergo } \mathbb{K}_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$$

À présent, si on passe au degré dans la tour (4) on trouve :

$$2^n = p - 1 = [\mathbb{Q}_(\omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] \times \ldots \times [\mathbb{K}_1 : \mathbb{Q}]}_{n \text{ facteurs}}$$

On a donc nécessairement tous les $[\mathbb{K}_{i+1} : \mathbb{K}_i]$ égaux à 2. En particulier :

$$[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) : \mathbb{Q}] = 2^{n-1}$$

D'où la constructibilité voulue (par la caractérisation usuelle, que l'on peut par exemple trouver dans [Car89] p. 25).

Références

[Car89] Jean-Claude Carrega. *Théorie des corps : la règle et le compas*. Hermann, 1989.