13 Polygones réguliers constructibles

Leçons 102, 125, 151, 191(, 104, 141, 144)

Ref : [Mercier]

Définition 1 Les nombres de Fermat sont les nombres premiers F_β s'écrivant $F_\beta = 1 + 2^{2^\beta}$, pour $\beta \in \mathbb{N}$.

Théorème 2 Soit $p \in \mathfrak{P}$ impair, et $\alpha \in \mathbb{N}^*$. Alors le polygône $\mathcal{P}_n$ régulier à n côtés, avec $n = p^\alpha$, est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat.

Démonstration. On rappelle que $\mathcal{P}_n$ est constructible si et seulement si $\cos\left(\frac{2\pi}{n}\right)$ l'est.

$\Longrightarrow$ On suppose $\mathcal{P}_n$ constructible et on pose $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Le théorème de Wantzel montre que $\mathbb{Q}(\omega)$ est le m-ième terme d'une suite d'extensions quadratiques de $\mathbb{Q}$. De plus, comme le polynôme minimal de ω est Φ_n, on a

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

Comme p est impair, on a donc $\alpha = 1$ et $p = 1 + 2^m$. Montrons que m est une puissance de 2. On écrit $m = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair. Ainsi, -1 est racine de $X^\lambda + 1$, donc $X + 1$ divise $X^\lambda + 1$ sur $\mathbb{Z}$. On en déduit que F_β divise $p = 1 + \left(2^{2^\beta}\right)^\lambda$. Mais comme p est premier, on a alors égalité : p est un nombre premier de Fermat.

$\Longleftarrow$ Soit $p = F_\beta$ un nombre premier de Fermat. On note $q = 2^\beta$, de sorte que $p = 1 + 2^q$. On pose aussi $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{p}}$.

Étape 1. Description des automorphismes de $\mathbb{Q}(\omega)$.
On a alors

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_p) = 2^q.$$

On note G le groupe des automorphismes de corps sur $\mathbb{Q}(\omega)$ laissant $\mathbb{Q}$ invariant [1]. Ainsi, si $g \in G$, il est entièrement déterminé par l'image de ω. Comme $\omega^p = 1$, $g(\omega)^p = 1$, donc $g(\omega)$ est une racine p-ième de l'unité, ce qui permet de décrire G [2] :

$$G = \left\{ g : \omega \longmapsto \omega^i,\ i \in [\![1, p-1]\!] \right\}.$$

On voit alors que l'application

$$\varphi : \left| \begin{array}{ccc} G & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ g_i & \longmapsto & i \end{array} \right.$$

est un isomorphisme de groupes [3], ce qui prouve que G est un groupe cyclique.

Étape 2. Une tour d'extensions de corps.
On notera dans la suite g un générateur de G. On définit pour $i \in [\![0, n]\!]$ le sous-corps

$$K_i := \ker\left(g^{2^i} - \mathrm{id}\right).$$

Comme $g^{2^{i+1}} = (g^{2^i})^2$, on a $K_i \subset K_{i+1}$. Montrons que $K_0 = \mathbb{Q}$. On remarque que les $(g^i(\omega))_{0 \leq i \leq p-2}$ forment une base de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$. Soit $z \in K_0$. On écrit $z = \sum_{i=0}^{p-2} z_i g^i(\omega)$. On a alors

$$z = g(z) = \sum_{i=0}^{p-2} z_i g^{i+1}(\omega).$$

Il vient que les z_i sont tous égaux, et on a donc

$$z = z_0 \sum_{i=0}^{p-1} g^i(\omega) = z_0 \sum_{i=1}^{p-1} \omega^i = -z_0 \in \mathbb{Q}.$$

Donc $K_0 \subset \mathbb{Q}$. Réciproquement, comme g est $\mathbb{Q}$-invariant, l'inclusion inverse est vraie aussi, et $K_0 = \mathbb{Q}$. De même, comme g est un générateur du groupe G, qui est d'ordre 2^q, on a $K_q = \mathbb{Q}(\omega)$.

