Rappel (Wantzel) $z \in \mathcal{C}$

$\iff z \in K_r / K_{r-1} / \dots / K_1 / K_0 = \mathbb{Q}$

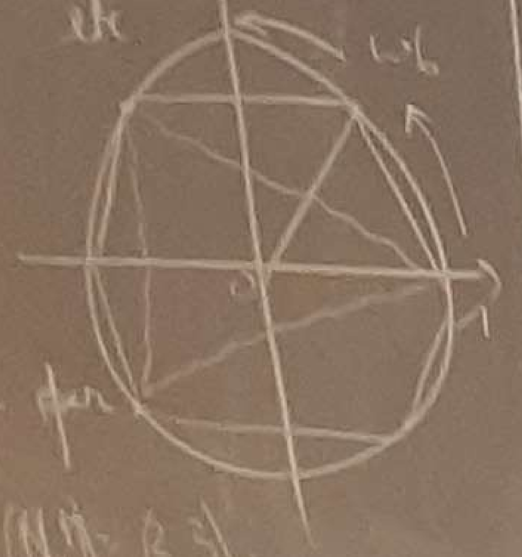
avec $[K_i : K_{i-1}] = 2$.

Th (Gauss-Wantzel) Le polygone à N côtés est constructible ssi

$$N = 2^r p_1 \dots p_n$$

où les p_i sont des nombres premiers de Fermat 2 à 2 distincts.

Rq • Construire le polygone, c'est construire $\omega = e^{2i\pi/N}$.



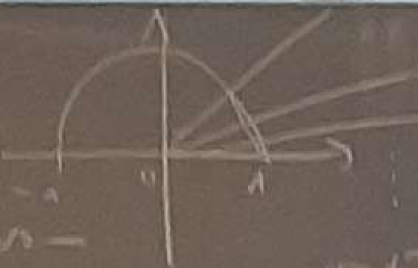
• Si $N \wedge M = 1$,

$\omega_{NM} \in \mathcal{C}$

$\iff \omega_N, \omega_M \in \mathcal{C}$ par rel. de Bézout.

ex : $(N, M) = (2, 3)$

• $\omega_{2^\beta} \in \mathcal{C}$ par construction des bissectrices.



But Si $N = p^\alpha$, montrons : $p \neq 2$

$\omega_N \in \mathcal{C} \iff \begin{cases} \alpha = 1 \\ p \text{ est premier de Fermat.} \end{cases}$

$\boxed{\Rightarrow}$ Si $\omega_N \in \mathcal{C}$, par Wantzel,

$\deg(\omega_N) = \deg(\Phi_N) = \varphi(N) = 2^n$, $n \in \mathbb{N}^*$

$= p^{\alpha-1}(p-1)$.

Ainsi $\boxed{\alpha = 1}$ et $p - 1 = 2^n$ i.e. $\boxed{p = 2^n + 1}$.

$\boxed{\Leftarrow}$ Supposons $p = 2^n + 1$, $n \in \mathbb{N}$, p premier.

Plan 1] Étudier $\mathrm{Aut}(\mathbb{Q}(\omega))$

2] Construire la tour avec ces infos

$\boxed{1}$ Soit $\sigma \in \mathrm{Aut}(\mathbb{Q}(\omega))$.

On a $\omega \in \mu_p$, d'où $\sigma(\omega) \in \mu_p$, $N = p$

i.e. $\sigma(\omega) = \omega^k$, d'où

$f : \mathrm{Aut}(\mathbb{Q}(\omega)) \to (\mathbb{Z}/p\mathbb{Z})^*$

$\sigma \mapsto k = k(\sigma)$.

Montrons que f est un iso de groupes.

(↪) Supposons $f(\sigma) = f(\sigma')$ pour $\sigma, \sigma' \in \mathrm{Aut}(\mathbb{Q}(\omega))$.

Alors $\sigma(\omega) = \omega^{f(\sigma)} = \omega^{f(\sigma')}$

$= \sigma'(\omega)$ et ω engendre $\mathbb{Q}(\omega)$

en tant que $\mathbb{Q}$-algèbre, d'où $\sigma = \sigma'$.

(↠) Soit $k \in (\mathbb{Z}/p\mathbb{Z})^*$.

On a $\mathbb{Q}(\omega) \xrightarrow[\psi_1]{\sim} \mathbb{Q}[X]/\Phi_p \xleftarrow[\psi_k]{\sim} \mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$

$\omega \longmapsto \bar{X} \longleftarrow \omega^k$

$\sigma_k : \omega \longmapsto \omega^k$

$\psi_k^{-1} \circ \psi_1$

donc $\sigma_k(\omega) = \omega^k$, i.e. $f(\sigma_k) = k$.

f est un morphisme.

