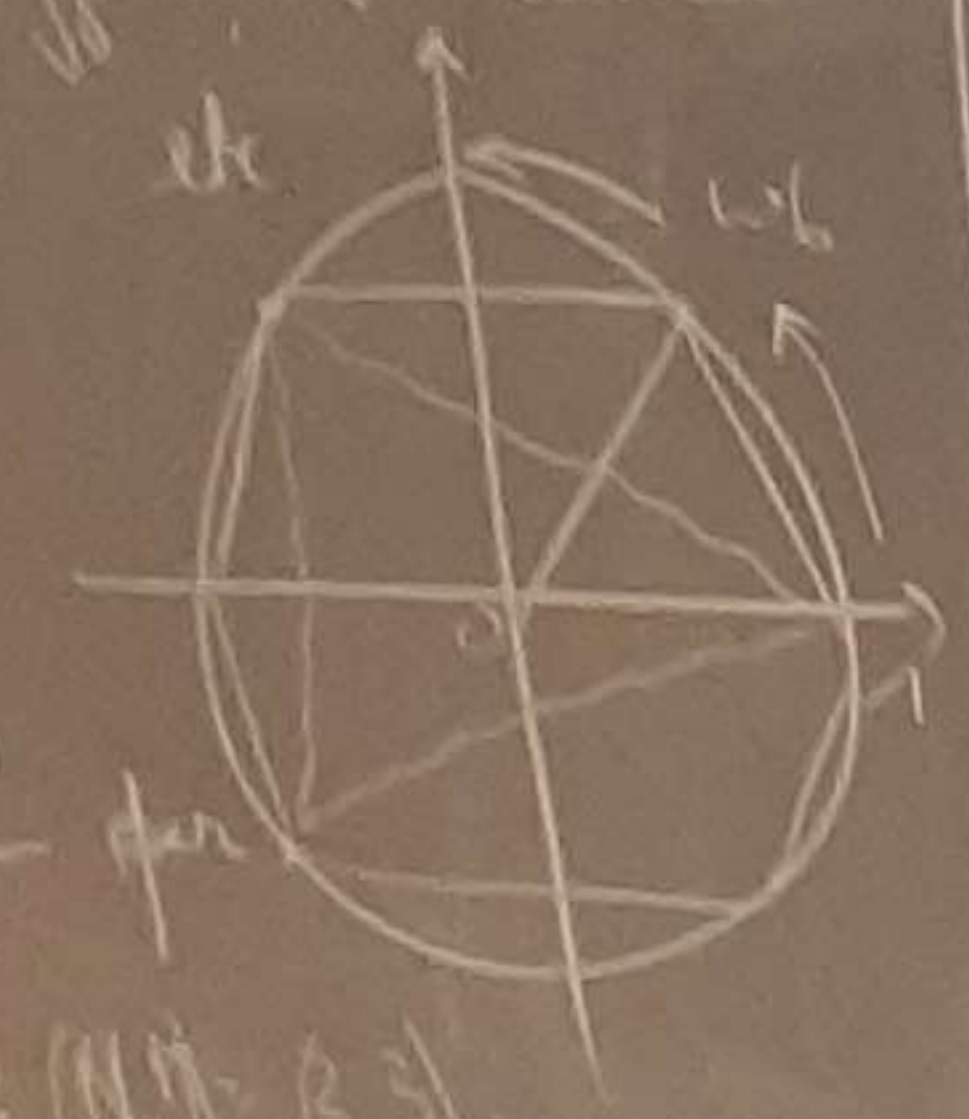


Rappel (Wahlzeit) $g \in \mathbb{C}$
 $\Rightarrow g \in K_1/K_0 = 1, K_1/K_0 = \mathbb{Q}$
 avec $[K_1:K_0] = 2$.