1. Si on veut passer vite sur certains arguments, une des possibilités (si l'on maîtrise un peu la théorie de Galois) est de dire que ce groupe est le groupe de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$, et certaines choses démontrées plus bas en découlent directement.
2. On vérifie que l'on obtient ainsi $p - 1$ automorphismes distincts.
3. On a $\varphi(g_i \circ g_j) = \varphi(g_{ij}) = ij = \varphi(g_i)\varphi(g_j)$.

Étape 3. Extensions quadratiques et conclusion.
Montrons que K_i est une extension quadratique de K_{i-1}, pour $i \geq 1$. On considère cette fois $z = \sum_{k=0}^{2^{q-i}-1} g^{k2^i}(\omega)$. On a

$$g^{2^i}(z) = \sum_{k=0}^{2^{q-i}-1} g^{(k+1)2^i}(\omega) = \sum_{k=1}^{2^{q-i}-1} g^{k2^i}(\omega) + \underbrace{g^{2^q}(\omega)}_{=\omega=g^0(\omega)} = z.$$

Donc $z \in K_i$. De plus,

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

Comme on a décalé chaque coordonnée non nulle de z de 2^{i-1}, alors que celles-ci sont espacées de 2^i, les coordonnées non nulles de z et $g(z)$ ne sont pas les mêmes. Donc $z \notin K_{i-1}$. Donc la suite

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq .. \subsetneq K_q = \mathbb{Q}(\omega)$$

est une suite d'extensions strictes. En passant au degré, on a alors

$$2^q = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=0}^{q-1} \underbrace{[K_{i+1} : K_i]}_{\geq 2} \geq 2^q,$$

ce qui implique que les extensions K_{i+1}/K_i sont quadratiques. Donc $\cos\left(\frac{2\pi}{p}\right) = \frac{\omega + \omega^{-1}}{2}$ est dans une extension qui est le terme d'une suite d'extensions quadratiques de $\mathbb{Q}$, donc est constructibles d'après le théorème de Wantzel, ce qui montre que $\mathcal{P}_p$ est constructible.

□

Théorème 3 (Gauß-Wantzel) Les seuls polygones réguliers constructibles sont les polygones à n côtés, avec $n = 2^m p_1..p_r$, où $m \in \mathbb{N}$ et les p_i sont des nombres premiers de Fermat distincts.

Démonstration. On démontre un lemme qui nous permettra d'effectuer une récurrence.

Lemme 4
- Pour $n \geq 3$, $\mathcal{P}_n$ est constructible si et seulement si $\mathcal{P}_{2n}$ l'est.
- Si pour $n, m \geq 3$ premiers entre eux, $\mathcal{P}_n$ et $\mathcal{P}_m$ sont constructibles si et seulement si $\mathcal{P}_{mn}$ l'est.

Démonstration.
- Si $\mathcal{P}_{2n}$ est construit, prendre un point sur deux permet de construire $\mathcal{P}_n$. Réciproquement, si $\mathcal{P}_n$ est construit, on trace les médiatrices de ses côtés, et leur intersection avec le cercle circonscrit forment les points manquants de $\mathcal{P}_{2n}$.
- Si $\mathcal{P}_{nm}$ est construit, prendre un point sur m (resp. un point sur n) permet de construire $\mathcal{P}_n$ (resp. $\mathcal{P}_m$). Pour la réciproque, on se donne une relation de Bézout $1 = un + vm$. On a alors

$$\frac{2\pi}{mn} = u\frac{2\pi}{m} + v\frac{2\pi}{n}.$$

Ainsi, si l'on reporte u fois l'angle $\frac{2\pi}{m}$ (que l'on a puisque $\mathcal{P}_m$ est construit) puis v l'angle $\frac{2\pi}{n}$, on obtient $\frac{2\pi}{mn}$.

□

□