Le théorème de Gauß pour les polygones réguliers constructibles.

Référence : Théorie des corps ; La règle et le compas.
Jean-Claude Carrega

2011-2012

Prérequis : Théorème de Wantzel.

On rappelle que le polygone régulier à n côtés est dit *constructible* si l'angle de mesure $\frac{2\pi}{n}$ est constructible, *i.e* si $e^{\frac{2\pi}{n}}$ est constructible.

On notera dans la suite $P(n)$ "le" polygone régulier à n côtés (on le suppose inscrit dans le cercle unité, avec un sommet coïncidant avec 1).

Théorème 1 : de Gauß, 1801
Les polygones réguliers constructibles sont ceux donc le nombre de côtés n est de la forme 2^α où $\alpha > 1$, ou de la forme $2^\alpha p_1 \cdots p_r$, $\alpha, i \in \mathbb{N}$, et les p_i sont des nombres premiers de Fermat distincts.

Démonstration. On commence par montrer qu'on peut se ramener à des nombres premiers.

Lemme 2
Si m et n sont premiers entre eux, alors $P(mn)$ est constructible si et seulement si $P(n)$ et $P(m)$ sont constructibles.

Démonstration. Le sens direct est évident :

$$\frac{2\pi}{n} = m\frac{2\pi}{mn} \text{ et } \frac{2\pi}{m} = n\frac{2\pi}{mn},$$

et il est facile de construit le multiple d'un angle constructible.

Pour le sens réciproque, on utilise l'identité de Bezout :

$$\exists \lambda, \mu \in \mathbb{Z},\ \lambda n + \mu m = 1.$$

On en déduit

$$\frac{2\pi}{mn} = \lambda\frac{2\pi}{n} + \mu\frac{2\pi}{m},$$

et on sait construire les produits et sommes d'angles constructibles. ◊

Par récurrence, on en déduit

Lemme 3
Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors $P(n)$ est constructible si et seulement si *$P(p_1^{\alpha_1}), \ldots, P(p_k^{\alpha_k})$ sont constructibles.*

Il nous reste maintenant à caractériser les p_i et α_i qui conviennent.

Lemme 4
Soit $\alpha \in \mathbb{N}^*$. Alors :

(i) $P(2^\alpha)$ est constructible.

(ii) Si p est un nombre premier impair, alors $P(p^\alpha)$ est constructible si et seulement si *$\alpha = 1$ et p est un nombre de Fermat (*i.e $p = 1 + 2^{(2^\beta)}$*).*

Démonstration. On se fixe $\alpha \in \mathbb{N}^*$.

(i) On sait construire la bissectrice d'un angle, et donc ce point est évident.

(ii) Soit p premier impair. On pose $q = p^\alpha$.

Supposons que $P(q)$ est constructible. Alors par définition, $e^{\frac{2\pi}{q}}$ est constructible, et donc par théorème de Wantzel :

$$\exists m \in \mathbb{N},\ \left[\mathbb{Q}\left(e^{\frac{2\pi}{q}}\right) : \mathbb{Q}\right] = 2^m.$$

On appelle $\omega = e^{\frac{2\pi}{q}}$. ω est une racine q-ième de l'unité, et donc son polynôme minimal est le q-ième polynôme cyclotomique Φ_q, qui est de degré $p^{\alpha-1}(p-1)$, et donc

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

On en déduit

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

et comme p est premier impair, on en déduit donc $\alpha = 1$ et $p = 2^m$.

Il nous reste à montrer que $m+1$ est nécessairement une puissance de 2. On écrit $m+1 = \lambda 2^\beta$, avec λ entier non nul impair et β entier.

On a donc

$$p = 1 + \left(2^{(2^\beta)}\right)^\lambda.$$

Comme λ est impair, $X+1$ divise $X^\lambda+1$, et donc $1+2^{(2^\beta)}$ divise p. Comme p est premier, on a le résultat.

Montrons maintenant le sens réciproque : soit $p = 1 + 2^n$ un nombre premier de Fermat.

On pose $\omega = e^{2i\pi/p}$, et $K = \mathbb{Q}(\omega)$. p étant premier, le degré de l'extension K sur $\mathbb{Q}$ est $p-1$. Une base de K est

$$\{1, \omega, \omega^2, \ldots, \omega^{p-2}\}.$$

Soit G le groupe des automorphismes de K (ils laissent $\mathbb{Q}$ invariants). Si $g \in G$, alors, g est entièrement déterminé par $g(\omega)$. Comme $g(\omega)$ reste une racine p-ième de l'unité, différente de 1, et réciproquement, toutes ces applications sont des automorphismes de K.

G est donc cyclique, d'ordre $p-1 = 2^n$. On peut ainsi se fixer un générateur de G, soit g.

Posons pour $0 \leqslant i \leqslant n$

$$K_i := \left\{z \in K \mid g^{2^i}(z) = z\right\}.$$

On a donc une tour d'extensions :

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K.$$

Il est assez clair que $\mathbb{Q} \subseteq K_0$, et si $z \in K_0$, alors on peut l'écrire sous la forme

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

et en applicant g, on obtient $z = -\lambda_0 \in \mathbb{Q}$.

Donc $K_0 = \mathbb{Q}$.
Montrons que toutes les inclusions sont strictes, par exemple $K_O \subset K_1$. On pose

$$z = \omega + g^2(\omega) + \cdots + g^{2^n-2}(\omega).$$

Alors $g^2(z) = z$ car $g^{2^n}(\omega) = \omega$, mais $g(z) \neq z$ par unicité de l'écriture de z dans la base $\{g^h(\omega) \mid 0 \leqslant h \leqslant p-2\}$.
On a donc une tour d'extensions strictes

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = K.$$

Comme $[K : \mathbb{Q}] = 2^n$, on obtient

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

et comme chaque facteur est différent de 1, on a nécessairement pour tout i :

$$[K_{i+1} : K_i] = 2.$$

Par théorème de Wantzel, ω est donc bien constructible.

$\Diamond$

□