Développement

Guillaume Pierron

2023-2024

Théorème de Kronecker-Weber, version faible

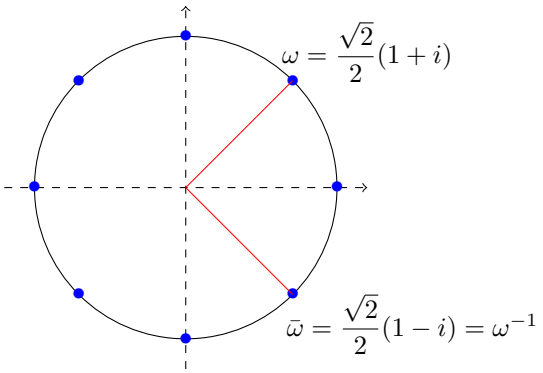
Référence : Livre de Gras, *Algèbre et Arithmétique fondamentales*

Théorème : Toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique de $\mathbb{Q}$

Preuve : Soit $\mathbb{K}$ une extension quadratique de $\mathbb{Q}$, c'est à dire $\mathbb{K} = \mathbb{Q}\left[\sqrt{d}\right]$, avec d un entier non-nul sans facteur carré. Nous noterons μ_n l'ensemble des racines de $X^n - 1$ dans $\mathbb{C}$, qui est un sous-groupe cyclique de $\mathbb{C}^*$ (appelé groupe des racines n-ièmes de l'unité). Nous désignons par μ_n^* l'ensemble des éléments générateurs du groupe μ_n (les racines primitives n-ièmes de l'unité). Nous allons montrer qu'il existe $n \in \mathbb{N}^*$ tel que $\mathbb{K} \subset \mathbb{Q}[\mu_n]$.

1. Cas où $d \in \{1, -1, 2, -2\}$

- Si $d = 1$: $\mathbb{Q}\left[\sqrt{1}\right] = \mathbb{Q}[\mu_1]\,(= \mathbb{Q})$
- Si $d = -1$:
  $\mathbb{Q}\left[\sqrt{-1}\right] = \mathbb{Q}[i] = \mathbb{Q}[\mu_4]$
- Si $d = -2$ ou $d = 2$:
  Soit $\omega = \exp\left(\dfrac{2i\pi}{8}\right)$: $\omega, \bar{\omega} \in \mu_8^*$
  De plus, on a
  $$\begin{cases} (\omega + \bar{\omega})^2 = \left(2\cos\left(\dfrac{\pi}{4}\right)\right)^2 = \left(\sqrt{2}\right)^2 = 2 \\ (\omega - \bar{\omega})^2 = \left(2i\sin\left(\dfrac{\pi}{4}\right)\right)^2 = \left(i\sqrt{2}\right)^2 = -2 \end{cases}$$
  Donc $\begin{cases} \mathbb{Q}\left[\sqrt{-2}\right] \subset \mathbb{Q}[\mu_8] \\ \mathbb{Q}\left[\sqrt{2}\right] \subset \mathbb{Q}[\mu_8] \end{cases}$



2. Cas où $d = p \in \pm\mathcal{P}$, avec $p = 1 \mod 4$

Nous choisissons ici $p \in \mathbb{Z}$ tel que $\begin{cases} |p| \in \mathcal{P} \\ p = 1 \mod 4 \end{cases}$

Remarque : cela revient à dire que $p = (-1)^{\frac{q-1}{2}} q$, avec $q \in \mathcal{P}$

Nous voulons montrer que $\mathbb{Q}\left[\sqrt{p}\right] \subset \mathbb{Q}[\mu_p]$.

Le p-ième polynôme cyclotomique est $\Phi_p(X) = \prod_{\xi \in \mu_p^*} (X - \xi)$.

C'est intéressant car on verra dans la suite que $\Phi_p(1) = p$, ce qui permet d'écrire p comme un produit d'éléments de $\mathbb{Q}[\mu_p]$.

Voyons pourquoi $\Phi_p(1) = p$. On sait que

$$\begin{aligned} X^p - 1 &= \prod_{d|p} \Phi_d(X) \\ &= \Phi_p(X)\Phi_1(X) \text{ car } p \in \mathcal{P} \\ &= \Phi_p(X)(X-1) \end{aligned}$$

Donc $\Phi_p(X) = \dfrac{X^p - 1}{X - 1} = 1 + X + ... + X^{p-1}$. Donc $\boxed{\Phi_p(1) = p}$

Or μ_p^* est de cardinal $\phi(p) = p - 1$, et ne contient pas 1 : donc $\mu_p^* = \mu_p \backslash \{1\}$, et donc, si l'on choisit $\xi \in \mu_p^*$,

$$\Phi_p(X) = \prod_{k=1}^{p-1} \left(X - \xi^k\right)$$

.

On obtient donc

$$\forall \xi \in \mu_p^*, \prod_{k=1}^{p-1} \left(1 - \xi^k\right) = p$$

En utilisant le fait que p est un nombre premier impair, on remarque que, pour $\xi \in \mu_p^*$, $\xi^2 \in \mu_p^*$. Observons ce qui se passe lorsque l'on injecte ξ^2 dans la formule ci-dessus.

$$\begin{aligned} p &= \prod_{k=1}^{p-1} \left(1 - \xi^{2k}\right) \\ &= \prod_{k=1}^{p-1} \left(\xi^k \xi^{-k} - \xi^{2k}\right) \\ &= \prod_{k=1}^{p-1} \xi^k \prod_{k=1}^{p-1} \left(\xi^{-k} - \xi^k\right) \end{aligned}$$

Or $\displaystyle\prod_{k=1}^{p-1} \xi^k = \xi^{\sum_{k=0}^{p-1} k}$, et

$S = \displaystyle\sum_{k=1}^{p-1} k = \frac{p(p-1)}{2}$ est un multiple de p, car p est impair et donc $\dfrac{p-1}{2} \in \mathbb{Z}$: donc $\xi^S = 1$

On obtient finalement $\boxed{p = \displaystyle\prod_{k=1}^{p-1} \left(\xi^{-k} - \xi^k\right)}$

On va essayer de couper ce produit en deux pour faire apparaître $\sqrt{p}$.

