Ref : MG 2019

DEV

Racines de l'unité dans $\mathbb{Q}(\xi)$

Énoncé : Soit $n \in \mathbb{N}^*$, et $\xi := e^{\frac{2i\pi}{n}}$. Les racines de l'unité contenues dans $\mathbb{Q}(\xi)$ sont exactement les $\pm \xi^k$, $k \in [\![0;n-1]\!]$. Il y en a n si n est pair, $2n$ sinon.

D/

Lemme : L'indicatrice d'Euler diverge : $\varphi(n) \xrightarrow[n\to+\infty]{} +\infty$. Plus précisément, $\varphi(n) \geq \sqrt{n}$ pour $n \neq 2, 6$.

D/ • Si p est premier impair, $\varphi(p) = p-1 \geq \sqrt{p}$ car les racines de $X^2 - 3X + 1$ sont $\frac{3 \pm \sqrt{5}}{2}$ et $\frac{3+\sqrt{5}}{2} < \frac{3+3}{2} \leq 3 \leq p$.

• Si p est premier et $\alpha \geq 2$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1) \geq p^{\alpha-1} \geq p^{\alpha/2}$ car $\alpha - 1 \geq \frac{\alpha}{2}$.

• On écrit $n = 2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $p_1 < \dots < p_r$ premiers impairs, $r \geq 1$.

$$\varphi(n) = \varphi(2^\alpha)\varphi(p_1^{\beta_1})\dots\varphi(p_r^{\beta_r}).$$ Si $\alpha \geq 2$, nous pouvons conclure.

Sinon $\alpha = 1$. Si il existe i avec $\beta_i \geq 2$, $\varphi(p_i^{\beta_i}) = p_i^{\beta_i - 1}(p_i - 1) \geq 2 p_i^{\beta_i - 1} \geq 2 p_i^{\beta_i/2} \geq \sqrt{2} p_i^{\beta_i/2}$

donc $\varphi(n) \geq p_1^{\beta_1/2} \dots (\sqrt{2} p_i^{\beta_i/2}) \dots p_r^{\beta_r/2} = \sqrt{n}$.

Sinon $n = 2 p_1 \dots p_r$. Si il existe i avec $p_i \geq 5$, alors $p_i - 1 \geq \sqrt{2 p_i}$ car le polynôme $X^2 - 4X + 1$ a pour racines $2 \pm \sqrt{3}$, et $2 + \sqrt{3} < 2 + 2 < 5 \leq p_i$.

Donc $\varphi(n) \geq \sqrt{n}$.

Sinon, $n = 2 \cdot 3 = 6$ et $\varphi(6) = 2$, $\sqrt{6} > 2$. ∎

G est bien un groupe.

• Soit $G := \{ z \in \mathbb{Q}(\xi) \mid \exists k \in \mathbb{N}^* \text{ avec } z^k = 1 \}$. Tout d'abord, G est fini (non vide : $1, \xi \in G$).

En effet, si $z \in G$, comme $\Pi_{z,\mathbb{Q}} = \Phi_K$ pour un certain entier $K \in \mathbb{N}^*$ (z est racine primitive K-ième), on a $[\mathbb{Q}(z):\mathbb{Q}] = \varphi(K) \leq [\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$. Or, il existe un nombre fini de $K \in \mathbb{N}^*$ tels que $\varphi(K) \leq \varphi(n)$, que l'on note $K_1, \dots, K_s$. Ainsi, $G \subset \{\text{racines de } \Phi_{K_1}, \dots, \Phi_{K_s} \text{ dans } \mathbb{C}\}$ donc G est fini.

• <u>G est cyclique</u>. En effet, tout élément de G s'écrit de façon unique sous la forme $e^{i\theta}$ où $\theta \in [0, 2\pi[$.

Soit $w = e^{i\theta_0}$ où $\theta_0 = \min \{ \theta \in]0, 2\pi[\,,\, e^{i\theta} \in G \}$: cela existe car G est fini et $\xi \in G$.

Soit $z = e^{i\theta} \in G \setminus \{1\}$. Il existe un unique $k \in \mathbb{N}^*$ tel que $k\theta_0 \leq \theta < (k+1)\theta_0$.

Alors $zw^{-k} = e^{i(\theta - k\theta_0)} \in G$ et $0 \leq \theta - k\theta_0 < \theta_0$. Par minimalité, $\theta - k\theta_0 = 0$

donc $z = w^k$. Ainsi, <u>$G = \{1, w, w^2, \dots, w^{n-1}\}$ où $n := |G|$.</u>

w est une racine primitive n-ième de l'unité.

• Comme $w \in G \subset \mathbb{Q}(\xi)$ on a $\mathbb{Q}(w) \subset \mathbb{Q}(\xi)$. De plus, $\xi \in G$ donc $w^k = \xi$ pour un certain $k \in \mathbb{N}^*$. Ainsi <u>$\mathbb{Q}(\xi) = \mathbb{Q}(w)$.</u>

De plus, $\xi^n = (w^n)^k = 1$ donc $m \mid n$. Par ailleurs, $z \in G$ si et seulement si $-z \in G$.

En effet, si $z \in \mathbb{Q}(\xi)$ et $z^l = 1$ alors $-z \in \mathbb{Q}(\xi)$ et $(-z)^{2l} = 1$ donc $-z \in G$. Puisque $\begin{array}{l} G \to G \\ z \mapsto -z \end{array}$ n'a pas de point fixe, n est pair. Donc <u>$m \mid n$ et si m est impair, $2m \mid n$.</u>

• Nous écrivons $n = 2^{\alpha} q_1^{\gamma_1} \cdots q_s^{\gamma_s}$ où $\alpha \geq 1$, $\gamma_1, \dots, \gamma_s \in \mathbb{N}^*$ et $q_1, \dots, q_s$ premiers impairs 2 à 2 distincts
$m = 2^{\alpha'} q_1^{\gamma_1'} \cdots q_s^{\gamma_s'}$ $0 \leq \alpha' \leq \alpha$, $\gamma_i' \leq \gamma_i$

On a $[\mathbb{Q}(w) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}]$ donc $\varphi(n) = \varphi(m)$

ie $2^{\alpha-1} q_1^{\gamma_1 - 1} \cdots q_s^{\gamma_s - 1} (q_1 - 1) \cdots (q_s - 1) = \underset{\text{si } m \text{ impair}}{\overset{\text{si } m \text{ pair}}{\begin{matrix} 2^{\alpha'-1} \\ 1 \end{matrix}}} \times \prod_{\substack{i + q \\ \gamma_i' \neq 0}} q_i^{\gamma_i' - 1} (q_i - 1)$

Donc $\dfrac{2^{\alpha - \alpha'}}{2^{\alpha - 1}} \times \prod_{\gamma_i' = 0} q_i^{\gamma_i - 1}(q_i - 1) \times \prod_{\gamma_i' \neq 0} q_i^{\gamma_i - \gamma_i'} = 1$. Comme $q_i^{\gamma_i - 1}(q_i - 1) \geq 2$, on a $\gamma_i' \neq 0 \ \forall i$.

Puis $\gamma_i = \gamma_i' \ \forall i$. Puis $\alpha = \alpha'$ si m pair, $\alpha = 1$ si m impair.

• Puisque G contient $\pm \xi^k$, $0 \leq k \leq m-1$ et que ces éléments sont deux à deux distincts, si m impair

on conclut $\boxed{G = \{ \pm \xi^k \mid 0 \leq k \leq m-1 \}}$. ou $\xi^0, \dots, \xi^{n-1}$ si m pair

Donc $n = m$ si m pair

$n = 2m$ si m impair.