

Développement : Théorème de Gauss-Wantzel

Leçons : 102, 121, 125, 182, 183

Théorème. Soit p premier, soit $\alpha \in \mathbb{N}^*$. L'angle $\frac{2\pi}{p^\alpha}$ est constructible ssi $p = 2$ ou ($\alpha = 1$ et p est un nombre de Fermat, soit $p = 1 + 2^{(2^\beta)}$).

Démonstration.

Étape 1 : Cas $p = 2$.

C'est immédiat par récurrence sur α : on sait construire l'angle $\frac{\pi}{2}$ et on sait construire des bissectrices. On suppose désormais $p \geq 3$.

Étape 2 : $\alpha = 1$ et $p = 1 + 2^k$.

Si $\frac{2\pi}{p^\alpha}$ constructible, en posant $q = p^\alpha$, on a $\cos(2\pi/q)$ constructible. Donc d'après le théorème de Wantzel, il existe $m \in \mathbb{N}$, $[\mathbb{Q}(\cos(2\pi/q)) : \mathbb{Q}] = 2^m$. On pose $\omega = e^{2i\pi/q}$. C'est une racine q -ème de $X^q - 1$ donc algébrique. Son polynôme minimal est Φ_q le q -ème polynôme cyclotomique, qui est de degré $\varphi(q) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Ainsi $[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1)$. Comme $\omega + \omega^{-1} = 2\cos(2\pi/q)$, on a $\cos(2\pi/q) \in \mathbb{Q}(\omega)$, et $\omega^2 - 2\omega\cos(2\pi/q) + 1 = 0$, donc ω est algébrique de degré 2 sur $\mathbb{Q}(\cos(2\pi/q))$: $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/q))] = 2$. Finalement, par multiplicativité du degré, $p^{\alpha-1}(p-1) = [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/q))][\mathbb{Q}(\cos(2\pi/q)) : \mathbb{Q}] = 2^{m+1}$. Par unicité de la décomposition en facteurs premiers et comme $p \geq 3$, nécessairement $\alpha = 1$ et $p = 1 + 2^{m+1}$.

Étape 3 : $m + 1 = 2^\beta$.

D'après le théorème de décomposition en facteurs premiers, $m + 1 = 2^\beta s$ avec s impair.

Ainsi $p = 1 + 2^{m+1} = 1 + 2^{(2^\beta s)} = 1 + (2^{(2^\beta)})^s$. Comme s impair, $1 + X$ divise $1 + X^s$ dans $\mathbb{Z}[X]$: donc $1 + 2^{(2^\beta)}$ divise p , mais comme p premier, $p = 1 + 2^{(2^\beta)}$.

Étape 4 : Les angles de cette forme sont constructibles.

Soit $p = 1 + 2^{(2^\beta)}$, on pose $q = 2^\beta$. Soit $\omega = e^{2i\pi/p}$. Montrons que p constructible. Soit G le groupe des automorphismes de corps de $\mathbb{Q}(\omega)$ induisant l'identité sur \mathbb{Q} . Alors, si $\sigma \in G$, on a $\Phi_p(\sigma(\omega)) = \sigma(\Phi_p(\omega)) = 0$ donc σ induit une permutation sur les racines de Φ_p , qui sont les $\omega^k, k \in \llbracket 1, p-1 \rrbracket$. Alors, si on note $\psi(\sigma) \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\sigma(\omega) = \omega^{\psi(\sigma)}$, on a $\psi : G \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ isomorphisme de groupes. Donc G cyclique d'ordre $p-1 = 2^q$. Soit σ générateur de G . On pose, pour tout $k \leq q$, $L_k = \{z \in \mathbb{Q}(\omega), \sigma^{2^k}(z) = z\}$. On vérifie que c'est un sous-corps de $\mathbb{Q}(\omega)$. On a ainsi $\mathbb{Q} \subset L_0 \subset \dots \subset L_q = \mathbb{Q}(\omega)$. De plus les inclusions sont strictes : en effet, $z :=$

$$\omega + \sigma^{2^k}(\omega) + \sigma^{2^{k+1}}(\omega) + \dots + \sigma^{2^q - 2^k}(\omega) = \sum_{j=0}^{2^q - k - 1} \sigma^{2^k j}(\omega) \in L_k \text{ (cela se vérifie immédiatement en composant par } \sigma^{2^k}\text{),}$$

mais $z \notin L_{k-1}$ (car sinon z posséderait deux écritures distinctes dans la base $(\omega, \dots, \omega^{p-1}) = \{\sigma^j(\omega), j \in \llbracket 1, p-1 \rrbracket\}$ de $\mathbb{Q}(\omega)$: en effet, dans l'une la composante en ω vaut 1, et pas dans 0 car la seule façon d'avoir ω est $\sigma^{p-1}(\omega)$ ce qui est impossible pour $k-1$). Donc, pour tout $k \leq q-1$, $[L_{k+1} : L_k] \geq 2$, mais par multiplicité du degré, $2^q = [\mathbb{Q}(\omega) : \mathbb{Q}] = [L_q : L_{q-1}] \times \dots \times [L_1 : L_0] \times [L_0 : \mathbb{Q}]$, donc $[L_0 : \mathbb{Q}] = 1$ et pour tout $k \leq q-1$, $[L_{k+1} : L_k] = 2$. On a donc une tour d'extensions quadratiques, et d'après le théorème de Wantzel, $\frac{2\pi}{p}$ est constructible. \square

Corollaire. Si un polygone régulier est constructible, son nombre de côtés est de la forme $2^\alpha p_1 \dots p_r$ où les p_i sont des nombres premiers de la forme ci-dessus.

Démonstration. Pour $m, n \in \mathbb{N}^*$ premiers entre eux, $\frac{2\pi}{mn}$ constructible ssi $\frac{2\pi}{m}, \frac{2\pi}{n}$ constructibles.

Supposons $\frac{2\pi}{mn}$ constructible. Alors $\frac{2\pi}{m} = n \frac{2\pi}{mn}$ est constructible en reportant n fois l'angle $\frac{2\pi}{mn}$.

De même, $\frac{2\pi}{n}$ est constructible.

Réciproquement, si $\frac{2\pi}{m}, \frac{2\pi}{n}$ constructibles, comme $m \wedge n = 1$, par Bézout il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Alors $\frac{2\pi}{mn} = u \frac{2\pi}{n} + v \frac{2\pi}{m}$, donc est constructible (la somme de deux angles constructibles est constructible en les construisant avec un côté adjacent). Le corollaire s'en déduit immédiatement. \square

Références

J.-C. Carrega, THÉORIE DES CORPS - LA RÈGLE ET LE COMPAS, Hermann, p. 48 et p. 214.

D.-J. Mercier, COURS DE GÉOMÉTRIE, EPU, p. 409.

Notes personnelles

L'étape 4 est à bien travailler et à bien comprendre. Selon la leçon, zapper l'étape 3 ou le corollaire.