Polygones réguliers constructibles [1]

Leçons : 102, 121, 125, 182, 183

[MerCdG], théorème 318

Théorème (*Gauss-Wantzel*)

Soit p un nombre premier impair, $\alpha \in \mathbb{N}^*$.
Alors l'angle $\widehat{\dfrac{2\pi}{p^\alpha}}$ est constructible $\Leftrightarrow$ $\alpha = 1$ et p est un nombre premier de Fermat (c'est-à-dire que p est un nombre premier qui s'écrit sous la forme $1 + 2^{2^\beta}$, où $\beta \in \mathbb{N}$).

Démonstration :

$\Rightarrow$ On pose $q = p^\alpha$ et $\omega = \exp\left(\dfrac{2i\pi}{q}\right)$.

On suppose que l'angle $\widehat{\dfrac{2\pi}{q}}$ est constructible, id est, que $\cos\left(\dfrac{2\pi}{q}\right)$ est un nombre constructible.
Alors, par le théorème de Wantzel [2], on obtient : $\left[\mathbb{Q}\left(\cos\dfrac{2\pi}{q}\right) : \mathbb{Q}\right] = 2^m$, où $m \in \mathbb{N}$.
Aussi, le polynôme cyclotomique Φ_q étant le polynôme minimal de ω, on a :

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

Comme $\omega^2 - 2\omega\cos\dfrac{2\pi}{q} + 1 = 0$, on a $\cos\dfrac{2\pi}{q} \in \mathbb{Q}(\omega)$ et même $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\dfrac{2\pi}{q}\right)\right] = 2$.
Par multiplicativité du degré, on obtient $2^{m+1} = p^{\alpha-1}(p-1)$.
Comme p est impair, il vient $\alpha = 1$, puis $p = 1 + 2^{m+1}$; montrons que $m+1$ est une puissance de 2.
On écrit alors $m + 1 = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair ; on a alors $p = 1 + \left(2^{2^\beta}\right)^\lambda$.
Or, λ étant impair, on a dans $\mathbb{Z}[X]$: $1 + X \big| 1 + X^\lambda$ et donc $1 + 2^{2^\beta} \big| p$ et donc, comme p est premier, on en déduit $\lambda = 1$.
Donc p est un nombre premier de Fermat.

$\Leftarrow$ On note $n = 2^\beta$, de sorte que $p = 1 + 2^n$, et $\xi = \exp\left(\dfrac{2i\pi}{p}\right)$.

On a : $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg \Phi_p = \varphi(p) = p - 1$.

1. On peut ajouter quelques résultats autour de ce développement pour détailler son utilité.

Lemme

- Les angles de la forme $\widehat{\dfrac{2\pi}{2^\alpha}}$ sont constructibles, où $\alpha \in \mathbb{N}^*$.
- Soient $m, n \in \mathbb{N}^*$, avec $m \wedge n = 1$,
  Alors l'angle $\widehat{\dfrac{2\pi}{mn}}$ est constructible $\Leftrightarrow$ $\widehat{\dfrac{2\pi}{m}}$ et $\widehat{\dfrac{2\pi}{n}}$ le sont.

En conséquence, les polygones réguliers constructibles sont ceux qui possèdent $2^{\alpha_2} \prod\limits_{p \in \mathcal{F}} p^{\alpha_p}$ côtés, où $\mathcal{F}$ est l'ensemble des nombres premiers de Fermat, et où les α_i sont des entiers naturels.

En effet :
- C'est immédiat, puisque par récurrence, il suffit de savoir tracer des bissectrices à la règle et au compas.
- $\Leftarrow$ Il est facile de construire le multiple d'un nombre constructible (en reportant avec le compas le bon nombre de fois la corde formée par l'angle sur le cercle unité).

  $\Rightarrow$ Par Bézout, $\exists \lambda, \mu \in \mathbb{Z}, \lambda m + \mu n = 1$; dès lors $\widehat{\dfrac{2\pi}{mn}} = \lambda \widehat{\dfrac{2\pi}{m}} + \mu \widehat{\dfrac{2\pi}{n}}$.
  Et on construit sans peine la somme de deux angles constructibles en traçant des représentants de ces angles avec un côté adjacent.

