

DM 2 : "Autour de la loi de réciprocité quadratique."

À remettre le 13 avril.

On trouvera en annexe un rappel sur la décomposition des nombres premiers dans une extension quadratique (vue en TD), à utiliser librement dans le problème.

Exercice.

Soit K une extension galoisienne de $\mathbb{Q}$, d'anneau des entiers $\mathcal{O}_K$, p un nombre premier *non ramifié* dans K et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_K$ au-dessus de p . On rappelle (cf. cours) que le groupe de décomposition $D_{\mathfrak{P}}$ de $\mathfrak{P}$ est alors cyclique et qu'il admet un générateur privilégié $\sigma_{\mathfrak{P}}$ appelé *automorphisme de Frobenius* en $\mathfrak{P}$, caractérisé par la propriété

$$\sigma_{\mathfrak{P}}(x) \equiv x^p \pmod{\mathfrak{P}} \text{ pour tout } x \in \mathcal{O}_K. \quad (1)$$

Soit F une sous-extension de K , elle-même galoisienne sur $\mathbb{Q}$, d'anneau des entiers $\mathcal{O}_F$. L'idéal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$ est alors un idéal premier de $\mathcal{O}_F$ au-dessus de p (cf. cours).

1. Montrer que $\mathfrak{p}$ est non ramifié dans F .
2. On note $\sigma_{\mathfrak{p}}$ l'automorphisme de Frobenius en $\mathfrak{p}$. Montrer que $\sigma_{\mathfrak{P}}|_F = \sigma_{\mathfrak{p}}$.

Problème.

Dans tout ce qui suit, p et q désignent deux nombres premiers impairs. On rappelle que si a est un entier premier à p , le *symbole de Legendre* $\left(\frac{a}{p}\right)$ est défini par

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } a \text{ est un carré modulo } p \\ -1 & \text{sinon.} \end{cases}$$

Le but du problème est d'établir la loi de réciprocité quadratique, qui affirme que, si p et q sont deux nombres premiers impairs, on a

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \quad (2)$$

Soit $K = \mathbb{Q}(\zeta)$ le corps engendré par une racine primitive p -ième de l'unité ζ dans $\mathbb{C}$. On rappelle que l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois G isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$. Explicitement, pour tout $\sigma \in G$, il existe un entier $j(\sigma)$ premier à p et uniquement déterminé modulo p , tel que $\sigma(\zeta) = \zeta^{j(\sigma)}$.

1. Montrer que G contient un unique sous-groupe H d'indice 2. En déduire que K contient un unique sous-corps quadratique F , et que $\text{Gal}(F/\mathbb{Q}) \simeq G/H$. À quel sous-groupe correspond H dans l'identification de $\text{Gal}(K/\mathbb{Q})$ avec $(\mathbb{Z}/p\mathbb{Z})^\times$?

2. Montrer que p est l'unique premier ramifié dans F . En déduire que $F = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{si } p \equiv 1 \pmod{4} \\ \mathbb{Q}(\sqrt{-p}) & \text{si } p \equiv 3 \pmod{4} \end{cases}$

soit, dans tous les cas,

$$F = \mathbb{Q}(\sqrt{d}) \text{ où } d = (-1)^{\frac{p-1}{2}} p. \quad (3)$$

3. Soit q un premier impair distinct de p , $\mathfrak{Q}$ un idéal premier de K au-dessus de q et $\sigma_{\mathfrak{Q}} \in G$ l'automorphisme de Frobenius en $\mathfrak{Q}$. Avec les notations rappelées ci-dessus, on a donc $j(\sigma_{\mathfrak{Q}}) = q$. Montrer que la restriction de $\sigma_{\mathfrak{Q}}$ à F est égale à l'identité si et seulement si $\left(\frac{q}{p}\right) = +1$.
4. Soit $\mathfrak{q}$ un idéal premier de F au-dessus de q , et $\tau_{\mathfrak{q}} \in \text{Gal}(F/\mathbb{Q})$ l'isomorphisme de Frobenius correspondant. Montrer que $\tau_{\mathfrak{q}}$ est égale à l'identité si et seulement si q est décomposé dans F .
5. Montrer par ailleurs que $\tau_{\mathfrak{q}} = \sigma_{\mathfrak{Q}}|_F$.
6. En confrontant les résultats obtenus en 3 et 4, conclure que

$$\left(\frac{q}{p}\right) = \left(\frac{d}{q}\right). \quad (4)$$

7. Montrer enfin que $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ et établir la loi de réciprocité quadratique à partir de (4).

Annexe : décomposition des nombres premiers dans une extension quadratique.

Soit $K = \mathbb{Q}(\sqrt{d})$, où d est un entier relatif sans facteur carré, et p un nombre premier.

- si p est impair, il est
 - ramifié dans $K/\mathbb{Q}$ si p divise d ,
 - inerte dans $K/\mathbb{Q}$ si $\left(\frac{d}{p}\right) = -1$,
 - décomposé dans $K/\mathbb{Q}$ si $\left(\frac{d}{p}\right) = +1$.
- 2 est
 - ramifié dans $K/\mathbb{Q}$ si $d \equiv 2$ ou $3 \pmod{4}$,
 - inerte dans $K/\mathbb{Q}$ si $d \equiv 5 \pmod{8}$,
 - décomposé dans $K/\mathbb{Q}$ si $d \equiv 1 \pmod{8}$.