

Feuille 10 : Chebotarev et corps de classes

1 CHEBOTAREV

Exercice 1 :

1. Soit $f \in \mathbb{Z}[x]$ tel que f est scindé modulo p pour presque tout p . Montrer que f est scindé sur $\mathbb{Q}$.
2. Montrer que si un groupe fini G agit transitivement sur un ensemble X non trivial, il existe $g \in G$ tel que $\forall x \in X, g \cdot x \neq x$.
3. Montrer qu'un polynôme $f \in \mathbb{Z}[x]$ irréductible qui a une racine modulo p pour presque tout p est de degré 1.
4. Trouver un polynôme à coefficients entiers qui n'a pas de racine dans $\mathbb{Z}$ mais en a modulo tout nombre premier.

Exercice 2 :

Soit K un corps de nombres. Montrer que les idéaux premiers sont équidistribués dans $\text{Cl}(K)$.

2 CORPS DE CLASSES

Soit K un corps de nombres, on appelle *module* un produit formel de places $\mathfrak{m} = \prod_v v^{e_v}$ 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. On le voit également comme la donnée d'un idéal entier $\mathfrak{m}_f$ de $\mathcal{O}_K$ et d'un sous-ensemble $\mathfrak{m}_\infty$ de places réelles.

Si $\mathfrak{m}$ est un module, on note $U_{\mathfrak{m}}$ le sous-groupe ouvert d'indice fini $U_{\mathfrak{m}} = \prod_v U_v(e_v)$ où pour $v = \mathfrak{p}$

une place non-archimédienne on note $U_{\mathfrak{p}}(0) = \mathcal{O}_{\mathfrak{p}}^\times$ et $U_v(k) = 1 + \mathfrak{p}^k$ pour $k > 0$, tandis que pour v archimédienne on note $U_v(0) = K_v^\times$ et $U_v(1) = \mathbb{R}_+^\times$ pour v réelle. Remarque : cette définition diffère sur les places infinies de la définition employée pour les caractères, en effet la théorie du corps de classe s'écrit modulo la composante neutre du groupe des classes d'idèles.

On note $C_K(\mathfrak{m}) = \mathbb{A}_K^\times / (K^\times U_{\mathfrak{m}})$ le groupe de classes de rayon $\mathfrak{m}$, et $K_{\mathfrak{m}}$ le corps de classes de rayon $\mathfrak{m}$, alors $C_K(\mathfrak{m}) \simeq \text{Gal}(K_{\mathfrak{m}}/K)$, et l'extension $K_{\mathfrak{m}}/K$ est ramifiée en $\mathfrak{m}$ et non ramifiée en dehors de $\mathfrak{m}$,

Exercice 3 :

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

1. Avec quel rayon $\mathfrak{m}$ obtient-on le groupe $C_{\mathbb{Q}}(\mathfrak{m}) = (\mathbb{Z}/n\mathbb{Z})^\times$?
2. Déterminer tous les corps de classes de rayon de $\mathbb{Q}$.
3. Montrer que tout groupe abélien est groupe de Galois d'une extension sur $\mathbb{Q}$.

Exercice 4 : corps de classes de Hilbert

Soit K un corps de nombres, on appelle *corps de classe de Hilbert*, et on note K_H , la plus grande extension abélienne non ramifiée de K .

1. Montrer que K_H existe, et que $\text{Gal}(K_H/K) \simeq \text{Cl}(K)$.
2. Déterminer le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{-5})$.
3. 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 $p \equiv 1, 9 \pmod{20}$ (on remarquera que $K_H/\mathbb{Q}$ est abélienne).
4. On suppose que K est de nombre de classe 1, et L/K une extension galoisienne non ramifiée. Montrer que $[L : K] \geq 60$.

5. Montrer que 3 divise le nombre de classes de $\mathbb{Q}(\sqrt{-23})$ (indice : $\text{disc}(x^3 - x - 1) = -23$).

Exercice 5 : théorème de capitulation

Soit K un corps de nombres, et K_H son corps de classes de Hilbert, on veut montrer que tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ devient principal dans K_H . On note $K_H^{(2)}$ le corps de classes de Hilbert de K_H , et $G = \text{Gal}(K_H^{(2)}/K)$. On note $G^{ab} = G/D(G)$ l'abélianisé de G .

1. Montrer que $K_H^{(2)}/K$ est galoisienne.

2. Montrer que $\text{Gal}(K_H^{(2)}/K_H) = D(G)$.

3. On admet les points suivants :

- si H est un sous-groupe de G d'indice n , on considère une partition en classes $G = \bigcup_{i=1}^n \bar{g}_i$, et pour $g \in G$ on pose $\sigma(g)$ tel que $\bar{g} = g\bar{\sigma(g)}$. On a alors un opérateur de transfert bien défini $G^{ab} \rightarrow H^{ab}$ par
$$V(g) = \prod_{i=1}^n g_i g \sigma(g_i)^{-1} \pmod{D(H)}.$$
- le transfert $V : G/D(G) \rightarrow D(G)/D^2(G)$ est trivial (Furtwangler).
- pour toute tour d'extensions galoisiennes $K \subset L \subset M$ et tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans M , le transfert du symbole d'Artin $\left(\frac{M/K}{\mathfrak{p}}\right)$ de $\text{Gal}(M/K')^{ab}$ à $\text{Gal}(M/L)^{ab}$ est dans la classe du symbole d'Artin $\left(\frac{M/L}{\mathfrak{p}\mathcal{O}_L}\right)$.

Terminer la démonstration.

Exercice 6 : Nombres de classes

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 7 :

On considère $K = \mathbb{Q}(\zeta_3)$, le module $\mathfrak{m} = (5 + 3\zeta_3)$ et le corps de classes de rayon $K_{\mathfrak{m}}$.

1. Montrer que $\text{Gal}(K_{\mathfrak{m}}/K) \simeq \mathbb{Z}/3\mathbb{Z}$. En déduire que $K_{\mathfrak{m}}$ est de la forme $K_{\mathfrak{m}} = K(\sqrt[3]{\zeta_3^k(5 + 3\zeta_3)})$.

2. Identifier $K_{\mathfrak{m}}$ (considérer le Frobenius en $4 + 3\zeta_3$).