leçons : 102 : Groupe des nb $\mathbb{C}$x de module 1 125 : Extensions de corps. 182 : Applications des nb $\mathbb{C}$x à la géométrie 183 : Utilisation des groupes en géométrie	Gauss - Wantzel (43)	Références : Tauvel Caniéga

Thm : Soit $p \geq 3$ premier et $\alpha \geq 1$.
Alors $e^{\frac{2i\pi}{p^\alpha}}$ est constructible ssi $\alpha = 1$ et p est un nombre premier de Fermat

preuve :

- sens direct : Supposons $\omega = e^{\frac{2i\pi}{p^\alpha}}$ constructible

D'après le thm de Wantzel : $\exists m \geq 0$ $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$

Or $\phi_{p^\alpha}(\omega) = 0$ et ϕ_{p^α} est irréductible sur $\mathbb{Q}$ donc ϕ_{p^α} est le polynôme minimal de ω sur $\mathbb{Q}$. D'où $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \phi_{p^\alpha} = \varphi(p^\alpha) = p^{\alpha-1}(p-1) = 2^m$

Donc $\alpha = 1$ et $p = 2^m + 1$ □

- Sens réciproque :

(1) On pose $\omega = e^{\frac{2i\pi}{p}}$ où $p = 2^m + 1$ est premier.

On pose $Q(X) = 1 + X + \dots + X^{p-1} \in \mathbb{Q}[X]$. $Q(\omega) = 0$ et Q est le polynôme minimal de ω sur $\mathbb{Q}$. On pose $K = \mathbb{Q}(\omega)$.

On a $[K : \mathbb{Q}] = p-1$ et $(\omega, \dots, \omega^{p-1})$ est une base du $\mathbb{Q}$-ev K.

(2) On pose $G = \mathrm{Aut}_{\mathbb{Q}}(K)$ et soit $g \in G$.

g est entièrement déterminer par sa valeur en ω : $g(\omega)$.

Or $Q(g(\omega)) = g(Q(\omega)) = g(0) = 0$

Donc $g(\omega)$ est une racine de Q.

les racines de Q étant les ω^i pour $i \in [\![1, p-1]\!]$,

$\exists i \in [\![1, p-1]\!] \mid g(\omega) = \omega^i$

Réciproquement : $\forall i \in [\![1, p-1]\!]$ $\exists g \in \mathrm{Aut}_{\mathbb{Q}}(K)$ $g(\omega) = \omega^i$

en effet par la Propriété universelle : $\exists g$, $\mathbb{Q}[X] \to \mathbb{Q}(\omega)$, $X \mapsto \omega^i$ morphisme surjectif

$\mathrm{Ker}\, g = (Q)$ et g passe au quotient en $g : \mathbb{Q}(\omega) \simeq \frac{\mathbb{Q}[X]}{(Q)} \xrightarrow{\simeq} \mathbb{Q}(\omega)$, $\bar{X} \mapsto \omega^i$

On en déduit un isomorphisme de groupes :

$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\simeq} G$, $i \mapsto (g_i : \omega \mapsto \omega^i)$ donc G est cyclique d'ordre $p-1$.

Soit g un générateur de G.

③ g est d'ordre $2^m = p-1$

Notons $G_i = \langle g^{2^i} \rangle$ pour $i \in [\![0,m]\!]$

On a $G_m = \{id\} \subset G_{m-1} \subset \dots \subset G_1 \subset G_0 = G$

Posons $K_i = \{ x \in K \mid g^{2^i}(x) = x \} = K^{G_i}$

Alors (i) $\forall i \in [\![0,m]\!]$ K_i est un sous-corps de K

(ii) $\forall i \in [\![0,m-1]\!]$ $K_i \subset K_{i+1}$

(iii) $K_0 = \mathbb{Q}$.

preuve de (iii) :

Soit $x \in K_0$. Alors $\forall i \in (\mathbb{Z}/p\mathbb{Z})^*$ $g_i(x) = x$

$\exists (\lambda_1, \dots, \lambda_{p-1}) \in \mathbb{Q} \mid x = \lambda_1 \omega + \dots + \lambda_{p-1} \omega^{p-1}$

$\forall i \in [\![1,p-1]\!]$ $\lambda_1 \omega + \dots + \lambda_{p-1} \omega^{p-1} = x = g_i(x) = \lambda_1 \omega^i + \dots + \lambda_{p-1} \omega^{i(p-1)}$ $(*)$

$\omega^p = 1$ et $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ est un isomorphisme de groupes
$\bar{k} \mapsto \bar{i}\bar{k}$

Soit $k \in [\![1,p-1]\!]$, soit $i \in [\![1,p-1]\!]$ tq $\bar{i}\bar{k} = 1$ (ie $\bar{i} = \bar{k}^{-1}$)

Alors on a $\lambda_k = \lambda_1$ par $(*)$; D'où $\lambda_1 = \lambda_2 = \dots = \lambda_k$

D'où $x = \lambda_1(\omega + \dots + \omega^{p-1}) = -\lambda_1 \in \mathbb{Q}$.

$K_0 \subset \mathbb{Q}$ et $\mathbb{Q} \subset K_0$ trivial.

(iv) $\forall i \in [\![0,m-1]\!]$ $K_i \subsetneq K_{i+1}$

preuve de (iv) : posons $z = \omega + g^{2^{i+1}}(\omega) + g^{2\times 2^{i+1}}(\omega) + \dots + g^{2^{i+1}[2^{m-i-1}-1]}(\omega)$

Alors $g^{2^i}(z) = g^{2^i}(\omega) + g^{3\times 2^i}(\omega) + g^{5\times 2^i}(\omega) + \dots + g^{2^i[2^{m-i}-1]}(\omega)$

Or $2^m - 2^i \leq p-1$ et $(\omega, \dots, \omega^{p-1})$ est une base

donc $z \neq g^{2^i}(z)$ (le coefficient devant ω n'est pas le même)

et $g^{2^{i+1}}(z) = g^{2^{i+1}}(\omega) + g^{2\times 2^{i+1}}(\omega) + g^{3\times 2^{i+1}}(\omega) + \dots + \underbrace{g^m(\omega)}_{=\omega} = z$

Donc $z \in K_{i+1} \setminus K_i$

④ Comme $K_m = K$, on a $[K:\mathbb{Q}] = 2^m = \prod_{i=0}^{m-1} \underbrace{[K_{i+1}:K_i]}_{\geq 2} \geq 2^m$

donc $\forall i \in [\![0,m-1]\!]$ $[K_{i+1}:K_i] = 2$

et $\omega \in K$ est constructible.