Si $\sigma(\omega) = \omega^{k_1}$ et $\sigma'(\omega) = \omega^{k_2}$,

$\sigma\sigma'(\omega) = \sigma(\omega^{k_2}) = \sigma(\omega)^{k_2} = (\omega^{k_1})^{k_2} = \omega^{k_1 k_2}$

d'où $f(\sigma\sigma') = k_1 k_2 = f(\sigma) f(\sigma')$.

Ainsi, $f : \mathrm{Aut}\,\mathbb{Q}(\omega) \simeq (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

$= \mathbb{Z}/2^n\mathbb{Z}$

cyclique

Fixons ρ un générateur de $\mathrm{Aut}(\mathbb{Q}(\omega))$.

$\boxed{2}$ On a $\mathcal{B} = (\omega, \rho(\omega), \dots, \rho^{2^n - 1}(\omega))$ base de $\mathbb{Q}(\omega)$,

car $\{\rho^k(\omega), k \in \mathbb{N}\} = \{\sigma(\omega), \sigma\}$

$= \{\omega^k\}$.

Soit $z \in \mathbb{Q}(\omega)$, $z = (z_0, z_1, \dots, z_{2^n - 1})$.

Alors $\rho(z) = (z_1, z_2, \dots, z_{2^n - 1}, z_0)$.

Donc ρ agit par permutations circulaires.

Posons pour $i \in [\![0, 2^n - 1]\!]$,

$$K_i = \{z \in \mathbb{Q}(\omega) \mid \rho^{2^i}(z) = z\},$$

extension de $\mathbb{Q}$ car ρ^{2^i} est un morph d'algèbres.

Ainsi, $z \in K_i \iff z_k$ sont 2^i-périodiques

---

d'où :

$K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = \mathbb{Q}(\omega)$.

car $\rho^{2^n} = \mathrm{id}$.

De plus, $K_0 = \mathbb{Q}$, car

si $z = (z_0, \dots, z_0)$,

$z = z_0 \underbrace{(1 + \dots + \omega^{p-1})}_{=1} = z_0 \in \mathbb{Q}$

Enfin, $\dim(K_i) = 2^i$ d'où $[K_{i+1} : K_i] = \frac{2^{i+1}}{2^i} = 2$.

(théorème de la base télé.)

Par le théorème de Wantzel, $\omega \in \mathcal{C}$.

Applications

* △, □, ⬠, ⬡ sont constructibles.
* L'heptagone régulier n'est pas constructible à la règle et au compas !

Rappel (Wantzel) $z \in \mathcal{C}$

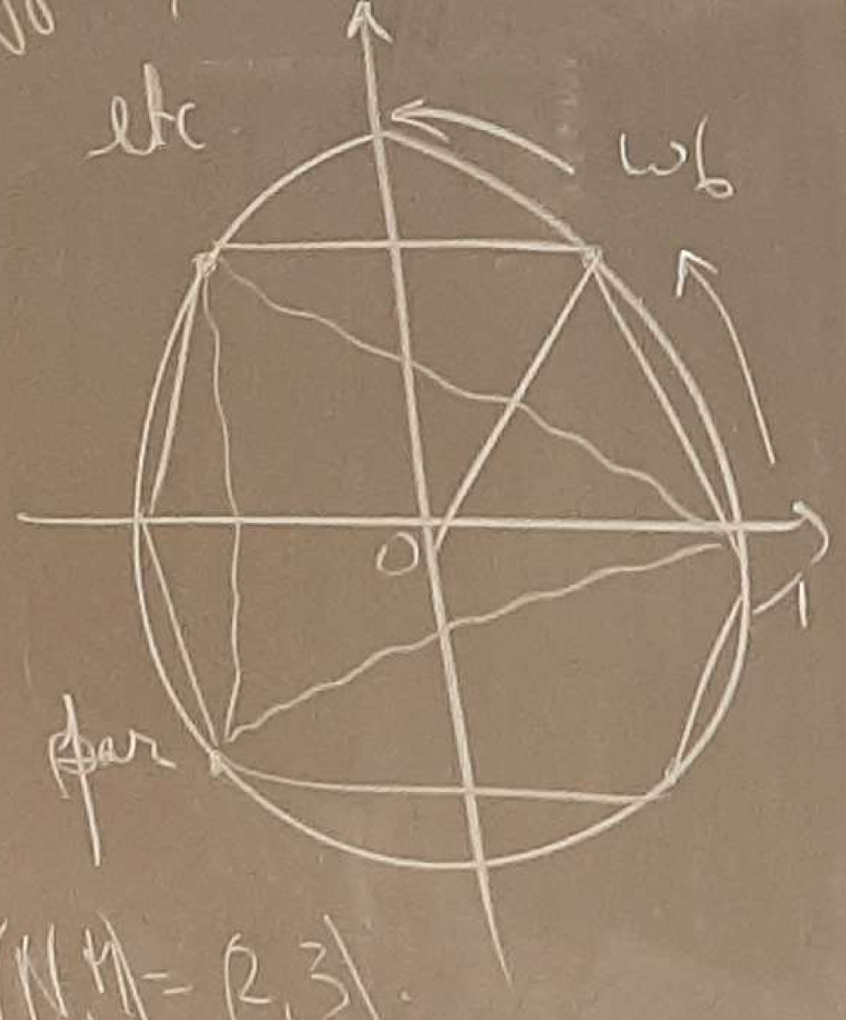
$\iff z \in K_i / K_{i-1} / \dots / K_1 / K_0 = \mathbb{Q}$
avec $[K_i : K_{i-1}] = 2$.

