VM
21/05/15
1

Polygones constructibles à la règle et au compas

125, 141, (151)

Réf : Carrega

Ce théorème utilise en l'admettant le résultat suivant :

Théorème (Wantzel)

Soit $z \in \mathbb{C}$. z est constructible ssi il existe $n \geq 1$ et une suite finie de sous-corps de $\mathbb{C}$, notée $K_1, \dots, K_n$, telle que $K_1 = \mathbb{Q}$; $z \in K_n$, $K_1 \subset \dots \subset K_n$ et $\forall i \in \{1, \dots, n-1\}$, $[K_{i+1} : K_i] = 2$.

On démontre dans ce développement le résultat suivant :

Théorème (Gauss)

Soit p premier impair. Alors le nombre $\xi_p = e^{2i\pi/p}$ est constructible ssi p est un nombre premier de Fermat (i.e de la forme $2^n + 1$).

qui est un cas particulier du résultat :

Théorème (Gauss)

Soit $m \geq 2$ un entier. Alors le nombre $\xi_m = e^{2i\pi/m}$ est constructible ssi $m = 2^n p_1 \dots p_r$, où $n \in \mathbb{N}$, $r \in \mathbb{N}$, p_i premiers impairs distincts de Fermat.

dém :

Soit p un premier impair tel que ξ_p est constructible.

Le polynôme minimal de ξ_p sur $\mathbb{Q}$ est ϕ_p (annulateur et irréductible). Donc $[\mathbb{Q}[\xi_p] : \mathbb{Q}] = \deg(\phi_p) = \varphi(p) = p - 1$.

On d'après le théorème de Wantzel, il existe un corps K tel que $[K : \mathbb{Q}] = 2^m$ pour un certain $m \in \mathbb{N}$ et $\xi_p \in K$.

On a donc :

K
|
$\mathbb{Q}(\xi_p)$
|
$\mathbb{Q}$

et par multiplicativité des degrés, $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = 2^n$ pour un certain $n \in \mathbb{N}$

Donc $p = 2^n + 1$: p est de Fermat.

· Réciproquement, soit p un nombre premier de Fermat : $p = 2^n + 1$.
On note $\omega = \xi^{\uparrow}$ et $K = \mathbb{Q}(\omega)$.
Soit G l'ensemble des automorphismes de corps de K.

· G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$: en effet, un élément g de G est entièrement déterminé par l'image de ω. On ϕ_p annule ω, donc $\phi_p(g(\omega)) = g(\phi_p(\omega)) = g(0) = 0$. Donc $g(\omega)$ est une racine de ϕ_p : il existe $k \in \{0, \dots, p-1\}$ tel que $g(\omega) = \omega^k$. On $k \neq 0$ car g est surjective.
Réciproquement, pour tout $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, on définit

$$g_k : K \to K, \quad P(\omega) \mapsto P(\omega^k) \quad \text{où } P \in \mathbb{Q}[X]$$

· g_k est bien définie : si $P(\omega) = Q(\omega)$, alors ω annule $P - Q$ donc ϕ_p divise $P - Q$. On $\phi_p(\omega^k) = 0$ donc $P(\omega^k) = Q(\omega^k)$.
· g_k est un morphisme de corps.
· g_k est bijective, de réciproque $g_{k^{-1}}$.
On a donc une bijection $(\mathbb{Z}/p\mathbb{Z})^\times \to G$ et on vérifie

$$k \mapsto g_k$$

que c'est un isomorphisme de groupe.

· Ainsi, G est cyclique. Soit g un générateur de G : g est d'ordre $p - 1 = 2^n$.
$\forall i \in \{0, \dots, n\}$, on définit $K_i = \{x \in K \mid g^{2^i}(x) = x\}$.
On remarque que : · $K_n = K$ car $g^{2^n} = id_K$.
· $K_i \subset K_{i+1}$ $\forall i$.

· De plus, $K_0 = \mathbb{Q}$:
En effet, $\{\omega, g(\omega), \dots, g^{\uparrow-2}(\omega)\} = \{\omega, \omega^2, \dots, \omega^{\uparrow-1}\}$ est une famille $\mathbb{Q}$-libre de taille $p-1$, donc une $\mathbb{Q}$-base de $\mathbb{Q}(\omega) = K$.
Tout $x \in K$ se décompose de manière unique en $x = \sum_{i=0}^{\uparrow-2} \lambda_i g^i(\omega)$, $\lambda_i \in \mathbb{Q}$.
Alors $g(x) = \sum_{i=0}^{\uparrow-2} \lambda_i g^{i+1}(\omega) = \sum_{i=1}^{\uparrow-2} \lambda_{i-1} g^i(\omega) + \lambda_{\uparrow-2}\, \omega$.

VH
21/05/15
2

Ainsi, par unicité de la décomposition, on a

$$g(x) = x \iff \forall i,\ \lambda_i = \lambda_0 \iff x = \lambda_0 \underbrace{\sum_{i=0}^{n-2} g^i(u)}_{\text{somme des racines primitives } p\text{-ièmes de l'unité} = -1}$$

$$\iff x \in \mathbb{Q}$$

Donc $K_0 = \mathbb{Q}$.

- $\forall i,\ [K_{i+1} : K_i] = 1$ ou 2.

Soit $i \leq n-1$. On a $g^{2^i}(K_{i+1}) \subset K_{i+1}$. En effet, si $x \in K_{i+1}$, $g^{2^{i+1}}(g^{2^i}(x)) = g^{2^i}(g^{2^{i+1}}(x)) = g^{2^i}(x)$ donc $g^{2^i}(x) \in K_{i+1}$.

Soit $\tau = g^{2^i}|_{K_{i+1}}$. $\tau|_{K_i} = g^{2^i}|_{K_i} = id_{K_i}$ donc τ est un K_i-endomorphisme de K_{i+1}. De plus, $\tau^2 = g^{2^{i+1}}|_{K_{i+1}} = id_{K_{i+1}}$ donc $X^2 - 1$ annule τ.

Donc τ est diagonalisable de valeurs propres 1 et -1.

Ainsi, $K_{i+1} = E_1 \oplus E_{-1}$ où $E_{\pm 1}$ sev propre associé à ± 1.

$E_1 = K_i$ par définition.

Si $E_{-1} \neq \{0\}$, soient x, x' non nuls dans E_{-1}.

Alors $\tau\left(\frac{x}{x'}\right) = \frac{\tau(x)}{\tau(x')} = \frac{-x}{-x'} = \frac{x}{x'}$ donc $\frac{x}{x'} \in K_i$: E_{-1} est au plus de dimension 1 donc $[K_{i+1} : K_i] \leq 2$.

On conclut :

$$2^n = [K : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{=1 \text{ ou } 2}$$

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

D'après le théorème de Wantzel, u est constructible.

Rem : Un nombre de Fermat est par définition de la forme $2^{2^m}+1$.

On si $p = 2^n + 1$ est premier, il est nécessairement de la forme $2^{2^m}+1$. En effet, $n = 2^k \ell$ avec ℓ impair

$$p = 2^{2^k \ell} + 1 = \left(2^{2^k}\right)^\ell - (-1)^\ell$$

$$= \left(2^{2^k}+1\right) \sum_{j=0}^{\ell-1} \left(2^{2^k}\right)^j (-1)^{\ell-j-1}$$

p premier donc $\ell = 1$.