* Théorème de Gauss-Wantzel : dagons 102, 125, 127, 141, 144, (121) [Carrégaud], IV 2 et X 4.1

1) Soit $n \geq 3$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors, $e^{\frac{2i\pi}{n}}$ est constructible ssi les $e^{\frac{2i\pi}{p_i^{\alpha_i}}}$ sont constructibles.

2) $\forall \alpha \in \mathbb{N}$, $e^{\frac{2i\pi}{2^\alpha}}$ est constructible.

3) Soient $p \geq 3$ un nombre premier et $\alpha \in \mathbb{N}^*$. Alors, $e^{\frac{2i\pi}{p^\alpha}}$ est constructible ssi $\alpha = 1$ et p est un nombre premier de Fermat (i.e. $p = 2^m + 1$ pour un certain $m \in \mathbb{N}^*$)

Remarques :

* On admettra le théorème de Wantzel :

$z \in \mathbb{C}$ est constructible $\Leftrightarrow \exists \mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\ell (\subseteq \mathbb{C})$ une tour d'extensions quadratiques tq $z \in K_\ell$.

* Si $p = 2^m + 1$ est un nombre premier de Fermat, alors $m = 2^k$. En effet, sinon on pourrait écrire $m = 2^k \ell$ avec $\ell \geq 3$ impair et alors :

$$p = (2^{2^k})^\ell + 1$$
$$= 1 - (-2^{2^k})^\ell$$
$$= \underbrace{(1 + 2^{2^k})}_{>1}\underbrace{(\cdots)}_{>1} \quad \lightning$$

preuve :

1) Il suffit de montrer, pour $m \wedge n = 1$: $e^{\frac{2i\pi}{mn}}$ constructible $\Leftrightarrow e^{\frac{2i\pi}{m}}$ et $e^{\frac{2i\pi}{n}}$ constructibles.

Le sens direct est immédiat car l'ensemble des nombres constructibles est un corps.

Réciproquement, supposons $e^{\frac{2i\pi}{m}}$ et $e^{\frac{2i\pi}{n}}$ constructibles. On a $m \wedge n = 1$ donc $\exists u, v \in \mathbb{Z}$ tq $mu + nv = 1$. Alors $\frac{2i\pi}{mn} = v\frac{2i\pi}{m} + u\frac{2i\pi}{n}$ donc $e^{\frac{2i\pi}{mn}} = (e^{\frac{2i\pi}{m}})^v (e^{\frac{2i\pi}{n}})^u$, ce qui permet de conclure.

2) C'est immédiat par récurrence car on sait construire les bissectrices.

3) $\Rightarrow$

Supposons $\omega = e^{\frac{2i\pi}{p^\alpha}}$ constructible.

Le corollaire du théorème de Wantzel nous indique alors que ω est algébrique (sur $\mathbb{Q}$) et qu'on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$ pour un $m \in \mathbb{N}$.

Or on sait également que ω est une racine primitive p^α-ième de l'unité et donc que son polynôme minimal sur $\mathbb{Q}$ est le polynôme cyclotomique Φ_{p^α} (on admet son irréductibilité sur $\mathbb{Q}$).

Dév. dég. 22

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

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

- Par unicité de la décomposition en facteurs premiers, on a :

$\alpha = 1$ et $p-1 = 2^m$

⟸ Soit $p = 2^m + 1$ un nombre premier de Fermat

Notons $\omega := e^{\frac{2i\pi}{p}}$ et $K := \mathbb{Q}(\omega)$.

Le polynôme minimal de ω est Φ_p qui est de degré $p-1$ et donc $(1, \omega, \omega^2, \dots, \omega^{p-2})$ est une $\mathbb{Q}$-base de K

Posons $G := \mathrm{Aut}(K) = \mathrm{Aut}_{\mathbb{Q}}(K)$.

* déjà $G \simeq \mathbb{F}_p^\times$:

- Pour $\bar{k} \in \mathbb{F}_p^\times$, posons $g_k : K \to K$, $P(\omega) \mapsto P(\omega^k)$

$g_k \in \mathrm{Aut}(K)$ car ω et ω^k ont le même polynôme minimal Φ_p et on dispose donc de deux isomorphismes $\varphi : \mathbb{Q}[X]/\Phi_p \to \mathbb{Q}(\omega)$, $\bar{P} \mapsto P(\omega)$ et $\theta : \mathbb{Q}[X]/\Phi_p \to \mathbb{Q}(\omega^k)$, $\bar{P} \mapsto P(\omega^k)$,

et donc $g_k = \theta \circ \varphi^{-1}$. De plus $\mathbb{Q}(\omega^k) \subseteq \mathbb{Q}(\omega) = K$ et on a égalité par égalité des dimensions

Posons alors $\Psi : \mathbb{F}_p^\times \to G$, $\bar{k} \mapsto g_k$

- Pour $\bar{k} \neq \bar{l} \in \mathbb{F}_p^\times$, on a $g_k(\omega) = \omega^k \neq \omega^l = g_l(\omega)$ donc Ψ est injective

- Soit $g \in G$.