Th. (Gauß-Wantzel) Le polygone à N côtés est constructible ssi

$$N = 2^\beta p_1 \dots p_m$$

où les p_i sont des nombres premiers de Fermat 2 à 2 distincts.

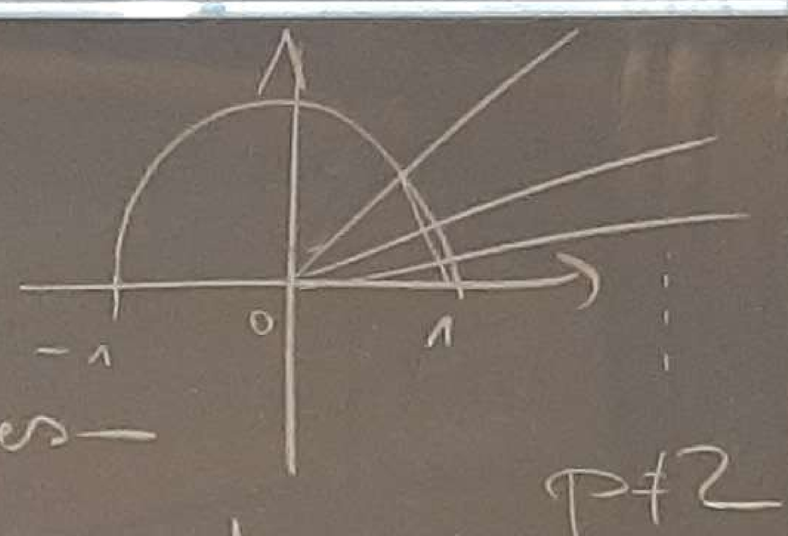
Rq * Construire le polygone, c'est construire $\omega = e^{2\pi/N}$ etc



* Si $N \wedge M = 1$, $\omega_{NM} \in \mathcal{C}$

$\iff \omega_N, \omega_M \in \mathcal{C}$ par rel. de Bézout, ex $(N, M) = (2, 3)$.

* $\omega_{2^\beta} \in \mathcal{C}$ par construct° des bissectrices.



$p \neq 2$

But Si $N = p^\alpha$, montrons :

$\omega_N \in \mathcal{C} \iff \begin{cases} \alpha = 1 \\ p \text{ est premier de Fermat.} \end{cases}$

$\Rightarrow$ Si $\omega_N \in \mathcal{C}$, par Wantzel,

$\deg(\omega_N) = \deg(\Phi_N) = \varphi(N) = 2^m$, $m \in \mathbb{N}^*$

$= p^{\alpha-1}(p-1)$.

Ainsi $\boxed{\alpha = 1}$ et $p - 1 = 2^m$ i.e. $\boxed{p = 2^m + 1}$.

$\Leftarrow$ Supposons $p = 2^m + 1$, $m \in \mathbb{N}$, p premier

Plan 1] Étudier $Aut(\mathbb{Q}(\omega))$

2] Construire la tour avec ces infos

1] Soit $\sigma \in Aut(\mathbb{Q}(\omega))$.

On a $\omega \in \mu_p$, d'où $\sigma(\omega) \in \mu_p$,

$N = p$ i.e. $\sigma(\omega) = \omega^k$, d'où :

$$f : Aut(\mathbb{Q}(\omega)) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$
$$\omega \longmapsto k = k(\omega).$$

Montrons que f est un iso de groupes.

($\hookrightarrow$) Supposons $f(\sigma) = f(\sigma')$ pour $\sigma, \sigma' \in Aut(\mathbb{Q}(\omega))$.

