
Feuille 5 : Corps de classe

Soit K un corps de nombres. On appelle *cycle arithmétique* ou *module* un produit formel de places

$$\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{e_v}$$

où $e_v \geq 0$ est de support fini, et $e_v \in \{0, 1\}$ si v est réelle et $e_v = 0$ si v est complexe (ici $\mathcal{P}_v$ est l'idéal maximal de $\mathcal{O}_K$ associé à v si v est non archimédienne et il est juste un symbole si v est archimédienne). On le voit également comme la donnée d'un idéal entier $\mathcal{M}_f$ de $\mathcal{O}_K$ et d'un sous-ensemble $\mathcal{M}_\infty$ de places réelles. Soit $\mathcal{M} = \prod_{v \in S_K} \mathcal{P}_v^{e_v}$ un module. Pour $(x_v)_{v \in S_K}$ on écrit $x \equiv 1 \pmod{\mathcal{M}}$ si $x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}}$ pour tout $v \in S_K$, avec la convention que $x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}}$ signifie :

- la congruence habituelle si v est non archimédienne et $e_v > 0$;
- $x \in \mathcal{O}_{K_v}^*$ si v est non archimédienne et $e_v = 0$;
- $x_v > 0$ si v est réelle et $e_v = 1$;
- aucune condition sinon.

On note $\mathcal{I}(K)^\mathcal{M}$ le sous-groupe du groupe $\mathcal{I}(K)$ des idéaux fractionnaires de K engendrés par les idéaux de $\mathcal{O}_K$ premiers à $\mathcal{M}$. On écrit $\mathcal{P}(K)^\mathcal{M}$ pour le sous-groupe de $\mathcal{I}(K)^\mathcal{M}$ engendré par les idéaux principaux de K de la forme $a\mathcal{O}_K$, avec $a \neq 0$ et $a - 1 \in \mathcal{P}_v^{e_v}$ pour tous v place fini et $a_v > 0$ si v est une place infinie avec $e_v = 1$. On pose

$$\mathbb{A}_K^*(\mathcal{M}) = \{(x_v)_{v \in S_K} \text{ tel que } x_v \equiv 1 \pmod{\mathcal{P}_v^{e_v}} \forall v \in S_K\}$$

On note $C_K^\mathcal{M} = \mathbb{A}_K^*(\mathcal{M}) \cdot K^*/K^*$ et $\text{Cl}(K)^\mathcal{M} = \mathcal{I}(K)^\mathcal{M}/\mathcal{P}(K)^\mathcal{M} \cong C_K/C_K^\mathcal{M}$ le groupe de classes de rayon $\mathcal{M}$ (où $C_K = \mathbb{A}_K^*/K^*$). On écrit $H^\mathcal{M}$ pour le corps de classes de rayon $\mathcal{M}$.

Exercice 1. Soit p un nombre premier impair. Combien existe-t-il d'extensions de $\mathbb{Q}_p$ ayant pour groupe de Galois $\mathbb{Z}/p\mathbb{Z}$? Combien sont-elles non ramifiées ?

Exercice 2. Soit L/K une extension finie abélienne de corps locaux p -adiques. Montrer qu'elle est non ramifiée si et seulement si $\mathcal{O}_K^* \subseteq \text{Norm}_{L/K}(L^*)$ (dans ce cas L est la seule extension non ramifiée de degré $[L : K]$ de K).

Exercice 3. Soit L/K une extension finie abélienne de corps locaux p -adiques. Montrer qu'elle est totalement ramifiée si et seulement si $\text{Norm}_{L/K}(L^*)$ contient une uniformisante de $\mathcal{O}_K$.

Exercice 4. On considère le corps $K = \mathbb{Q}$.

1. Quels sont les diviseurs arithmétiques ?

2. Supposons $\mathcal{M} = 1$.
 - (a) Expliciter $\mathcal{I}(\mathbb{Q})^{\mathcal{M}}$ et $\mathcal{P}(\mathbb{Q})^{\mathcal{M}}$ puis déterminer $\text{Cl}(\mathbb{Q})^{\mathcal{M}}$.
 - (b) Expliciter $\mathbb{A}_{\mathbb{Q}}^*(\mathcal{M})$ et $C_{\mathbb{Q}}^{\mathcal{M}}$. Vérifier que

$$C_{\mathbb{Q}}/C_{\mathbb{Q}}^{\mathcal{M}} \cong \text{Cl}(\mathbb{Q})^{\mathcal{M}}$$

En déduire que

$$C_{\mathbb{Q}} \cong \left(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / \{\pm 1\}$$

- (c) Déterminer $H^{\mathcal{M}}$.
3. Mêmes questions pour $\mathcal{M} = (\infty)$, en déduisant que

$$C_{\mathbb{Q}} \cong \mathbb{R}_{>0}^* \times \prod_p \mathbb{Z}_p^*$$

(Attention : cette dernière décomposition n'est pas utile dans la pratique, car elle ne respecte pas l'inclusion diagonale.)

