

Kronecker-Weber faible

Ce développement présente une démonstration par une somme de Gauss du théorème de Kronecker-Weber (version faible), qui permet de dire que tout corps de nombre de degré 2 est inclus dans une extension cyclotomique. On montre d'abord que toute extension quadratique peut se ramener sous une forme 'canonique', puis un calcul du carré d'une somme de Gauss permet de conclure.

Côté recasage, l'utilisation des racines de l'unité permet de le mettre dans la leçon 102. L'utilisation des corps cyclotomiques (même si on n'utilise que très peu de résultats de la théorie des corps) permet un recasage honnête dans les leçons 125 et 127. Enfin, la manipulation de racines primitives, les corps $\mathbb{F}_p$ et l'utilisation de la décomposition en premier permet un recasage en 121.

I - Le développement

🔗 Théorème 1

⌋ Toute extension quadratique de $\mathbb{Q}$ est incluse dans une extension cyclotomique.

Nous allons d'abord présenter un résultat intermédiaire qui permet de ramener l'étude des extensions quadratiques à un cas plus simple qu'on pourra exploiter.

🔗 Lemme 2

⌋ Soit L une extension quadratique de $\mathbb{Q}$. Il existe $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré tel que $L = \mathbb{Q}(\sqrt{d})$ (avec pour convention $\sqrt{d} = i\sqrt{-d}$ si d est négatif).

🔗 Preuve :

Soit $x \in L \setminus \mathbb{Q}$. On a $L = \mathbb{Q}(x)$ (car $[L : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}] = 2$). Notons $M(X) = X^2 + bX + c$ son polynôme minimal. On peut alors l'écrire sous la forme

$$M(X) = X^2 + bX + c = \left(X + \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4}.$$

Posons $y = 2x + b$, de sorte à avoir

$$y^2 = b^2 - 4c \in \mathbb{Q} \quad \text{et} \quad L = \mathbb{Q}(x) = \mathbb{Q}(y).$$

Écrivons $b^2 - 4c = \frac{r}{s}$, avec $(r, s) \in \mathbb{Z}^* \times \mathbb{N}^*$. Alors $z = sy$ vérifie

$$z^2 = rs \in \mathbb{Z} \quad \text{et} \quad L = \mathbb{Q}(z).$$

Finalement, en écrivant $rs = m^2d$ dans $\mathbb{Z}$, avec d sans facteur carré, on obtient

$$L = \mathbb{Q}(z) = \mathbb{Q}\left(\frac{z}{m}\right) = \mathbb{Q}(\sqrt{d}) \quad \text{car} \quad d = \left(\frac{z}{m}\right)^2.$$



Passons maintenant à la preuve du théorème.

Preuve :

Étape 1 : Calcul d'une somme de Gauss

Soit p un nombre premier impair, ζ une racine primitive p -ième de l'unité et $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre modulo p . On fera l'abus d'écrire $\left(\frac{x}{p}\right)$ où $x \in \mathbb{F}_p$, pour désigner le symbole de Legendre d'un de ses représentants dans $\mathbb{Z}$ (les propriétés du symbole de Legendre donnent la bonne définition de cet abus). De même, on fera l'abus d'écrire ζ^x pour désigner ζ à la puissance d'un représentant de x . On pose

$$s(1) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \zeta^x.$$

Alors

$$s(1)^2 = \left(\frac{-1}{p}\right) p.$$

En effet :

$$\begin{aligned} s(1)^2 &= \sum_{x, y \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{x+y} \\ &= \sum_{x, y \in \mathbb{F}_p^\times} \left(\frac{xy^{-1}}{p}\right) \zeta^{x+y} \quad \text{car } \left(\frac{y}{p}\right) = \left(\frac{y^{-1}}{p}\right) \\ &= \sum_{x \in \mathbb{F}_p^\times} \left(\frac{-1}{p}\right) \zeta^0 + \sum_{\substack{x, y \in \mathbb{F}_p^\times \\ x \neq -y}} \left(\frac{xy^{-1}}{p}\right) \zeta^{x+y}. \end{aligned}$$

On réalise le changement d'indice

$$\begin{cases} xy^{-1} = t \\ x + y = u \end{cases} \quad \text{i.e.} \quad \begin{cases} x = \frac{tu}{1+u} \\ y = \frac{u}{1+t} \end{cases} \quad \text{avec } t \neq -1, u \neq 0.$$

On obtient ainsi

$$s(1)^2 = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{-1}{p}\right) + \sum_{t \in \mathbb{F}_p^\times \setminus \{-1\}} \left(\frac{t}{p}\right) \sum_{u \in \mathbb{F}_p^\times} \zeta^u.$$

Or, la double somme peut s'écrire sous la forme

$$\sum_{t \in \mathbb{F}_p^\times \setminus \{-1\}} \left(\frac{t}{p}\right) = - \sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)$$

car $\sum_{u \in \mathbb{F}_p} \zeta^u = \sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) = 0$. On a donc :

$$s(1)^2 = (p-1) \left(\frac{-1}{p}\right) + \text{left} \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) p.$$

Étape 2 : Démonstration du théorème par le lemme et la somme de Gauss.

