DVP Théorème de Gauss

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Leçons : 141, 191.

— Références :

  — Carrega.

Théorème 1 Les polygones réguliers constructibles (à la règle et au compas) sont ceux dont le nombre de côtés n est de la forme 2^α avec $\alpha \geq 2$ ou de la forme $2^\alpha p_1 \dots p_r$ avec $\alpha \in \mathbb{N}$ et où les p_i sont des nombres premiers distincts qui sont des nombres de Fermat $(2^{2^n}+1)$.

Preuve. **Lemme 2** Si m et n sont premiers entre eux, $\widehat{\frac{2\pi}{mn}}$ est constructible si et seulement si $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ sont constructibles.

Preuve.
— Si $\widehat{\frac{2\pi}{mn}}$ est constructible, on a $\widehat{\frac{2\pi}{n}} = m\widehat{\frac{2\pi}{nm}}$ et $\widehat{\frac{2\pi}{m}} = n\widehat{\frac{2\pi}{nm}}$. Ainsi, en reportant l'angle un nombre fini de fois, on peut construire les deux autres !
— Si $\widehat{\frac{2\pi}{n}}$ et $\widehat{\frac{2\pi}{m}}$ sont constructibles, par la relation de Bezout, on a accès à $\lambda, \mu \in \mathbb{Z}$ tel que $\lambda n + \mu m = 1$, d'où $\widehat{\frac{2\pi}{mn}} = \lambda\widehat{\frac{2\pi}{m}} + \mu\widehat{\frac{2\pi}{n}}$. Il suffit donc de savoir construire la somme de 2 angles, donc ok.

□

Lemme 3 Si $n \geq 3$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, le polygone régulier à n côtés est constructible si et seulement si les angles $\widehat{\frac{2\pi}{p_i^{\alpha_i}}}$ sont constructibles.

Preuve. C'est une récurrence immédiate sur k grâce au Lemme précédent.

□

Proposition 4

1. Les angles de la forme $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles,
2. Si $p \in \mathcal{P}$, $p \geq 3$, $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha = 1$ et que p est un nombre de Fermat.

Preuve.
1. Il suffit de savoir construire une bissectrice et de procéder par récurrence.
2. Soit $p \in \mathcal{P}$, $p \geq 3$.
   — Supposons $\widehat{\frac{2\pi}{p^\alpha}}$ constructible avec $\alpha \in \mathbb{N}^*$. Alors, par définition, $\cos\left(\frac{2\pi}{p^\alpha}\right)$ est constructible, et, par théorème de Wantzel, on a :

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right) : \mathbb{Q}\right] = 2^m \text{ pour un certain } m \in \mathbb{N}.$$

   On note $q = p^\alpha$, et on considère $\omega = e^{\frac{2i\pi}{q}}$. ω est racine q-ème de l'unité, i.e. racine de $X^q - 1$, donc ω est algébrique sur $\mathbb{Q}$.

Le polynôme minimal de ω sur $\mathbb{Q}$ est $P(X) = \prod_{i=1}^{h}(X - \omega_i)$ avec les ω_i parcourant $e^{\frac{2\imath k\pi}{q}}$, $k \wedge q = 1$, $k \in [\![1, q]\!]$: c'est le $q^{\text{ème}}$ polynôme cyclotomique.
On a $h = p^{\alpha-1}(p-1)$ par résultat sur l'indicatrice d'Euler, donc

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

$\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{p^\alpha}\right)$, donc $\cos\left(\frac{2\pi}{p^\alpha}\right) \in \mathbb{Q}(\omega)$ et on a $\omega^2 - 2\omega\cos\left(\frac{2\pi}{p^\alpha}\right) + 1 = 0$.
Ainsi, ω est algébrique et de degré 2 sur $\mathbb{Q}\left(\cos\left(\frac{2\pi}{q}\right)\right)$, d'où :

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{q}\right)\right)\right] = 2.$$

Il vient donc

$$p^{\alpha-1}(p-1) = 2^{m+1},$$

puis $\alpha = 1$ et $p = 1 + 2^{m+1}$. Montrons que $m+1$ est une puissance de 2 (on utilise juste le fait que p est premier).
On peut écrire $m + 1 = \lambda 2^\beta$ avec λ impair. On a donc $p = 1 + \left(2^{2^\beta}\right)^\lambda$. Comme λ est impair, $1 + X^\lambda$ est divisible par $1 + X$, donc p est divisible par $1 + 2^{2^\beta}$. Comme p est premier, $p = 1 + 2^{2^\beta}$.

