Leçons:
102, 125, 127, 148, 131

Lemme:
Soit $p \in P$. On a l'isomorphisme suivant:
$\psi : Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) \xrightarrow{\sim} \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$, en particulier $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ est cyclique.
$g_k : w \mapsto w^k \longmapsto \bar{k}$

Théorème:
Si $p (= 2^{2^\beta}+1)$ est un nombre premier de Fermat alors $\frac{2\pi}{p^\alpha}$ est constructible.

V3

Référence:
Carrega; théorie des corps: règle et compas

Pour le lemme, [CAR] p. 147

Posons $G := Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ et $w := \zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$

- Pour $g \in G$, mq $g(w)$ est encore une racine de ϕ_p

$$\phi_p(g(w)) = \sum_{i=0}^{p-1} g(w)^i$$
$$= g\left(\sum_{i=0}^{p-1} w^i\right)$$
$$= g\underbrace{(\phi_p(w))}_{=0} = 0$$

- Mq ψ est bien un isomorphisme de groupe

Puisque $g(w)$ est une racine de ϕ_p, w est une racine primitive donc il existe $k \in \{1, \dots, p-1\}$ tq $g(w) = w^k$. Puisque $B = \{w, \dots, w^{p-2}\}$ est une base de $\mathbb{Q}(w)$ dans $\mathbb{Q}$ g est entièrement déterminée.

ψ est clairement un morphisme. L'injectivité provient de l'unicité de l'écriture dans B.

La surjectivité: Pour $\bar{k} \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$, $g(w) = w^{\bar{k}}$ convient, $\psi(g) = \bar{k}$

Finalement, ψ est bien un isomorphisme de groupe.

- On a bien que G est cyclique d'ordre $p-1$

car $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$

Pour le théorème,

Le but va être de mq $\mathbb{Q}(w)$ est 2-

• Construisons une bonne tour de corps 5min

Posons $n = 2^\beta$

→ Créons une suite de grp d'ordre $p-1 = 2^n$

D'après le lemme G est cyclique, notons g un générateur de G ($G = (g)$)

Les sous grp de G sont les $\left(g^{\frac{2^n}{d}}\right)$ où $d | 2^n$, donc les sous groupes de G sont les

$$G_i = (g^{2^i}) \text{ où } i \in \{0, \dots, n\} \text{ et } o(G_i) = 2^{n-i}.$$

De telle sorte que

$$\{1_G\} = G_n \subset \dots \subset G_0 = G$$

→ Associons à ces groupes un corps

Notons $K := \mathbb{Q}(w)$ et posons $K_i := \{z \in K \mid g^{2^i}(z) = z\}$

Ces K_i sont bien des corps (cela vient du fait que g^{2^i} est un automorphisme).

De plus $K_0 \subset \dots \subset K_n = K$ (car $g^{2^{i+1}} = (g^{2^i})^2 = g^{2^i} \circ g^{2^i}$)

• Mq cette tour de corps convient

→ Mq $K_0 = \mathbb{Q}$ 3min

. On a évidemment que $\mathbb{Q} \subset K_0$

. Réciproquement, mq $K_0 \subset \mathbb{Q}$

On sait que $[K : \mathbb{Q}] = \varphi(p) = p-1$ donc $B = \{w, \dots, w^{p-1}\}$ est une base de K. D'après le lemme on a :

$$B = \{w, g(w), \dots, g^{p-2}(w)\}$$

Prenons $z \in K_0 (\subset K)$ et écrivons le dans cette base :

$$z = \lambda_0 w + \dots + \lambda_{p-2} g^{p-2}(w)$$

Donc

$$g(z) = \lambda_0 g(w) + \dots + \lambda_{p-2} \underbrace{g^{p-1}(w)}_{= w \text{ car } o(g) = p-1}$$

On en déduit que $\lambda_0 = \dots = \lambda_{p-2}$, donc

$$\begin{aligned} z &= \lambda_0 \left(g(w) + \dots + g^{p-2}(w) + w \right) \\ &= \lambda_0 \underbrace{\left(w + \dots + w^{p-1} \right)}_{=-1} \\ &= -\lambda_0 \end{aligned}$$

| w racine de $\phi_p = 1 + \dots + X^{p-1}$

Donc $z \in \mathbb{Q}$.

→ Mq $K_i \subsetneq K_{i+1}$ 3min 30

Montrons déjà que $K_0 \subsetneq K_1$:

Il nous faut un z tq $g^2(z) = z$ et $g(z) \neq z$

Prenons

$$\begin{aligned} z &= w + g^2(w) + g^{2\times 2}(w) + \dots + g^{2\times(2^{n-1}-1)}(w) \\ &= w + g^2(w) + \dots + g^{2^n-2}(w) \end{aligned}$$

Et

$$g^2(z) = g^2(w) + \dots + \underbrace{g^{2^n}(w)}_{= g^{p-1}(w) = w}$$

$$= z$$

Et

$$g(z) = g(w) + g^3(w) + \dots + g^{2^n-1}(w) \neq z$$ par unicité de l'écriture dans B

Pour $K_i \subsetneq K_{i+1}$:

$$z = w + g^{2^{i+1}}(w) + g^{2^{i+1}\times 2}(w) + \dots + g^{2^{i+1}\times(2^{n-(i+1)}-1)}(w)$$

convient.

- Concluons 2min 20

Par théorème de la base telescopique on a :

$$\underbrace{[K : K_0]}_{= 2^n} = \underbrace{[K : K_{n-1}] \dots [K_1 : K_0]}_{n \text{ éléments} \neq \text{de } 1 \text{ car } K_i \subsetneq K_{i+1}}$$

Donc $[K_{i+1} : K_i] = 2$

Ainsi par Wantzel w est constructible donc $\cos\frac{2\pi}{p}$ est constructible et finalement $\frac{2\pi}{p}$ est constructible.

□

Commentaires:

- de manière générale on a $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$
- Savoir démontrer l'autre sens
- Savoir démontrer Wantzel
- Savoir pq Gauss a reussi a construire 17 côté (car il a trouvé un générateur de $\left(\frac{\mathbb{Z}}{17\mathbb{Z}}\right)^\times$
- Savoir construire cfly n-gones.