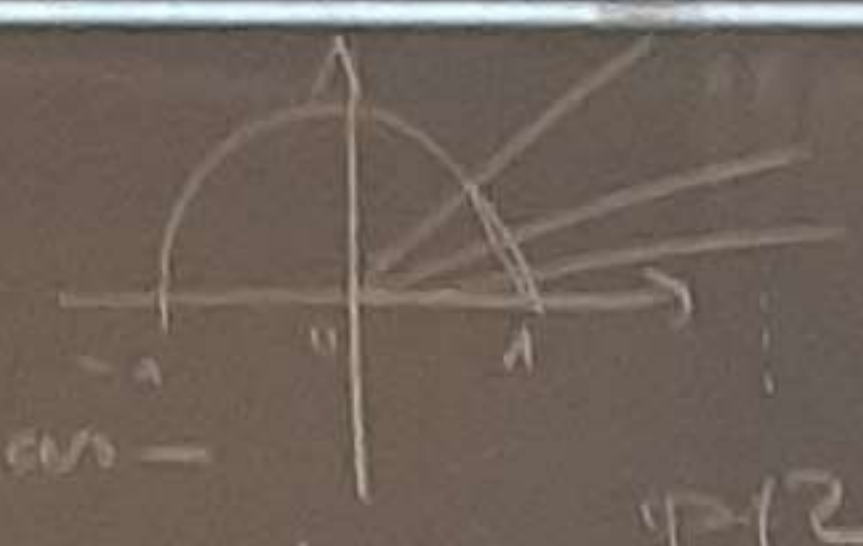
\mathcal{H} (Goup d'ordre) Le polygone N
 est constructible si
 $N = 2^m \cdot p_1 \cdot \dots \cdot p_r$
 où les p_i sont des nombres premiers de Fermat.

Rq : L'axe du polygone est vertical
 $\omega = e^{2\pi i/n}$ et



* Si $N \equiv 1 \pmod{4}$
 $\omega \in \mathbb{C}$
 $\Rightarrow \omega, \omega^3 \in \mathbb{C}$ pour
 tel de Fermat $(2^{2^m} + 1)$.

* $\omega \in \mathbb{C}$
 par construction
 des abscisses -



But : Si $N = p^a$, montrons
 $\omega_N \in \mathbb{C} \Leftrightarrow \frac{1}{p}$ est puissance de 2.

\Rightarrow Si $\omega_N \in \mathbb{C}$, par abscisse,
 $\deg(\omega_N) = \deg(\Phi_N) = \varphi(N) = 2^m$, où $\omega_N^k = \omega_N^{k \cdot 2^m}$
 $\Rightarrow \varphi(N) = 2^m \cdot (p-1)$
 $\Rightarrow \frac{1}{p} \in \mathbb{Z}$ et $p-1 = 2^m$ i.e.
 $p = 2^m + 1$.

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

Plan 1) Étudier $\text{Aut}(\mathbb{Q}(\omega))$
 2) Construire la tour avec
 ces info.

1) Soit $\sigma \in \text{Aut}(\mathbb{Q}(\omega))$.
 On a $\omega \in \mathbb{Q}(\omega)$, donc $\sigma(\omega) = \omega^k$
 i.e. $\sigma(\omega) = \omega^k$, donc
 $f: \text{Aut}(\mathbb{Q}(\omega)) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$
 $\omega \mapsto k = h(\sigma)$.

Montrons que f est un iso de groupes.
 Soit $\sigma, \sigma' \in \text{Aut}(\mathbb{Q}(\omega))$.
 Alors $\sigma(\omega) = \omega^{h(\sigma)} = \omega^{f(\sigma)}$
 $= \sigma'(\omega)$ et ω engende $\mathbb{Q}(\omega)$
 ce qui implique que $\sigma = \sigma'$.

\Rightarrow Soit $f \in (\mathbb{Z}/p\mathbb{Z})^\times$.
 On a $\mathbb{Q}(\omega) \xrightarrow{\sim} \mathbb{Q}(\omega^k) \xrightarrow{\sim} \mathbb{Q}(\omega^{k^2}) \dots$
 $\omega \mapsto \omega^k \mapsto \omega^{k^2} \dots$
 donc $\sigma_k(\omega) = \omega^{k^2}$, i.e. $f(\sigma_k) = k^2$.

f est un isomorphisme.
 Δ $\sigma(\omega) = \omega^k$ et $\sigma'(\omega) = \omega^{k^2}$,
 $\sigma\sigma'(\omega) = \sigma(\omega^{k^2}) = \omega^{k^2 k} = \omega^{k^3}$
 donc $f(\sigma\sigma') = k^3 = f(\sigma)f(\sigma')$.
 Ainsi, $f: \text{Aut}(\mathbb{Q}(\omega)) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$
 Fixons p un générateur de $\text{Aut}(\mathbb{Q}(\omega))$.

