Polygones réguliers constructibles

Références : Mercier, *Cours de Géométrie*, p 428-429 et 433-436

Théorème.

Soit p un nombre premier impair, $\alpha \in \mathbb{N}^*$.
Alors le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ 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. On pose $q = p^\alpha$. On rappelle que le polygone régulier à q côtés $\mathcal{P}_q$ est constructible ssi $\omega = \exp\left(\frac{2i\pi}{q}\right)$ est constructible ssi $\cos\left(\frac{2\pi}{q}\right)$ est constructible.

$\Rightarrow$ On suppose que $\mathcal{P}_q$ est constructible.
Alors, par le théorème de Wantzel [1], on obtient : $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$, où $m \in \mathbb{N}^*$.
Aussi, le polynôme cyclotomique Φ_q étant le polynôme minimal de ω, on a :

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

On obtient $2^m = p^{\alpha-1}(p-1)$.
Comme p est impair, il vient $\alpha = 1$, puis $p = 1 + 2^m$; montrons que m est une puissance de 2.
On écrit alors $m = \lambda 2^\beta$, 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 $1 + X \big| 1 + X^\lambda$ dans $\mathbb{Z}[X]$ (car (-1) est racine). D'où $1 + 2^{2^\beta} \Big| p$ et donc, comme p est premier, on en déduit $\lambda = 1$.
p est bien un nombre premier de Fermat.

$\Leftarrow$ • On note $n = 2^\beta$, de sorte que $p = 1 + 2^n$, et $\omega = \exp\left(\frac{2i\pi}{p}\right)$.
On a : $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_p = p - 1 = 2^n$.
On va vouloir trouver une suite d'extensions quadratiques menant à $\mathbb{Q}(\omega)$.
On note $G = \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$; et si $g \in G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par $g(\omega)$.
On a $\omega^p = 1$, donc $g(\omega)^p = 1$ et $g(\omega)$ est une racine de l'unité.
Les automorphismes de G sont donc de la forme $g_i(\omega) = \omega^i$ (avec $i \neq 0$) et on vérifie facilement que ce sont bien des automorphismes. On a donc

$$G = \left\{ g_i : \omega \mapsto \omega^i \middle| i \in [\![1, p-1]\!] \right\}.$$

On pose

$$\varphi : \begin{array}{ccc} G & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ g_i & \mapsto & i \end{array}.$$

Alors

$$\varphi(g_i \circ g_j) = \varphi(g_{ij}) = ij = \varphi(g_i)\varphi(g_j),$$

donc φ est un isomorphisme de groupes. G est donc un **groupe cyclique** (C'est le résultat le plus important de cette preuve.).

• Désormais, g désignera un générateur de G.
Pour $i \in [\![0, n]\!]$, on note $K_i = \mathrm{Ker}\left(g^{2^i} - id\right)$; c'est un sous-corps de $\mathbb{Q}(\omega)$.
De plus, $\forall i \in [\![0, n-1]\!], g^{2^{i+1}} = \left(g^{2^i}\right)^2$ implique $K_i \subseteq K_{i+1}$.

1. 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.
Pour le montrer, il suffit de voir que les points constructibles sont des intersections de cercles et droites, donc des racines de polynômes de degré 2. Les nombres constructibles sont donc dans des tours d'extensions quadratiques.

• Montrons que $K_0 = \mathbb{Q}$.
Les $(\omega^j)_{1\leqslant j\leqslant p-1}$ forment une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$, donc $\left(g^i(\omega)\right)_{0\leqslant i\leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$.
Soit $a \in K_0$, $\exists a_0, \dots, a_{p-2} \in \mathbb{Q}$,

$$a = a_0\omega + ... + a_{p-2}g^{p-2}(\omega),$$

mais

$$a = g(a) = a_{p-2}\omega + a_0 g(\omega) + ... + a_{p-1}g^{p-2}(\omega).$$

Il vient $a_0 = a_1 = ... = a_{p-2}$, donc

$$a = a_0(\omega + ... + g^{p-2}(\omega)) = -a_0 \in \mathbb{Q}.$$

Donc $K_0 = \mathbb{Q}$.