4. Mêmes questions pour $\mathcal{M} = (5)$.
5. Mêmes questions pour $\mathcal{M} = ((5)\infty)$ (pour la dernière question, considérer le corps $\mathbb{Q}(\zeta_5)$).

Exercice 5. Soient a et b des entiers premiers entre eux.

1. Montrer que

$$\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_{ab})$$

et en déduire que si $a \geq 3$ alors un premier p est ramifié dans $\mathbb{Q}(\zeta_a)$ si et seulement si $p \mid a$.

2. Montrer que

$$\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}$$

3. En déduire que $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Exercice 6. On considère encore le corps $K = \mathbb{Q}$ et soit $n \in \mathbb{N}$.

1. Montrer que le groupe de classes d'idèles de rayon $\mathcal{M}$ de $\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*/\{\pm 1\}$ si $\mathcal{M} = (n)$ et à $(\mathbb{Z}/n\mathbb{Z})^*$ si $\mathcal{M} = (n)\infty$.
2. Soit p un premier non divisant n et soit $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ correspondant à $p \in (\mathbb{Z}/n\mathbb{Z})^*$. Montrer que σ est la substitution de Frobenius en p .
3. Montrer que le corps de classe de $\mathbb{Q}$ de rayon $(n)\infty$ est $\mathbb{Q}(\zeta_n)$.

Exercice 7. 1. Montrer le *théorème de Kronecker-Weber* : toute extension abélienne finie de $\mathbb{Q}$ est incluse dans une extension cyclotomique.
 2. En déduire que tout groupe abélien est groupe de Galois d'une extension de $\mathbb{Q}$.

Exercice 8. Pour L une extension abélienne finie de K , on note $N(L) = \text{Norm}_{L/K}(L^*)$ le sous-groupe des normes. Soit L_1 et L_2 deux extensions abéliennes finies d'un corps local K contenues dans K^{ab} .

1. Montrer que si $L_1 \subseteq L_2$ alors $N(L_2) \subseteq N(L_1)$.
2. Montrer que $N(L_1 L_2) = N(L_1) \cap N(L_2)$.
3. En déduire que $L_1 \subseteq L_2 \iff N(L_2) \subseteq N(L_1)$.
4. Montrer que $N(L_1 \cap L_2) = N(L_1)N(L_2)$.

Exercice 9. Soit K un corps de nombres. On appelle *corps de classe de Hilbert de K* , noté K_H , la plus grande extension abélienne non ramifiée de K .

1. Montrer que le corps de classes de Hilbert K_H existe, et que

$$\text{Gal}(K_H/K) \cong \text{Cl}(K).$$

2. Déterminer le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{-5})$.
3. Soit encore $K = \mathbb{Q}(\sqrt{-5})$. Montrer qu'un nombre premier $p \neq 5$ s'écrit $p = x^2 + 5y^2$ si et seulement si p est totalement décomposé dans K_H , si et seulement si $p \equiv 1, 9 \pmod{20}$.
4. On suppose que K est de nombre de classe 1, et L/K une extension galoisienne non ramifiée (avec $L \neq K$). Montrer que $[L : K] \geq 60$.
5. Montrer que 3 divise le nombre de classes de $\mathbb{Q}(\sqrt{-23})$ (indication : $\text{disc}(x^3 - x - 1) = -23$).

Exercice 10. 1. Soit L/K une extension de corps de nombres telle que $L \cap K_H = K$. Montrer que l'application norme $\text{Cl}(L) \rightarrow \text{Cl}(K)$ est surjective.

2. Soit L/K une extension telle qu'un premier $\mathfrak{p}$ de $\mathcal{O}_K$ est totalement ramifié dans L . Montrer que les nombres de classes vérifient $h_K \mid h_L$.

Exercice 11. On considère $K = \mathbb{Q}(\zeta_3)$, le module $\mathcal{M} = (5 + 3\zeta_3)$ et L le corps de classe de rayon $\mathcal{M}$.

1. Montrer que $\text{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$. En déduire que L est de la forme

$$L = K \left(\sqrt[3]{\zeta_3^k (5 + 3\zeta_3)} \right).$$

2. Identifier L (considérer le Frobenius en $4 + 3\zeta_3$).