Cas 1 : Soit $\zeta \in \mu_8^\times(\mathbb{C})$ (racines primitives huitièmes). Alors $\zeta^4 = -1$, d'où $\zeta^2 + \zeta^{-2} = 0$ et $(\zeta + \zeta^{-1})^2 = 2$, d'où $\sqrt{2} = \pm(\zeta + \zeta^{-1}) \in \mathbb{Q}(\zeta)$, et donc $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta) = \mathbb{Q}(\mathbb{U}_8)$ (corps cyclotomique associé aux racines huitièmes de l'unité). Remarquons aussi que $i \in \mathbb{Q}(\zeta)$, d'où $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\zeta) = \mathbb{Q}(\mathbb{U}_8)$.

Cas 2 : Soit p premier impair. Soit $\zeta \in \mu_p^\times(\mathbb{C})$.

On a

$$s(1) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \zeta^x \in \mathbb{Q}(\zeta) \quad \text{et} \quad s(1)^2 = \left(\frac{-1}{p}\right) p \quad (\text{étape 1}),$$

d'où,

$$\sqrt{p} = \pm s(1) \quad \text{et} \quad \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\mathbb{U}_p)$$

ou

$$\sqrt{p} = \pm i s(1) \quad \text{et} \quad \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(i, \zeta) \subset \mathbb{Q}(\mathbb{U}_{4p})$$

selon le signe de $\left(\frac{-1}{p}\right) p$.

Cas général : D'après le lemme, on peut se ramener à l'étude de $\mathbb{Q}(\sqrt{d})$, avec $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré.

On peut écrire $d = \pm 2^k p_1 \cdots p_r$ avec $k = 0, 1$ et les p_j premiers impairs distincts. Par ce qui précède, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(i, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}) \subset \mathbb{Q}(\mathbb{U}_8, \mathbb{U}_{4p_1}, \dots, \mathbb{U}_{4p_r}) \subset \mathbb{Q}(\mathbb{U}_m)$ où $m = 8p_1 \cdots p_r$ car $\mu_8 \subset \mu_\ell$ ssi $8 \mid \ell$



II - Un résultat à connaître

Dans ce développement, pour le calcul de la somme de Gauss, on a utilisé un petit résultat à savoir redémontrer.

✚ Propriété 3

Soit G un groupe et $\chi : G \rightarrow \mathbb{C}^\times$ un morphisme de groupes non trivial. Alors :

$$\sum_{g \in G} \chi(g) = 0.$$

Preuve :

Soit $g' \in G$ tel que $\chi(g') \neq 1$ (possible car χ non trivial). On a alors :

$$\chi(g') \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g'g) \underbrace{=}_{h=g'g} \sum_{h \in G} \chi(h) = \sum_{g \in G} \chi(g),$$

d'où

$$\sum_{g \in G} \chi(g) = 0.$$



III - Remarques

1 - Ce développement est généralement fait sans le lemme, en prenant directement des extensions de la forme $\mathbb{Q}(\sqrt{d})$, mais je trouve que c'est quand même oublier une partie du travail (le lemme n'est pas compliqué

à obtenir, mais il n'est pas si trivial que ça, il se trouve au début du [Goz]). Si vous êtes à cours de temps, vous pouvez toujours l'admettre et le présenter dans les grandes lignes.

2 - L'idée du lemme est de partir d'un générateur de L , puis de passer étape par étape à générateur situer dans un anneau 'plus' simple : d'abord $y \in \sqrt{\mathbb{Q}}$, puis $z \in \sqrt{\mathbb{Z}}$

3 - Pour la somme de Gauss, j'ai préféré faire un changement d'indice multiple en un coup, car cela me paraissait plus clair. Si vous n'êtes pas à l'aise, vous pouvez toujours découper en deux changements d'indices. Par ailleurs, même si vous êtes aussi feignant que moi, il faudra (au moins à l'oral) décrire les notations utilisées dans la somme de Gauss et au moins dire (même sans justifier, au pire ça fera une question) qu'elles sont cohérentes et bien définies.

4 - La version forte du théorème donne en réalité l'inclusion dans des corps cyclotomiques de toute extension galoisienne dont le groupe de Galois est abélien.

5 - Je n'ai pas trouvé d'application particulière de cette version affaiblie. L'intérêt de ce développement réside pour moi dans le fait de démontrer dans un cadre plus habituel (les corps de nombres de degré 2) le théorème de Kronecker-Weber. (et faut-il vraiment trouver une application concrète à tout ce que l'on fait ?).

IV - Références

[Goz] : *Théorie de Galois*, Ivan Gozard