2) On a $B = (\omega, \omega^2, \dots, \omega^{p-1})$ d'où
 base de $\mathbb{Q}(\omega)$,
 car $\{p^k(\omega), k \in \mathbb{N}\} = \{\omega^k, p^k\}$
 $= \{\omega^k\}$.

Soit $z \in \mathbb{Q}(\omega)$, $z = (z_0, z_1, \dots, z_{p-1})$
 Alors $p(z) = (z_0, z_1, \dots, z_{p-1})$
 Dans p agit par permutation circulaire.
 Posons pour $i \in \{0, 2^m - 1\}$
 $K_i = \{z \in \mathbb{Q}(\omega) \mid p^{2^i}(z) = z\}$,
 extension de \mathbb{Q} car p^2 est un corps
 d'algèbre.
 Alors, $z \in K_i \Leftrightarrow z$ est 2^i -périodique.

$K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = \mathbb{Q}(\omega)$
 car $p^0 = \text{id}$.

De plus, $K_0 = \mathbb{Q}$, car
 $z = (z_0, \dots, z_0)$,
 $z = z_0 \frac{1 + \omega + \dots + \omega^{p-1}}{p} = z_0 \cdot \frac{0}{p} = 0$
 (théorème de Fermat)
 Par le théorème de Watzel, $\omega \in \mathbb{C}$.

Applications
 * $\Delta, \square, \text{pentagone}, \text{hexagone}$ sont
 constructibles.
 * L'heptagone régulier n'est pas
 constructible à la règle et au
 compas!

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

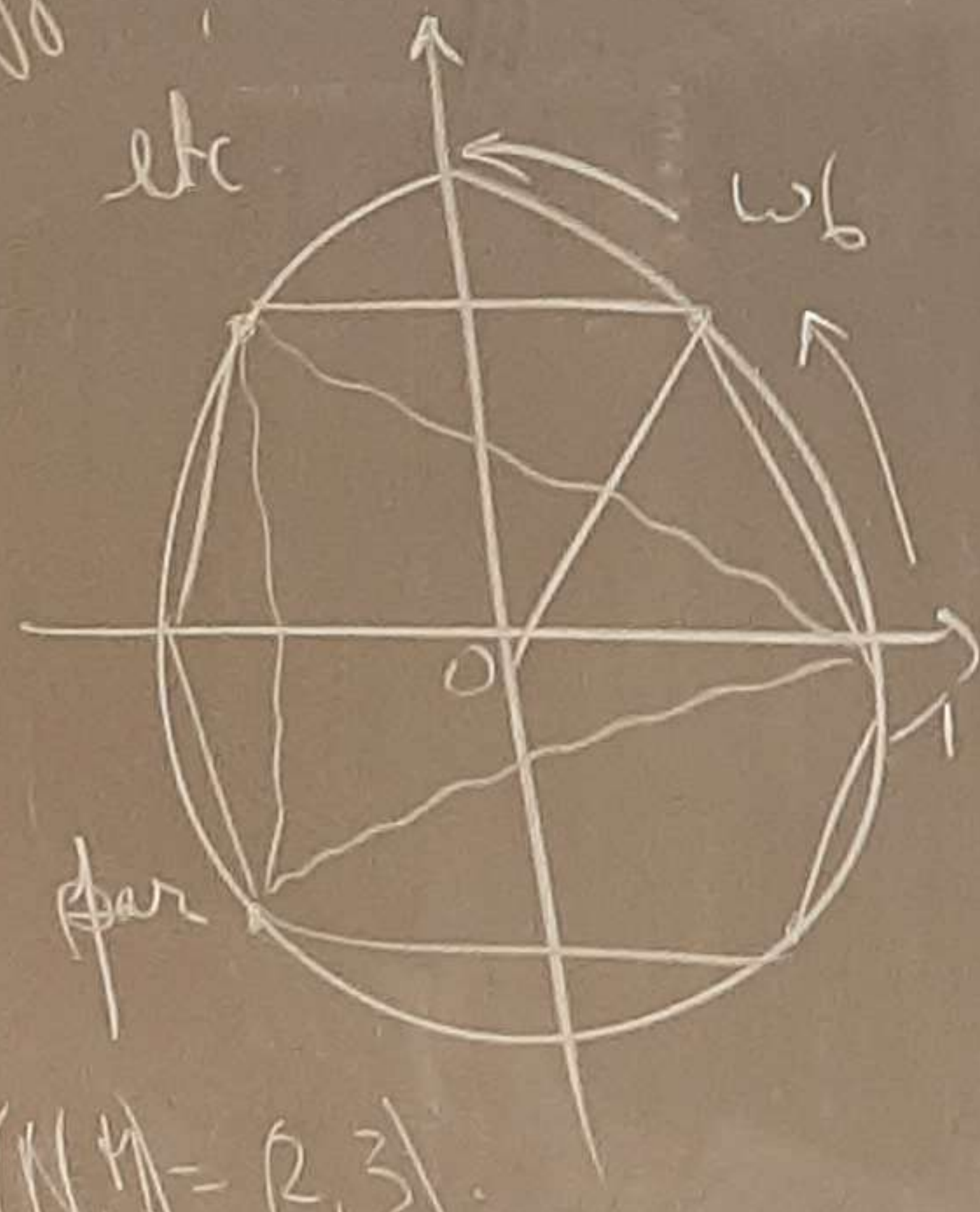
$\Leftrightarrow z \in K_n / K_{n-1} / \dots / K_1 / K_0 = \mathbb{Q}$
avec $[K_i, K_{i-1}] = 2$.

