Les polygones réguliers constructibles

Quelques pré-requis

Théorème (Wanzel)**.** *Un nombre est constructible si et seulement s'il appartient à une tout d'extensions quadratiques de* $\mathbf{Q}$*.*

Le polygone régulier à n côtés est constructible lorsque l'angle $2\pi/n$ est constructible, ce qui revient à dire $\cos(2\pi/n)$ est constructible.

Les nombres de Fermat sont les nombres de la forme $2^{(2^m)}+1$, $m \in \mathbf{N}$.

Ce qu'on va montrer.

Théorème (Gauß-Wanzel)**.** *Les polygones réguliers constructibles sont ceux dont le nombre de côtés n sont de la forme 2^α avec $\alpha \geq 2$ ou de la forme $2^\alpha p_1 p_2 \dots p_r$ où les p_i sont des nombres premiers de Fermat distincts.*

La preuve de ce théorème résulte de la concaténation des quatre résultats suivants, classés par ordre de difficulté.

Proposition 1. *Les angles de la forme $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles.*

Preuve. Il suffit de savoir construire des bissectrices. □

Proposition 2. *Si m et n sont premiers entre eux, l'angle $\widehat{\frac{2\pi}{mn}}$ est constructible si et seulement si $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ sont constructibles. En conséquence, si n a pour décomposition en facteurs premiers $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, le polygône régulier à n côtés est constructible si et seulement si les angles $\widehat{\frac{2\pi}{p_1^{\alpha_1}}}, \dots, \widehat{\frac{2\pi}{p_k^{\alpha_k}}}$ le sont.*

Preuve. Prouvons la première partie de l'énoncé. Le sens direct est facile et ne nécessite pas que m et n soient premiers entre eux : les angles $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ sont des multiples entiers de l'angle $\widehat{\frac{2\pi}{mn}}$. Pour la réciproque, on écrit une relation de Bézout entre m et n et il s'agit ensuite de construire la somme de deux angles constructibles, ce qui est possible. □

Proposition 3. *Soit $p \geq 3$ un nombre premier. Si $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible alors $\alpha = 1$ et p est un nombre de Fermat.*

Preuve. Notons $q = p^\alpha$ et $\omega = \exp(2i\pi/q)$. Par le théorème de Wanzel, on a :

$$[\mathbf{Q}(\omega) : \mathbf{Q}] = 2^m, \quad \text{pour un certain } m \in \mathbf{N}.$$

Mais comme le q-ème polynôme cyclotomique Φ_q est le polynôme annulateur de ω sur $\mathbf{Q}$, on a :

$$[\mathbf{Q}(\omega) : \mathbf{Q}] = 2^m = \varphi(q) = p^{\alpha-1}(p-1).$$

Comme p est impair, on a déjà $\alpha = 1$ et $p = 2^m + 1$. Reste à montrer que m est une puissance de 2. En écrivant $m = 2^\beta \lambda$ avec λ impair, on a : $p = 1 + (2^{(2^\beta)})^\lambda$ et comme $1 + X | 1 + X^\lambda$ (car (-1) est racine lorsque λ est impair), on a $1 + 2^{(2^\beta)} | p$ et le résultat suit puisque p est premier. □

Proposition 4. *La réciproque de la proposition 3 est vraie.*

PREUVE. Notons $p = 1 + 2^n$, ω une racine primitive p-ème de l'unité et $K = \mathbf{Q}(\omega)$. On a $[K : \mathbf{Q}] = p - 1$ et une base de K sur $\mathbf{Q}$ est $\{1, \omega, \ldots, \omega^{p-2}\}$.

Étape 1. Le groupe des automorphismes de K, sa vie, son oeuvre.

On note G le groupe des automorphismes de $K/\mathbf{Q}$. En appliquant $g \in G$ à $\Phi_p(\omega) = 0$, on voit que g est entièrement déterminé par l'image de ω qui ne peut être qu'un ω^k, $1 \leq k \leq p-1$. On note désormais $g_k \in G$ tel que

$$g_k(\omega) = \omega^k.$$

On a donc $G = \{g_1, \ldots, g_{p-1}\}$ mais on peut en dire plus : en considérant l'application :

$$\psi : G \to (\mathbf{Z}/p\mathbf{Z})^\times, \;\; g_k \mapsto \bar{k}$$

dont on peut montrer que c'est un isomorphisme de groupes, on sait aussi que G est un groupe cyclique d'ordre $p-1 = 2^n$, disons engendré par $g \in G$. Intéressons-nous maintenant aux sous-groupes : $G_i := \langle g^{2^i} \rangle$ pour $i \in \{1, \ldots, n\}$. Ils sont d'ordre 2^{n-i} et on a :

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G.$$

Étape 2. De la théorie de Galois sans le dire.

L'idée principale de la preuve consiste à associer aux sous-groupes G_i les sous corps :

$$K_i = \{z \in K, \; g^{2^i}(z) = z\} \subset K.$$

De ces sous-corps, proviendra la tour d'extensions quadratiques recherchée. Comme $g^{2^{i+1}} = (g^{2^i})^2$, on a déjà $K_i \subseteq K_{i+1}$ et comme $g^n = Id$, on a $K_n = K$. Reste à montrer :

$$(i) \;\; K_0 = \mathbf{Q} \qquad (ii) \;\; \forall i \in \{0, \ldots, n-1\}, \;\; [K_{i+1} : K_i] = 2.$$

Étape 3. Faisons le.

(i) On a clairement $\mathbf{Q} \subset K_0$. De plus, si $z \in K$, z s'écrit de façon unique :

$$z = \lambda_0\omega + \lambda_1 g(\omega) + \ldots + \lambda_{p-2} g^{p-2}(\omega).$$

Ainsi, si $z \in K_0$, on trouve en appliquant g à cette égalité : $\lambda_0 = \lambda_1 = \ldots = \lambda_{p-2}$ et alors :

$$z = \lambda_0(\omega + \omega^2 + \ldots + \omega^{p-1}) = -\lambda_0 \in \mathbf{Q}.$$

(ii) On montre d'abord que les inclusions $K_i \subset K_{i+1}$ sont strictes. Il suffit pour cela de voir que :

$$z = \sum_{h=0}^{2^{n-i-1}-1} g^{h2^{i+1}} \in K_{i+1} \setminus K_i.$$

Ensuite, il n'y a qu'à écrire :

$$2^n = [K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0].$$

Il y a n facteurs non égaux à 1 (car les inclusions sont strictes) d'où le résultat.

Étape 4. La conclusion.

Pour revenir à $\cos(2\pi/p)$, il suffit d'écrire :

$$\cos\frac{2\pi}{p} = \frac{1}{2}(\omega + \omega^{-1}) \in \mathbf{Q}(\omega).$$

En fait, on a même :

$$K_{n-1} = \mathbf{Q}\left(\cos\frac{2\pi}{p}\right)$$

mais c'est inutile. □

Référence. J-C. Carrega, *Théorie des corps, la règle et le compas*

102 Groupe des nombres complexes de module 1. Sous-groupe des racines de l'unité. Applications.
121 Nombres premiers. Applications.
125 Extensions de corps. Exemples et applications.
183 Utilisation des groupes en géométrie.