

Théorème de Kronecker-Weber faible.

Recherches: 102, 125, 124

Théorème:

Toute extension galoisienne et contenue dans une extension cyclotomique

Preuve: Soit $d \in \mathbb{Z}^+$ sans facteurs carrés

Montrons qu'il existe $n \in \mathbb{N}^*$ tq $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mu_n)$.

Étape 1: les premiers cas:

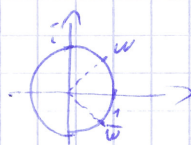
• Si $d = 1$, $\mathbb{Q}(\sqrt{1}) = \mathbb{Q}(\mu_1)$ donc ok!

• Si $d = -1$, $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \mathbb{Q}(\mu_4)$

• Si $d = \pm 2$, $\mathbb{Q}(\sqrt{\pm 2}) \subset \mathbb{Q}(\mu_8)$, en effet:

$$\text{Soit } w = e^{\frac{2\pi i}{8}} = \frac{\sqrt{2}}{2}(1+i)$$

$$\text{On a: } \begin{cases} w + \bar{w} = \sqrt{2} \\ w - \bar{w} = \sqrt{2}i \end{cases}$$



Étape 2: La "première moitié" des cas

Soit $p \in \mathbb{P}$ avec $p \equiv 1 \pmod{4}$.

Montrons que $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\mu_p)$.

Pour cela on cherche à écrire $\sqrt{p}$ comme un élément de $\mathbb{Q}(\mu_p)$ i.e p comme un carré de $\mathbb{Q}(\mu_p)$.

On a, d'abord, $p = \Phi_p(1)$.

On a, d'autre part, pour $\zeta \in \mu_p^*$ on a: $\Phi_p(x) = \prod_{i=1}^{p-1} (x - \zeta^i)$

On, p étant impair, $\zeta^2 \in \mu_p^*$ donc on a:

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i) = \prod_{i=1}^{p-1} (\zeta^i \zeta^{-i} - \zeta^{2i}) = \prod_{i=1}^{p-1} \zeta^i \prod_{i=1}^{p-1} (\zeta^{-i} - \zeta^i)$$

$$\text{On a } S = \prod_{i=1}^{p-1} \zeta^i = \zeta^{\sum_{i=1}^{p-1} i} = \zeta^{\frac{p(p-1)}{2}} = (\zeta^p)^{\frac{p-1}{2}} = 1$$

$$\text{Finalement, } p = \prod_{i=1}^{p-1} (\zeta^{-i} - \zeta^i).$$

Il reste à montrer que le produit ci-dessus peut s'écrire comme un carré de $\mathbb{Q}(\mu_{p^2})$.

On pose $w = \prod_{i=1}^{\frac{p-1}{2}} (z^i - z^{-i})$ et on remarque :

$$w = \prod_{i=1}^{\frac{p-1}{2}} (z^i - z^{-i}) = \prod_{i=1}^{\frac{p-1}{2}} (z^{p-i} - z^{i-p}) = \prod_{l=\frac{p+1}{2}}^{p-1} (z^l - z^{-l})$$

$$= (-1)^{\frac{p-1}{2}} \prod_{l=\frac{p+1}{2}}^{p-1} (z^l - z^{-l})$$

$$= 1 \text{ car } p \equiv 1 \pmod{4}$$

En effet,

p est le produit des $(z^i - z^{-i})$ pour i allant de 1 à $\frac{p-1}{2}$ et w est le produit pour i allant de 1 à $\frac{p-1}{2}$ et le produit pour i allant de $\frac{p-1}{2} + 1$ à $p-1$.

En notant (ou en posant), $p = w^2$.

Étape 3 : Cas général.

Écrivons $d = \pm 2^s \prod_{i=1}^t p_i$ avec $\begin{cases} s = 0 \text{ ou } 1 \\ t \geq 0 \text{ et } p_1, \dots, p_t \in \mathcal{P} \setminus \{2\} \end{cases}$

Quitte à remplacer 1 par -1, on peut poser, pour $i=1, \dots, t$, $q_i = \pm p_i$ tels que : $\forall i, q_i \in \pm \mathcal{P}$ et $q_i \equiv 1 \pmod{4}$ et $d = \pm 2^s \prod_{i=1}^t q_i$.

Par la deuxième étape, pour $i=1, \dots, m$, $\mathbb{Q}(\sqrt{q_i}) \subset \mathbb{Q}(\mu_{q_i+1})$.

$\gamma = S; \alpha \in \mu_m, \beta \in \mu_m$
donc $\alpha \beta \in \mu_m$ d'où, $\mathbb{Q}(\sqrt{q_1 \dots q_t}) \subset \mathbb{Q}(\mu_{q_1+1} \dots \mu_{q_t+1}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t})$
car $(\alpha \beta)^m = (\alpha^m)^t (\beta^m)^t = 1$.

Il reste à traiter le terme $\pm 2^s$:

→ Si $s = 0$, on a : • Si $\pm 1 = 1$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t+1})$
• Si $\pm 1 = -1$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t+1}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t})$
car $d = -1$.

→ Si $s = 1$, $d = \pm 2 \prod_{i=1}^t q_i$ donc $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t+1}) \subset \mathbb{Q}(\mu_{q_1 \dots q_t})$