

Introduction à la théorie du corps de classes

Jean Kieffer

GT Corps de classes, 17/11/2020

1 Qu'est-ce que la théorie du corps de classes ?

La description suivante est tirée de [2]. Soit K un corps de nombres (une extension finie de $\mathbb{Q}$). Le but de la théorie du corps de classes tient en trois points.

1. “Décrire” toutes les extensions finies *abéliennes* de K en termes de l'arithmétique de K . Une extension L/K est dite abélienne si elle est finie galoisienne et si son groupe de Galois, noté $\text{Gal}(L/K)$, est abélien.
2. Si L/K est abélienne, décrire $\text{Gal}(L/K)$ canoniquement en termes de l'arithmétique de K .
3. Si L/K est abélienne, et si $\mathfrak{p}$ est un idéal premier l'anneau d'entiers $\mathbb{Z}_K$, décrire la décomposition de $\mathfrak{p}$ dans L en termes de l'arithmétique de K .

Par l'*arithmétique de K* , on entend les propriétés de son groupe des idéaux fractionnaires ou des idèles, de ses groupes de classes, et de leurs sous-groupes/quotients. Pour expliquer le point 3, on rappelle le résultat suivant.

Proposition 1. *Soit K un corps de nombres et L/K une extension finie galoisienne de degré n . Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_K$. Alors il existe un entier $e \geq 1$ et des idéaux $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ de $\mathbb{Z}_L$ distincts tels que*

$$\mathfrak{p}\mathbb{Z}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e. \quad (1)$$

Cette décomposition est unique à l'ordre près des $\mathfrak{P}_i$. Les corps résiduels $\mathbb{Z}_L/\mathfrak{P}_i$ sont deux à deux isomorphes, et contiennent le corps résiduel $\mathbb{Z}_K/\mathfrak{p}$. Soit

$$f = [\mathbb{Z}_L/\mathfrak{P}_i : \mathbb{Z}_K/\mathfrak{p}].$$

Alors $efg = n$.

On appelle e l'*indice de ramification* de $\mathfrak{p}$ dans L , et on dit que $\mathfrak{p}$ est *non ramifié* si $e = 1$. L'entier f est le *degré résiduel* de $\mathfrak{p}$. On dit que $\mathfrak{p}$ est *complètement décomposé* dans L , ou (osons l'anglicisme) *splitte complètement* dans L , si $g = n$.

Par exemple, une partie de l'objectif 3 est de caractériser les premiers qui se décomposent complètement dans une extension abélienne donnée de K .

Note historique. L'histoire de la théorie du corps de classes est exposée par Hasse dans le chapitre XI du livre de Cassels et Fröhlich [1]. En un sens, elle commence avec Gauss et la loi de réciprocité quadratique. La "théorie classique" se développe à partir de 1880 environ (Kronecker, Weber, Hilbert, Takagi, Artin, Hasse, ...). En 1933, Chevalley reformule cette théorie en termes d'idèles, et à peu près simultanément, développe la théorie du corps de classes local (extensions finies de $\mathbb{Q}_p$) de façon indépendante du cas global (corps de nombres). Après la seconde guerre mondiale, de nouvelles preuves sont données à l'aide de "méthodes cohomologiques" (Tate, Serre, ...). Ce sont ces dernières qui sont utilisées dans le livre de Cassels et Fröhlich publié en 1967 [1, chap. I–VII], que nous allons suivre.

2 Énoncé des théorèmes principaux

Groupe de classes d'idèles. Soit K un corps de nombres. Si $\mathfrak{p}$ est une place de K , on note $K_{\mathfrak{p}}$ le corps complété : il est muni de la topologie associée à la valeur absolue $|\cdot|_{\mathfrak{p}}$. On définit l'ouvert $U_{\mathfrak{p}}$ de $K_{\mathfrak{p}}^{\times}$ par

$$U_{\mathfrak{p}} = \{x : |x| = 1\} \quad \text{si } \mathfrak{p} \text{ est une place finie,} \quad U_{\mathfrak{p}} = K_{\mathfrak{p}}^{\times} \quad \text{sinon.}$$

Le *groupe des idèles* I_K de K est le groupe topologique donné comme le produit restreint :

$$I_K = \prod'_{\mathfrak{p}} (K_{\mathfrak{p}}^{\times}, U_{\mathfrak{p}}).$$

Les éléments de I_K sont donc des suites $(x_{\mathfrak{p}})$ indexées par les places de K , qui vérifient que $x_{\mathfrak{p}} \in U_{\mathfrak{p}}$ pour tout $\mathfrak{p}$ sauf éventuellement un nombre fini.