Alors $\sigma(\omega) = \omega^{f(\sigma)} = \omega^{f(\sigma')}$
$= \sigma'(\omega)$ et ω engendre $\mathbb{Q}(\omega)$ en tant que $\mathbb{Q}$-algèbre, d'où $\sigma = \sigma'$.

($\longrightarrow$) S…

On a $\mathbb{Q}(\omega) \xrightarrow{\sim}$ …

$\omega \mapsto$ …

$\tau_k : \omega \mapsto$ …

donc $\tau_k(\omega) = \omega^k$, …

f est un morphisme …

Si $\sigma(\omega) = \omega^{k}$ et $\sigma'(\omega)$ …

$\sigma \circ \sigma'(\omega) = \sigma(\omega^{k'}) =$ …

d'où $f(\sigma\sigma') = kk'$ …

Ainsi, $f : Aut(\mathbb{Q}($…

Fixons ρ un géné…

$\mathrm{Aut}(\mathbb{Q}(\omega))$
la tour avec

$(\mathbb{Q}(\omega))$.
$\sigma(\omega) \in \mu_p$,
$) = \omega^k$, d'où
$\longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$
$\mapsto k = k(\omega)$.
est un iso de groupes.
pposons $f(\sigma) = f(\sigma')$
$\mathrm{Aut}(\mathbb{Q}(\omega))$.
$\omega) = \omega^{f(\sigma)} = \omega^{f(\sigma')}$
(ω) et ω engendre $\mathbb{Q}(\omega)$
$\mathbb{Q}$-algèbre, d'où $\sigma = \sigma'$.

$\Longrightarrow$ Soit $k \in (\mathbb{Z}/p\mathbb{Z})^*$.

On a $\mathbb{Q}(\omega) \xrightarrow[\psi_1]{\sim} \mathbb{Q}[X]/\Phi_p \xleftarrow[\psi_2]{\sim} \mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$

$\omega \longmapsto \overline{X} \longleftarrow \omega^k$

$\sigma_k : \omega \longmapsto \omega^k$, $\sigma_k = \psi_2^{-1} \circ \psi_1$

donc $\sigma_k(\omega) = \omega^k$, i.e. $f(\sigma_k) = k$.

f est un morphisme.

Si $\sigma(\omega) = \omega^{k_1}$ et $\sigma'(\omega) = \omega^{k_2}$,

$\sigma\sigma'(\omega) = \sigma(\omega^{k_2}) = \sigma(\omega)^{k_2} = (\omega^{k_1})^{k_2} = \omega^{k_1 k_2}$

d'où $f(\sigma\sigma') = k_1 k_2 = f(\sigma) f(\sigma')$.

Ainsi, $f : \mathrm{Aut}\,\mathbb{Q}(\omega) \simeq (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/2^n\mathbb{Z}$.
cyclique

Fixons ρ un générateur de $\mathrm{Aut}(\mathbb{Q}(\omega))$.

---

2) On a $\mathcal{B} = (\omega, \rho(\omega), \dots, \rho^{p-2}(\omega) = \rho^{2^n - 1}(\omega))$ base de $\mathbb{Q}(\omega)$,

car $\{\rho^k(\omega), k \in \mathbb{N}\} = \{\sigma(\omega), \sigma\} = \{\omega^k\}$.

Soit $z \in \mathbb{Q}(\omega)$, $z = (z_0, z_1, \dots, z_{2^n - 1})$.

Alors $\rho(z) = (z_1, z_2, \dots, z_{2^n-1}, z_0)$.

Donc ρ agit par permutations circulaires.

Posons pour $i \in [\![0, 2^n - 1]\!]$,

$$K_i = \{z \in \mathbb{Q}(\omega) \mid \rho^{2^i}(z) = z\},$$

extension de $\mathbb{Q}$ car ρ^{2^i} est un morph d'algèbres.

Alors, $z \in K_i \iff z_*$ sont 2^i-périodiques

---

d'où

$$K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = \mathbb{Q}(\omega),$$

car $\rho^{2^n} = \mathrm{id}$.

De plus, $K_0 = \mathbb{Q}$, car

si $z = (z_0, \dots, z_0)$,

$z = z_0 \underbrace{(1 + \dots + \omega^{p-1})}_{=1} = z_0 \in \mathbb{Q}$

Enfin, $\dim(K_i) = 2^i$ d'où $[K_{i+1} : K_i] = \frac{2^{i+1}}{2^i} = 2$.
(théorème de la base télé)

Par le théorème de Wantzel, $\omega \in \mathcal{C}$.

<u>Applications</u>

* △, □, ⬠, ⬡ sont constructibles.
* L'heptagone régulier n'est pas constructible à la règle et au compas !