2. Le théorème de Pierre-Laurent Wantzel, énoncé en 1837, donne une condition nécessaire et suffisante pour qu'un nombre soit constructible à la règle et au compas : il faut et il suffit que ce nombre appartienne à une extension de $\mathbb{Q}$ qui soit le terme d'une suite d'extensions quadratiques.

On note $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$; et si $g \in G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par $g(\xi)$.
g étant un morphisme d'anneaux, on a : $0 = g(0) = g\left(\Phi_p(\xi)\right) = \Phi_p(g(\xi))$.
Donc $g(\xi)$ est nécessairement une racine de Φ_p, donc $g(\xi) \in \left\{\xi, \xi^2, \ldots, \xi^{p-1}\right\}$.
Il faudrait alors montrer qu'on définit bien ainsi des automorphismes du corps $\mathbb{Q}(\xi)$; et alors

$$G = \left\{g_k : \xi \mapsto \xi^k \middle| k \in [\![1, p-1]\!]\right\} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \underset{3}{\simeq} \mathbb{Z}/(p-1)\mathbb{Z}.$$

Désormais, g désignera un générateur de G.
Pour $i \in [\![0, n]\!]$, on note $K_i = \mathrm{Ker}\left(g^{2^i} - \mathrm{Id}\right)$; c'est un sous-corps de $\mathbb{Q}(\xi)$.
De plus, $\forall i \in [\![0, n-1]\!], g^{2^{i+1}} = \left(g^{2^i}\right)^2$ implique $K_i \subseteq K_{i+1}$.
Comme g génère G, $\left(g^i(\xi)\right)_{0 \leqslant i \leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\xi)$.
Soit $z \in K_0$, $\exists \lambda_0, \ldots, \lambda_{p-2} \in \mathbb{Q}$, $z = \sum_{i=0}^{p-2} \lambda_i g^i(\xi)$; mais $z = g(z) = \lambda_{p-2}\xi + \sum_{i=1}^{p-2} \lambda_{i-1} g^i(\xi)$.
Tous les scalaires λ_i sont donc égaux et $z = \lambda_0 \sum_{i=0}^{p-2} g^i(\xi) = \lambda_0 \sum_{j=1}^{p-1} \xi^j = -\lambda_0 \in \mathbb{Q}$. Donc $K_0 = \mathbb{Q}$.

Pour montrer que $\forall i \in [\![0, n-1]\!], K_i \neq K_{i+1}$, il faudrait considérer l'élément $z = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\xi)$.[4]
On en déduit alors qu'on a la suite d'extensions :

$$\mathbb{Q} = K_0 \underset{\neq}{\subset} K_1 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} K_n = \mathbb{Q}(\xi).$$

Mais $2^n = [\mathbb{Q}(\xi) : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{\geqslant 2}$.
Ainsi, $\forall i \in [\![0, n-1]\!], [K_{i+1} : K_i] = 2$.
Par le théorème de Wantzel, tous les éléments de $\mathbb{Q}(\xi)$ sont donc constructibles ; mais $\cos \frac{2\pi}{p} = \frac{\xi + \xi^{-1}}{2}$ en fait partie. ■

Références

[MerCdG][5] D.-J. MERCIER – *Cours de géométrie, préparation au CAPES et à l'agrégation*, Publibook, 2008.

3. Pour la cyclicité de $\mathbb{F}_p^\times$, on renvoie à la page **??**.

4. Okay, je le fais, mais c'est vraiment parce que c'est vous. On a : $g^{2^i}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h + 2^i}(\xi) \neq z$ car les vecteurs de base intervenant dans la décomposition ne sont pas les mêmes (on a décalé les coordonnées de 2^i, alors qu'entre deux coordonnées non-nulles, il y a $2^{i+1} - 1$ zéros). Et aussi : $g^{2^{i+1}}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}(h+1)}(\xi) = \sum_{h=1}^{2^{n-i-1}-1} g^{2^{i+1}h}(\xi) + \underbrace{g^{2^{i+1}2^{n-i-1}}(\xi)}_{=\xi} = z$.

5. On trouvera également dans cette référence une façon de construire le pentagone régulier à la règle et au compas.