Le groupe multiplicatif $K^{\times}$ s'injecte naturellement dans I_K . Le quotient est le *groupe de classes d'idèles* $C_K = I_K/K^{\times}$.

Soit L/K une extension finie galoisienne de groupe de Galois G . Alors $I_K \subset I_L$, et I_L est un G -module. On a également $C_K \subset C_L$, et C_L est un

G -module. On en déduit une application norme

$$N_{L/K} : C_L \rightarrow C_K$$

en faisant le produit des conjugués sous Galois.

Dans le cas $K = \mathbb{Q}$, le groupe des idèles est particulièrement simple :

$$I_{\mathbb{Q}} = \mathbb{Q}^{\times} \times \mathbb{R}_+^{\times} \times \prod_p U_p.$$

Le groupe de classes d'idèles est donc $C_{\mathbb{Q}} = \mathbb{R}_+^{\times} \times \prod_p U_p$. De plus $U_p = \mathbb{Z}_p^{\times}$.

Frobenius locaux, symbole d'Artin. Soit L/K une extension finie galoisienne. On appelle S l'ensemble fini des places de K constitué des places archimédiennes et des places finies qui ramifient dans L . Alors si $\mathfrak{P}|\mathfrak{p} \notin S$, on a un isomorphisme entre

- le groupe de décomposition de $\mathfrak{P}$, qui est le sous-groupe de $\text{Gal}(L/K)$ laissant stable l'idéal $\mathfrak{P}$ de $\mathbb{Z}_L$.
- le groupe de Galois local $\text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.
- le groupe de Galois de l'extension résiduelle, $\text{Gal}((\mathbb{Z}_L/\mathfrak{P})/(\mathbb{Z}_K/\mathfrak{p}))$.

Ce dernier groupe est cyclique, engendré par le Frobenius. Son image dans $\text{Gal}(L/K)$ est appelé le *Frobenius local* associé à $\mathfrak{P}$.

On peut montrer que le Frobenius local ne dépend pas de $\mathfrak{P}$, à conjugaison près dans $\text{Gal}(L/K)$. On le note $\text{Frob}_{\mathfrak{p}}$.

Supposons maintenant L/K abélienne. Alors le Frobenius local ne dépend pas de $\mathfrak{P}$, mais seulement de la place $\mathfrak{p}$ de K .

Pour une place finie $\mathfrak{p}$ de K , notons π une uniformisante de $K_{\mathfrak{p}}$, on note $i(\pi)$ l'élément de I_K donné par 1 dans toutes les coordonnées sauf $\mathfrak{p}$, et par π à la coordonnée $\mathfrak{p}$.

Définition 2. Soit L/K une extension abélienne. On dit qu'un morphisme de groupes $\psi : I_K \rightarrow \text{Gal}(L/K)$ est une application d'Artin si les conditions suivantes sont vérifiées :

1. ψ est continue.
2. $\psi(K^{\times}) = 1$.
3. Pour toute place finie $\mathfrak{p} \notin S$ et pour toute uniformisante π de $K_{\mathfrak{p}}$, on a $\psi(i(\pi)) = \text{Frob}_{\mathfrak{p}}$.

On peut montrer que si ψ existe, elle est unique. On la note également $\psi_{L/K}$ ou $(\cdot, L/K)$. Comme elle est triviale sur $K^{\times}$, on peut également la voir comme une application $C_K \rightarrow \text{Gal}(L/K)$.

Les grands résultats de la théorie du corps de classes.

Théorème 3 (Loi de réciprocité d'Artin). *Soit L/K une extension abélienne finie. Alors l'application d'Artin associée à L/K existe, et on a une suite exacte*

$$1 \longrightarrow N_{L/K}C_L \longrightarrow C_K \xrightarrow{(\cdot, L/K)} G \longrightarrow 1.$$

Cela répond à l'objectif 2 de la théorie du corps de classes.