— Pour la réciproque, on se donne $p = 1 + 2^{2^n} \in \mathcal{P}$.

(a) Comme $p \in \mathcal{P}$, avec $\omega = e^{\frac{2\imath\pi}{p}}$, on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p) = p-1$, et $\mathcal{B} = \{\omega^i\}_{i\in[\![0,p-2]\!]}$ est une base de $\mathbb{K} := \mathbb{Q}(\omega)$, donc $\mathcal{B}' = \{\omega^i\}_{i\in[\![1,p-1]\!]}$ aussi.

(b) Un automorphisme de $\mathbb{K}$ laisse invariant les éléments de $\mathbb{Q}$. L'ensemble des automorphismes de $\mathbb{K}$, noté G est donc $\{g_k : \omega \mapsto \omega^k\}_{k\in[\![1,p-1]\!]}$ (car $g \in G$ est déterminé par l'image de ω, qui doit être une racine primitive de l'unité, ...).

(c) On montre que $\begin{pmatrix} (\mathbb{Z}/p\mathbb{Z})^* & \xrightarrow{\sim} & G \\ k & \longmapsto & g_k \end{pmatrix}$ est un isomorphisme de groupe. Ainsi, G est cyclique d'ordre $p-1$, et possède donc un générateur, noté g. Puisque $\omega = g^0(\omega)$, on peut réécrire $\mathcal{B}' = \{g^h(\omega)\}_{h\in[\![0,p-2]\!]}$.

(d) Comme G est d'ordre $p - 1 = 2^n$, g l'est aussi, et $G_i := \left\langle g^{2^i}\right\rangle$ est donc d'ordre 2^{n-i}, pour $i \in [\![1, n]\!]$. On a :

$$\{1\} = G_n \subset \cdots \subset G_1 \subset G_0 := G.$$

On associe à cette suite les sous-corps $\mathbb{K}_i := \{z \in \mathbb{K}, g^{2^i}(z) = z\} = \mathbb{K}^{G_i}$. Par définition, on a :

$$\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n = \mathbb{K}.$$

(e) Montrons que $\mathbb{K}_0 = \mathbb{Q}$. On a $\mathbb{Q} \subseteq \mathbb{K}_0$. Si $z \in \mathbb{K}_0$, on a :

$$z = \sum_{i=0}^{p-2} \lambda_i g^i(\omega),$$

donc

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

Ainsi, $\lambda_0 = \cdots = \lambda_{p-2}$, et :

$$z = \lambda_0 \sum_{i=0}^{p-2} \omega = -\lambda_0 \in \mathbb{Q}.$$

(f) Montrons que la suite d'inclusions est stricte : Pour $\mathbb{K}_i \subsetneq \mathbb{K}_{i+1}$, avec $z = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\omega)$, on a $z = g^{2^{i+1}}(z) \neq g^{2^i}(z)$, d'où le résultat.

(g) Par relation sur les degrés d'extensions, il vient :

$$[\mathbb{K} : \mathbb{K}_0] = 2^n = \prod_{i=0}^{n-1} \underbrace{[\mathbb{K}_{i+1} : \mathbb{K}_i]}_{\geq 2}.$$

Il vient donc $[\mathbb{K}_i : \mathbb{K}_{i+1}] = 2$, puis, par théorème de Wantzel, il vient que $\omega \in \mathbb{K}$ est constructible, d'où le résultat !

□

Cela permet d'achever la preuve grâce au Lemme 3 !

□