• Montrons que K_i est une extension quadratique de K_{i-1}.
Pour montrer que $\forall i \in [\![0, n-1]\!]$, $K_i \neq K_{i-1}$, on considère l'élément $b = \sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega)$.
On a :

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

Donc $b \in K_i$.
Puis

$$g^{2^{i-1}}(b) = \sum_{k=0}^{2^{n-i}-1} g^{k2^i+2^{i-1}}(\omega) \neq b$$

car on a décalé tous les indices de 2^{i-1} ; les coordonnées de b dans la famille des g^{k2^i} ne sont que des zéros.
On en déduit alors qu'on a la suite d'extensions :

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

Mais $2^n = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{\geqslant 2}$.
Ainsi, $\forall i \in [\![0, n-1]\!], [K_{i+1} : K_i] = 2$.

• Conclusion
Par le théorème de Wantzel, tous les éléments de $\mathbb{Q}(\omega)$ sont donc constructibles. [2]

□

Lemme.

→ Soit $n \geqslant 3$, alors $\mathcal{P}_n$ est constructible ssi $\mathcal{P}_{2n}$ est constructible.
→ Soit $n, m \geqslant 3$ sont premiers entre eux, alors $\mathcal{P}_{nm}$ est constructible ssi $\mathcal{P}_n$ et $\mathcal{P}_m$ le sont.

Démonstration. • Si $\mathcal{P}_{2n}$ est construit, on prend un point sur deux et on obtient les sommets de $\mathcal{P}_n$.
Réciproquement, si on a $\mathcal{P}_n$, on trouve le centre du polygone en construisant les médiatrices des côtés, puis on cherche les intersections du cercle circonscrit avec les médiatrices de chaque côté. Cela donne les sommets de $\mathcal{P}_{2n}$.
• Si $\mathcal{P}_n$ et $\mathcal{P}_m$ sont construits, on trouve une relation de Bézout $un + vm = 1$, ce qui donne $\frac{2\pi}{mn} = u\frac{2\pi}{m} + v\frac{2\pi}{n}$.
Il suffit de reporter u fois le premier angle et v fois le deuxième pour obtenir l'angle voulu. (On reporte juste u fois le côté associé à l'angle $\frac{2\pi}{m}$ sur le cercle, puis v fois l'autre et on aura alors le côté associé à l'angle voulu, donc un des côtés de $\mathcal{P}_{nm}$.)
Réciproquement, si $\mathcal{P}_{nm}$ est construit, on ignore $m-1$ sommets consécutifs sur m pour obtenir $\mathcal{P}_n$ et vice versa pour $\mathcal{P}_m$. □

2. Pour revenir à $\cos\frac{2\pi}{p}$, il suffit d'écrire $\cos\frac{2\pi}{p} = \frac{\omega + \omega^{-1}}{2} \in \mathbb{Q}(\omega)$, donc $\cos\frac{2\pi}{p}$ est constructible. En fait, on a même $K_{n-1} = \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)$.

Théorème (Gauss-Wantzel)**.**

Les seuls polygones réguliers à n côtés constructibles sont ceux pour lesquelles n est de la forme $n = 2^m p_1 ... p_k$ avec $m \in \mathbb{N}$ et p_i des nombres **premiers** de Fermat **distincts**.

Remarques : • C'est beau !
• Les seuls nombres premiers de Fermat connus à ce jour sont 3, 5, 17, 257, 65537. Il a été montré qu'il était très probable que ce soit les seuls.
• Pour faire ce développement, il faut savoir reprouver que $\mathbb{Q}(\omega)$ est un $\mathbb{Q}$ espace vectoriel de dimension $p - 1 = \varphi(p)$. Il faut aussi savoir reprouver que $(\omega, ..., \omega^{p-1})$ en forme une base.
Il faut faire attention à prendre comme exemple non trivial le plus simple $\mathbb{Q}(j)$. Pour $\mathbb{Q}(i)$, ça ne marche pas car i est une racine quatrième de l'unité et 4 n'est pas premier !

Adapté du travail de Florian Lemonnier.