Soit $\xi \in \mu_p^*$: soit $\omega = \displaystyle\prod_{k=1}^{\frac{p-1}{2}} \left(\xi^{-k} - \xi^k\right)$

On remarque que

$$\begin{aligned} \omega &= \prod_{k=1}^{\frac{p-1}{2}} \left(\xi^{p-k} - \xi^{k-p}\right) \text{ car } \xi^{\pm p} = 1 \\ &= \prod_{j=\frac{p+1}{2}}^{p-1} \left(\xi^j - \xi^{-j}\right) \text{ par } j := k - p \\ &= (-1)^{\frac{p-1}{2}} \prod_{j=\frac{p+1}{2}}^{p-1} \left(\xi^{-j} - \xi^j\right) \end{aligned}$$

Or $\dfrac{p-1}{2}$ est un entier pair, car $p \equiv 1[4]$. Donc $(-1)^{\frac{p-1}{2}} = 1$

Il vient finalement $\omega = \prod_{j=\frac{p+1}{2}}^{p-1} \left(\xi^{-j} - \xi^{j}\right)$, et donc

$$\begin{aligned} \omega^2 &= \left(\prod_{k=1}^{\frac{p-1}{2}} \left(\xi^{-k} - \xi^{k}\right)\right)\left(\prod_{j=\frac{p+1}{2}}^{p-1} \left(\xi^{-j} - \xi^{j}\right)\right) \\ &= \prod_{k=1}^{p-1} \left(\xi^{-k} - \xi^{k}\right) \end{aligned}$$

Conclusion : $\boxed{\omega^2 = p}$, et, comme $\omega \in \mathbb{Q}[\xi] = \mathbb{Q}[\mu_p]$, on a bien $\boxed{\mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\mu_p]}$.

3. Cas général

Soit d un entier sans facteur carré : écrivons $d = s\, 2^{\delta} p_1 p_2 \cdots p_n$, avec $\begin{cases} s \in \{-1, 1\} \\ \delta \in 0, 1 \\ p_1, ..., p_n \in \mathcal{P}\backslash\{2\}, \text{ distincts deux à deux} \end{cases}$

Soit $q_i = s_i p_i$, avec $s_i = (-1)^{\frac{p_i - 1}{2}}$:
alors $q_i \equiv 1[4]$, donc nous sommes dans le cas **2** : $\mathbb{Q}\left[\sqrt{q_i}\right] \subset \mathbb{Q}[\mu_{q_i}]$

Remarque : si $\alpha \in \mu_n$ et $\beta \in \mu_m$, alors $(\alpha\beta)^{mn} = (\alpha^n)^m (\beta^m)^n = 1$, donc $\alpha\beta \in \mu_{mn}$.

Ici, cette remarque implique que $\mathbb{Q}\left[\sqrt{q_1 \cdots q_n}\right] \subset \mathbb{Q}[\mu_{q_1 \cdots q_n}]$
Cela nous intéresse parce que nous pouvons en fait réécrire d à partir des q_i :

$$d = t 2^{\delta} q_1 \cdots q_n,$$

avec

$$t = s \cdot \prod_{i=1}^{n} s_i$$

Il reste à gérer la partie $t2^{\delta}$.

- Si $\delta = 0$:
  - · Si $t = 1$: Alors $d = q_1 \cdots q_n$, et donc $\mathbb{Q}\left[\sqrt{d}\right] \subset \mathbb{Q}[\mu_{q_1 \cdots q_n}] = \mathbb{Q}\left[\mu_{|d|}\right]$
  - · Si $t = -1$: Alors $\mathbb{Q}\left[\sqrt{d}\right] \subset \mathbb{Q}[\mu_4, \mu_{q_1 \cdots q_n}] \subset \mathbb{Q}[\mu_{4q_1 \cdots q_n}] = \mathbb{Q}\left[\mu_{4|d|}\right]$
- Si $\delta = 1$: alors $\mathbb{Q}\left[\sqrt{2t}\right] = \mathbb{Q}\left[\sqrt{\pm 2}\right] \subset \mathbb{Q}[\mu_8]$, donc $\mathbb{Q}\left[\sqrt{d}\right] \subset \mathbb{Q}[\mu_8, \mu_{q_1 \cdots q_n}] \subset \mathbb{Q}[\mu_{4q_1 \cdots q_n}] = \mathbb{Q}\left[\mu_{4|d|}\right]$

  Le théorème est donc démontré !

Remarques :

Le plus petit entier f tel que $\mathbb{Q}\left[\sqrt{d}\right] \subset \mathbb{Q}[\mu_f]$ vérifie $f \in \{|d|, 4|d|\}$ et est bien donné par la méthode ci-dessus. Cet entier est appelé **conducteur** de $\mathbb{Q}\left[\sqrt{d}\right]$

En fait, le théorème est vrai pour toute extension abélienne de $\mathbb{Q}$; c'est même une caractérisation : une extension de $\mathbb{Q}$ est abélienne si et seulement si elle est une sous-extension d'une extension cyclotomique.

Ce théorème est aujourd'hui démontré comme une conséquence de la théorie des corps de classes.
Dans le cas général, la notion de conducteur est définie comme ci-dessus et est utilisée en théorie des nombres.