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

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

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

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



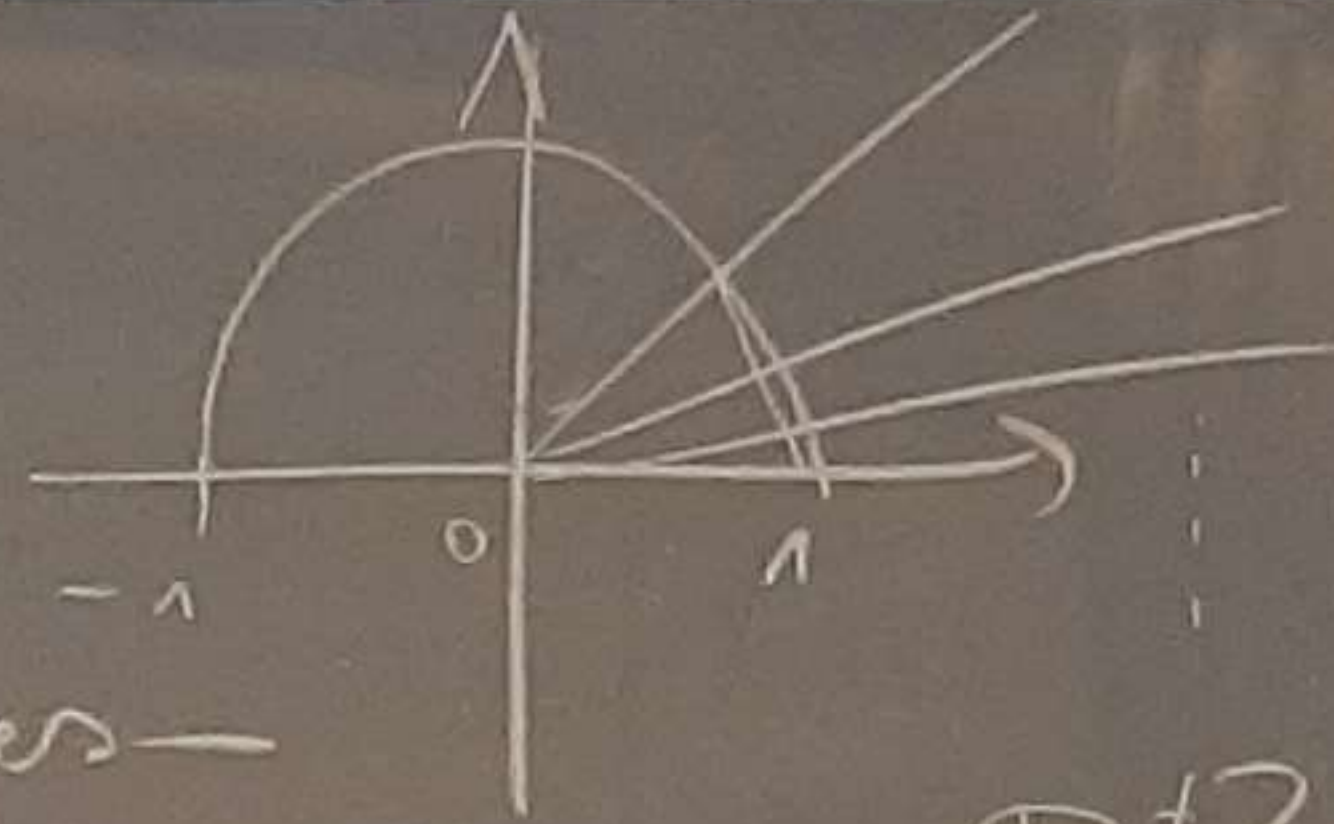
* Si $N \wedge m = 1$,

$$\omega_{N/n} \in \mathbb{C}$$

$\Rightarrow \omega_n, \omega_m \in \mathbb{C}$ par

rel. de Bézout, car $(N, m) = (2, 3)$.

* $\omega_{2^k} \in \mathbb{C}$
par construction des bissectrices



But Si $N = p^\alpha$, montrons $\omega_N \in \mathbb{C} \Leftrightarrow \alpha = 1$
 p est premier de Fermat.

\Rightarrow Si $\omega_N \in \mathbb{C}$, par Wantzel,
 $\deg(\omega_N) = \deg(\mathbb{Q}(\omega_N)) = \varphi(N) = 2^m, m \in \mathbb{N}^*$
 $= p^{\alpha-1}(p-1)$.

Alors $\boxed{\alpha=1}$ 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 $\text{Aut}(\mathbb{Q}(\omega))$
2] Construire la tour avec ces infos

1] Soit $\sigma \in \text{Aut}(\mathbb{Q}(\omega))$.
On a $\omega \in \mu_p$, d'où $\sigma(\omega) \in \mu_p$,
i.e. $\sigma(\omega) = \omega^k$, d'où

$$f: \text{Aut}(\mathbb{Q}(\omega)) \rightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$

$$\omega \mapsto k = k(\omega)$$

Montrons que f est un iso de groupes.

\hookrightarrow Supposons $f(\sigma) = f(\sigma')$

pour $\sigma, \sigma' \in \text{Aut}(\mathbb{Q}(\omega))$.

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 $\sigma = \sigma'$.

\rightarrow Soit

On a $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$

d'où $\sigma(\omega) = \omega^k$

d'où $\sigma(\omega) = \omega^k$

f est un isomorphisme.