$0 = g(\Phi_p(\omega)) = \Phi_p(g(\omega))$, or les racines de Φ_p sont $\{\omega, \omega^2, \dots, \omega^{p-2}\}$ et donc $g(\omega) = \omega^k$ pour un $k \in [\![1; p-1]\!]$.

Ainsi, $g(\omega) = g_k(\omega)$ et donc $g = g_k$ car $K = \mathbb{Q}(\omega)$

Ainsi, Ψ est surjective.

- $g_{kl}(\omega) = \omega^{kl} = (\omega^l)^k = g_k \circ g_l(\omega)$ donc $g_{kl} = g_k \circ g_l$ et donc Ψ est un morphisme de groupes.

- Ainsi, on dispose bien d'un isomorphisme $\Psi : \mathbb{F}_p^\times \xrightarrow{\sim} G$

Or, on sait que le groupe multiplicatif d'un corps fini est cyclique et donc il en est de même pour G :

$$\exists g \in G \text{ tq } G = \langle g \rangle = \{g^k,\ 1 \leq k \leq p-1\}$$

Posons $\beta = (g(\omega), g^2(\omega), \dots, g^{p-1}(\omega))$

Par ce qu'on vient de dire, β est simplement une permutation de $(g_2(\omega), \dots, g_{p-1}(\omega)) = (\omega, \dots, \omega^{p-2})$ qui est une $\mathbb{Q}$-base de $\mathbb{K}$, donc β est également une $\mathbb{Q}$-base de $\mathbb{K}$

Pour $i \in [\![0; m]\!]$, posons $G_i := \langle g^{2^i} \rangle$

La suite (G_i) est clairement décroissante et on a : $G_0 = \langle g \rangle = G$ et $G_m = \langle g^{2^m} \rangle = \langle g^{p-1} \rangle = \langle id \rangle = \{id\}$.

On dispose donc de :

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{id\}$$

Posons alors $\mathbb{K}_i := \{z \in \mathbb{K},\ \forall h \in G_i : h(z) = z\}$, c'est un sous-corps de $\mathbb{K}$

La suite $(\mathbb{K}_i)$ est alors clairement croissante : $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$

On a : $\mathbb{K}_m = \{z \in \mathbb{K},\ z = z\} = \mathbb{K}$.

* Alg $\mathbb{K}_0 = \mathbb{Q}$:

$\forall h \in G$, h fixe $\mathbb{Q}$ et donc $\mathbb{Q} \subseteq \mathbb{K}_0$

Soit $z = \sum_{k=1}^{p-1} \lambda_k g^k(\omega) \in \mathbb{K}_0$

On a $g(z) = z$, i.e. : $\lambda_1 g^2(\omega) + \lambda_2 g^3(\omega) + \dots + \lambda_{p-2} g(\omega) = \lambda_1 g(\omega) + \dots + \lambda_{p-2} g^{p-1}(\omega)$.

Par liberté de β, on déduit : $\forall k \in [\![1; p-2]\!]$: $\lambda_k = \lambda_{k+1}$ et donc :

$$z = \sum_{k=1}^{p-1} \lambda_1 g^k(\omega) = \lambda_1 \left(\sum_{k=1}^{p-1} g^k(\omega) \right) = \lambda_1 \left(\sum_{k=1}^{p-1} \omega^k \right) = -\lambda_1$$

(grâce aux relations coeff/racines sur Φ_p)

Donc : $z = -\lambda_1 \in \mathbb{Q}$.

* Alg $\mathbb{K}_i \subsetneq \mathbb{K}_{i+1}$:

Soit $z := \sum_{k=1}^{2^{m-i-1}} g^{2^i \cdot k}(\omega)$

On a : $g^{2^{i+1}}(z) = \sum_{k=1}^{2^{m-i-1}} g^{2^{i+1}(k+1)}(\omega)$

$$= \sum_{k=2}^{2^{m-i-1}+1} g^{2^{i+1} \cdot k}(\omega)$$

$$= \sum_{k=2}^{2^{m-i-1}} g^{2^{i+1} \cdot k}(\omega) = z$$

Donc : $z \in \mathbb{K}_{i+1}$.

On a : $g^{2^i}(z) = \sum_{k=1}^{2^{m-i-1}} g^{2^{i+1} \cdot k + 2^i}(\omega)$

En particulier, $g^{2^i}(z)$ a un coefficient non nul devant $g^{2^i}(\omega)$, ce qui n'est pas le cas de z, donc : $g^{2^i}(z) \neq z \rightsquigarrow z \notin \mathbb{K}_i$

Dev. Alg. 23

Ainsi, on a $[K_{i+1} : K_i] \geq 2$.

Donc, par le théorème de la base télescopique :

$$2^m \leq [K_1 : K_0][K_2 : K_1] \cdots [K_m : K_{m-1}] = [K_m : K] = [K : \mathbb{Q}] = 2^{\alpha_m}$$

On a donc égalité partout et donc $\forall i : [K_{i+1} : K_i] = 2$.

Ainsi, on a une tour d'extensions quadratiques :

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K \quad \text{et} \quad \omega \in K$$

Donc, par le théorème de Wantzel : ω est constructible.