Polygones réguliers constructibles
Thm de Gauss-Wantzel

Référence :Carrega : Théorie des corps, la règle et le compas p.48 et 214 ou Mercier : Cours p.395.
Leçons : 125, 182, *102*, *183*

Lemme

1. Les angles de la forme $\widehat{\dfrac{2\pi}{2^\alpha}}$ sont constructibles, où $\alpha \in \mathbb{N}^*$.
2. 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, un polygone régulier à $n = \prod p_i^{\alpha_i}$ est constructible ssi les angles $\widehat{\dfrac{2\pi}{p_i^{\alpha_i}}}$ le sont.

Preuve :

1. C'est immédiat, puisque par récurrence, il suffit de savoir tracer des bissectrices à la règle et au compas.
2. $\Leftarrow$ 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.

■

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 $\beta \in \mathbb{N}$).

Preuve :

$\Rightarrow$ On pose $\omega = \exp\left(\dfrac{2i\pi}{p^\alpha}\right)$. On suppose que $\widehat{\dfrac{2\pi}{p^\alpha}}$ est constructible ie que $\cos\left(\dfrac{2\pi}{p^\alpha}\right)$ est constructible.

Alors, par le théorème de Wantzel [1], on obtient : $\left[\mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right] = 2^m$, où $m \in \mathbb{N}$.

Aussi, le polynôme cyclotomique Φ_{p^α} étant le polynôme minimal de ω, on a :

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

Comme $\omega + \omega^{-1} = 2\cos\dfrac{2\pi}{p^\alpha}$

$$\omega^2 - 2\omega\cos\frac{2\pi}{p^\alpha} + 1 = 0 \qquad (\star)$$

1. p.28 : Tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2. Ce théorème est puissant : il montre qu'on ne peut pas dupliquer le cube ($2^{\frac{1}{3}}$ non constructible) ou encore qu'on ne peut pas trisecter un angle.

on a $\cos\dfrac{2\pi}{p^\alpha} \in \mathbb{Q}(\omega)$ et même $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\dfrac{2\pi}{p^\alpha}\right)\right] = 2$.
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 on note toujours $\omega = \exp\left(\dfrac{2i\pi}{p}\right)$. But : vérifier les hypothèses du 2ème théorème de Wantzel [2].

Etape 1 Construire la bonne suite croissante de sous-corps.
On a : $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_p = \varphi(p) = p - 1$.
On note $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$; et si $g \in G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par [3] $g(\omega)$.
g étant un morphisme d'anneaux, on a : $0 = g(0) = g\left(\Phi_p(\omega)\right) = \Phi_p(g(\omega))$.
Donc $g(\omega)$ est nécessairement une racine de Φ_p, donc $g(\omega) \in \left\{\omega, \omega^2, \dots, \omega^{p-1}\right\}$.
Il faudrait alors montrer qu'on définit bien ainsi des automorphismes du corps $\mathbb{Q}(\omega)$; et alors [4]

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

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

Etape 2 Montrons que $K_0 = \mathbb{Q}$.
Comme g génère G, $\left(g^i(\omega)\right)_{0 \leqslant i \leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$.
Soit $z \in K_0$, $\exists \lambda_0, \dots, \lambda_{p-2} \in \mathbb{Q}$, $z = \displaystyle\sum_{i=0}^{p-2} \lambda_i g^i(\omega)$; mais $z = g(z) = \lambda_{p-2}\omega + \displaystyle\sum_{i=1}^{p-2} \lambda_{i-1} g^i(\omega)$.
Tous les scalaires λ_i sont donc égaux et $z = \lambda_0 \displaystyle\sum_{i=0}^{p-2} g^i(\omega) = \lambda_0 \sum_{j=1}^{p-1} \omega^j = -\lambda_0 \in \mathbb{Q}$. Donc $K_0 = \mathbb{Q}$.