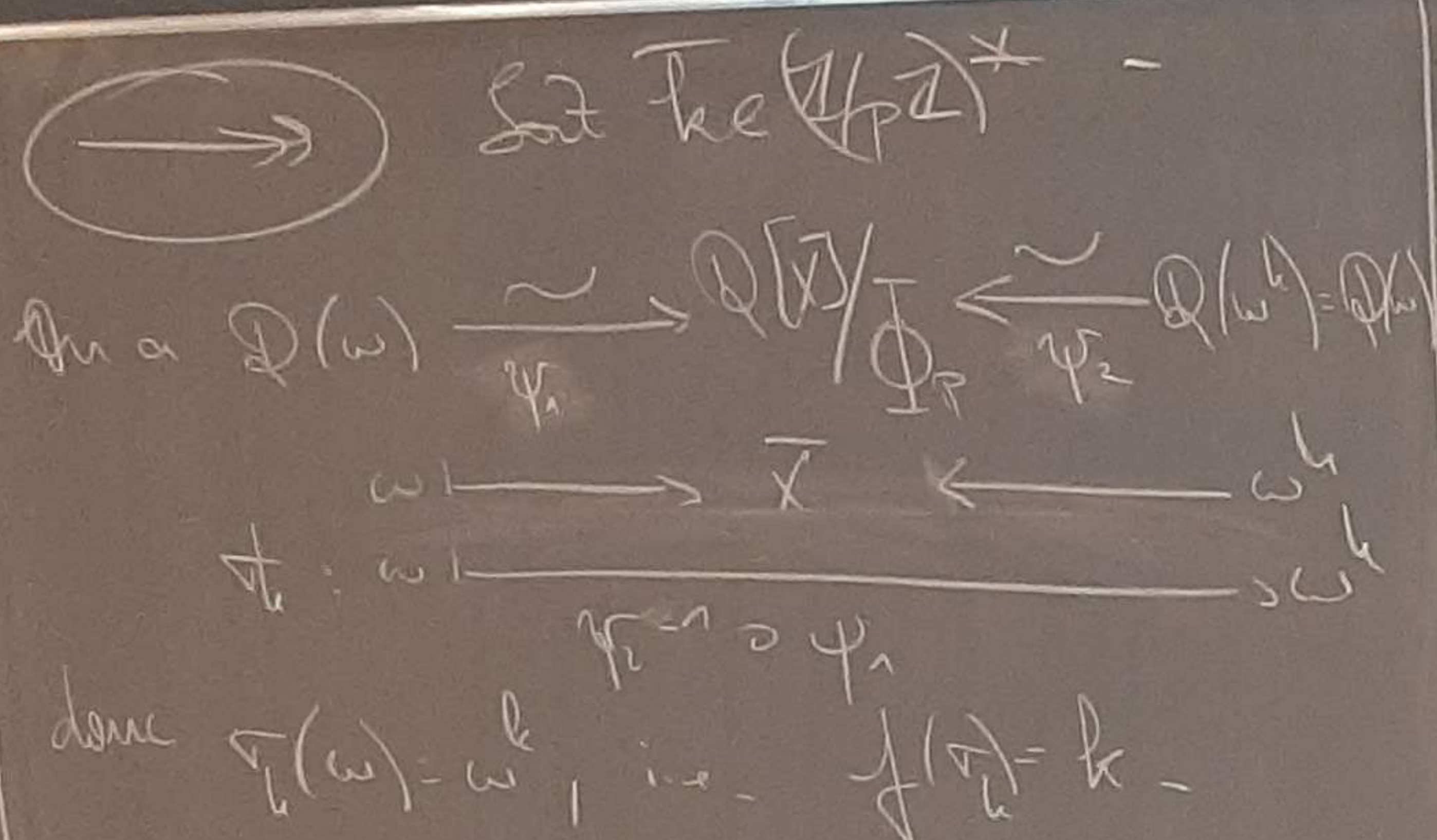
Si $\sigma(\omega) = \omega^k$ et $\sigma'(\omega) = \omega^l$

d'où $f(\sigma\sigma') = f(\sigma)f(\sigma')$

Alors, $f: \text{Aut}(\mathbb{Q}(\omega)) \rightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$

Fixons p un générateur

Aut(Q(w))
 la tour avec
 (Q(w))
 $\sigma(w) \in \mu_p$
 $\sigma^k(w)$
 $\mathbb{Z}/p\mathbb{Z}$
 $\sigma^k(w)$
 et un no de jauge
 opérons $f(\sigma) = f(\sigma')$
 Aut(Q(w))
 $w = \omega^{1/p} = \omega^{1/p^2}$
 w et ω engendrent Q(w)
 Q-algèbre, donc $\sigma = \sigma'$



f est un morphisme.

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

Alors, $f: \text{Aut}(Q(w)) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$
 cyclique

Fixons ρ un générateur de $\text{Aut}(Q(w))$

2) On a $B = (w, p(w), \dots, p^{2^m-1}(w))$
 base de $Q(w)$,
 Car $\{p^k(w), k \in \mathbb{N}\} = \{\sigma^k(w), \sigma^k\} = \{\omega^{k^2}\}$

Soit $z \in Q(w)$, $z = (z_0, z_1, \dots, z_{2^m-1})$
 Alors $p(z) = (z_1, z_2, \dots, z_{2^m-1}, z_0)$

Donc p agit par permutation circulaire.

Prenons pour $i \in \{0, 2^m-1\}$
 $K_i = \{z \in Q(w) \mid p^{2^i}(z) = z\}$,
 extension de \mathbb{Q} car p^{2^i} est un morphisme d'algèbres.

Alors, $z \in K_i \Leftrightarrow z_{k+2^i} = z_k$ sont 2^i -périodiques

d'où $K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = Q(w)$,
 car $p^{2^m} = \text{id}$.

De plus, $K_0 = \mathbb{Q}$, car
 $z = (z_0, \dots, z_0)$,
 $z = z_0 \underbrace{(1 + \dots + \omega^{2^m-1})}_{=1} = z_0 \in \mathbb{Q}$

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

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

Applications

* $\Delta, \square, \text{pentagone}, \text{hexagone}$ sont constructibles.

* L'heptagone régulier n'est pas constructible à la règle et au compas!