Théorème 4 (Théorème d'existence). *L'application $L \mapsto N_{L/K}(C_L)$ induit une bijection entre les extensions abéliennes finies de K et les sous-groupes ouverts de C_K .*

Cet énoncé correspond à l'objectif 1. En passant à la limite, on obtient un isomorphisme de groupes topologiques :

$$C_K/D_K \simeq G(K^{\text{ab}}/K)$$

où D_K est la composante connexe de l'identité dans le groupe C_K . On déduit de ces deux énoncés le résultat suivant :

Théorème 5 (Théorème de décomposition). *Soit L/K une extension abélienne finie et $\mathfrak{p}$ un idéal de K non ramifié dans L . Alors le degré résiduel de $\mathfrak{p}$ est l'ordre de $i(\pi)$ dans le quotient $C_K/N_{L/K}C_L$, pour toute uniformisante π de $K_{\mathfrak{p}}$.*

Cela répond à l'objectif 3.

3 La théorie du corps de classes local

Soit v une place de K , et soit L/K une extension abélienne finie. Alors on peut restreindre le symbole d'Artin à $K_v^{\times}$: on obtient un *symbole d'Artin local*

$$\psi_v : K_v^{\times} \rightarrow \text{Gal}(L_w/K_v)$$

où w est une place de L au-dessus de v . Par continuité, on a

$$\psi_{L/K}((x_v)) = \prod_v \psi_v(x_v)$$

donc le symbole d'Artin global détermine la collection des symboles d'Artin locaux et réciproquement.

Dans la théorie classique du corps de classe, c'est le symbole global qui est construit en premier : la méthode moderne que nous allons suivre prend le chemin inverse. La théorie du corps de classe local décrit, à l'aide du symbole d'Artin local, les extensions abéliennes des corps locaux.

Théorème 6 (Loi de réciprocité locale). *Soit K un corps local non-archimédien. Alors il existe un unique morphisme de groupes continu*

$$\psi_K : K^\times \rightarrow \text{Gal}(K^{\text{ab}}/K)$$

tel que

1. Pour toute uniformisante π de K , et toute extension finie non ramifiée L/K , $\psi_K(\pi)$ agit sur L comme $\text{Frob}_{L/K}$.
2. Pour toute extension finie abélienne L/K , ψ_K induit un isomorphisme

$$K^\times / N_{L/K}(L^\times) \rightarrow \text{Gal}(L/K).$$

En particulier l'indice de $N_{L/K}(L^\times)$ dans $K^\times$ est $[L : K]$.

4 Le cas $K = \mathbb{Q}$

En guise d'exemple, appliquons les théorèmes de la théorie du corps de classes pour étudier les extensions abéliennes de $\mathbb{Q}$.

Le théorème de Kronecker–Weber. Soit $L = \mathbb{Q}(\zeta)$ où ζ est une racine primitive m -ième de l'unité. Alors on vérifie les faits suivants :

- Si p est un nombre premier non ramifié dans L (i.e. $p \nmid m$), alors $\text{Frob}_p \in \text{Gal}(L/K)$ satisfait

$$\text{Frob}_p(\zeta) = \zeta^p.$$

(En effet, les puissances de ζ ont alors des images distinctes dans $\mathbb{F}_p$).

- Notons $\zeta \mapsto \zeta^u$ l'action naturelle de $\widehat{\mathbb{Z}}$ sur le groupe μ de toutes les racines de l'unité dans $\mathbb{C}$, et notons $r : C_{\mathbb{Q}} \rightarrow \widehat{\mathbb{Z}}$ l'application naturelle. Alors pour tout $x \in I_{\mathbb{Q}}$, on a

$$\psi_{L/K}(x)(\zeta) = \zeta^{r(x)^{-1}}.$$

(On le vérifie pour $x = i(p)$, s'étend par continuité).

- $\mathbb{Q}^{\text{ab}}$ est la composée de toutes les extensions cyclotomiques. C’est le théorème de Kronecker–Weber. (On a utilisé la loi de réciprocité, et la partie facile (unicité) du théorème d’existence).

Références

- [1] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory*. Academic Press, London, 1967.
- [2] D. Garbanati. Class field theory summarized. *Rocky Mt. J. Math.*, 11(2), 1981.