Etape 3 Montrons que les inclusions sont strictes.
Pour montrer que $\forall i \in [\![0, n-1]\!], K_i \neq K_{i+1}$, il faudrait considérer l'élément $z = \displaystyle\sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\omega)$. [5]
On en déduit alors qu'on a la suite d'extensions :

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

Etape 4 Montrons que $\cos\left(\dfrac{2\pi}{p}\right)$ appartient bien à la dernière extension.
Déjà vu : $\cos\left(\dfrac{2\pi}{p}\right) \in K_n = \mathbb{Q}(\omega)$ par $(\star)$.

---

2. p.25. $t \in \mathbb{R}$ est constructible ssi $\exists s \in \mathbb{N}^*$, $L_1, \cdots, L_s$ des sous-corps de $\mathbb{R}$ tq
— $L_1 = \mathbb{Q}$,
— $L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
— $t \in L_s$

3. car une base de $\mathbb{Q}(\omega)$ est $\{1, \omega, \cdots, \omega^{p-2}\}$
4. ça se montre à la main, il faut expliciter l'isomorphisme.
5. Il faut se rappeler par cœur de ce z à l'oral. Calculatoire et pénible :

On a : $g^{2^i}(z) = \displaystyle\sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h + 2^i}(\omega) \neq z$ 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 : $g^{2^{i+1}}(z) = \displaystyle\sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}(h+1)}(\omega) = \sum_{h=1}^{2^{n-i-1}-1} g^{2^{i+1}h}(\omega) + \underbrace{g^{2^{i+1}2^{n-i-1}}(\omega)}_{=\omega} = z$.

Etape 5 Montrons qu'on a des extensions de degré 2 et conclusion.

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

Ainsi, $\forall i \in [\![0, n-1]\!], [K_{i+1} : K_i] = 2$ et on conclut par le théorème de Wantzel car $\cos\left(\frac{2\pi}{p}\right)$ constructible donc $\widehat{\frac{2\pi}{p}}$ aussi.

■

Notes :

✓ **A l'oral**, sans le **Lemme** 15'22 avec hésitation. Une seconde fois 14'14 en balançant le z qui marche bien pour l'inclusion stricte.
✓ Déf constructible p14. Nombre constructible : coordonnée d'un point constructible. Angle constructible : son cos est constructible.
✓ Il faut absolument savoir construire le pentagone régulier : c'est fait dans les livres. ✓ On peut montrer un truc plus fort : $K_{n-1} = \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)$. En effet,
Notons $f = g^{2^{n-1}}$; alors $K_{n-1} = \mathrm{Ker}(f - \mathrm{Id})$; et soit $\lambda \in \mathbb{Z}$ tel que $f(\omega) = \omega^\lambda$.
On a : $\omega = f^2(\omega) = \omega^{\lambda^2}$, donc $\omega^{\lambda^2-1} = 1$, d'où $\lambda^2 \equiv 1\,[p]$, puis $\lambda \equiv \pm 1\,[p]$.
Comme $f \neq \mathrm{Id}$, on a : $\lambda \not\equiv 1\,[p]$ donc $f(\omega) = \omega^{-1}$.
Donc $f\left(\cos\frac{2\pi}{p}\right) = f\left(\frac{1}{2}(\omega + f(\omega))\right) = \frac{1}{2}(f(\omega) + \omega) = \cos\frac{2\pi}{p}$.
Finalement, $\cos\frac{2\pi}{p} \in K_{n-1}$ et $\mathbb{Q}\left(\cos\frac{2\pi}{p}\right) \subseteq K_{n-1}$.
Or $\omega^2 - 2\omega\cos\frac{2\pi}{p} + 1 = 0$ donc $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)\right] = 2$.
Puis, il vient : $1 < [\mathbb{Q}(\omega) : K_{n-1}] \leqslant 2$ donc $[\mathbb{Q}(\omega) : K_{n-1}] = 2$ et $K_{n-1} = \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)$.