Complex multiplication constructions of abelian extensions of quartic fields

Asuncion, J.G.

Introduction

Les polynômes sont des elements de base importants dans presque toutes les ma thé ma tiques. En théorie des nombres, un nombre qui est la racine d'un polynôme à coefficients dans $\mathbb{Q}$, comme

$$a_n x^n + \ldots + a_1 x + a_0 \qquad \text{où} \qquad a_i \in \mathbb{Q},$$

s'appelle un *nombre algébrique*. Par exemple, le nombre complexe

$$\zeta_5 := \exp(2\pi i/5)$$

qui est une racine du polynôme

$$f = x^4 + x^3 + x^2 + x + 1$$

de degré 4, dont les coefficients sont tous $1 \in \mathbb{Q}$, est un nombre algébrique.

Un corps de nombres est une extension du corps $\mathbb{Q}$ obtenue en adjoignant un ensemble fini de nombres algébriques à $\mathbb{Q}$. Par exemple, le plus petit corps contenant $\mathbb{Q}$ et toutes les racines du polynôme f est écrit $\mathbb{Q}(\zeta_5)$. Ce corps est obtenu en adjoignant l'ensemble des racines du polynôme f à $\mathbb{Q}$. Plus concrètement, ce corps de nombres $\mathbb{Q}(\zeta_5)$ est donné par

$$\left\{a + b\,\zeta_5 + c\,\zeta_5^2 + d\,\zeta_5^3 + e\,\zeta_5^4 : a, b, c, d, e \in \mathbb{Q}\right\}.$$

La théorie de Galois, developpée par le mathématicien français Évariste Galois pendant les années 1800s, décrit les symétries entre les racines des polynômes et les symétries liées dans les corps de nombres qui leur sont associés. Il a fait cette description en termes de ce qu'on appelle maintenant un *groupe de Galois*. Le groupe de Galois d'une extension de corps galoisienne $L/\mathbb{Q}$ est composé des automorphismes du corps de nombres L qui fixent $\mathbb{Q}$.

Le théorème de Kronecker-Weber est un résultat classique de la théorie des nombres. Il concerne les extensions abéliennes, extensions galoisiennes d'un corps de nombres avec un groupe de Galois abélien.

> **Théorème de Kroncker-Weber.** Toute extension abélienne finie de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_m)$ avec $\zeta_m = \exp(2\pi i/m)$ pour un certain entier m.
>
> Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times$ via l'application
>
> $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a + m\mathbb{Z} &\mapsto (\zeta_m \mapsto \zeta_m^a).\end{aligned}$$

Ce théorème combiné à la théorie de Galois nous dit que toute extension abélienne de $\mathbb{Q}$ peut être exprimée comme $\mathbb{Q}(\boldsymbol{\alpha})$ où $\boldsymbol{\alpha}$ est un polynôme en une racine m-ème de l'unité pour un certain entier m. Par exemple, l'extension abélienne

$$L = \mathbb{Q}[X]/(X^3 - 3X + 1)$$

est contenue dans le corps cyclotomique $\mathbb{Q}(\zeta_9)$. Effectivement, le corps L est égal à

$$\mathbb{Q}(\zeta_9 + \zeta_9^8).$$

Bien que L soit aussi contenu dans d'autres corps cyclotomiques $\mathbb{Q}(\zeta_n)$ pour d'autres entiers n, le plus petit entier vérifiant cette condition est 9. Cet entier est appelé le conducteur de l'extension $L/\mathbb{Q}$.

Le douzième problème de Hilbert, aussi connu comme le Jugendtraum de Kronecker, demande de chercher un analogue du théorème de Kronecker-Weber quand le corps de base est remplacé par un autre corps de nombres.

La théorie des corps de classes nous dit que pour tout corps de nombres K, et pour tout entier positif m, il existe une bijection entre l'ensemble des sous-groupes du groupe appelé *groupe* $Cl_K(m)$ *de classes de rayon* m de K et l'ensemble des extensions abéliennes L/K dont le conducteur divise m. Toutefois, étant donné un sous-groupe de $\mathrm{Cl}_K(m)$, la bijection correspondante ne fournit pas a priori une description explicite des extensions abéliennes.

Tout espoir n'est pas perdu parce qu'il existe un cas pour lequel un analogue explicite du théorème de Kroncker-Weber est connu. C'est le cas où le corps de base K est un corps de nombres quadratique imaginaire, au lieu du corps $\mathbb{Q}$ de Kronecker-Weber. La théorie de la multiplication complexe (CM) pour les courbes elliptiques nous fournit cet analogue. En utilisant la théorie CM, on peut trouver des polynômes de définition de n'importe quelle extension abélienne d'un corps de nombres quadratique imaginaire.

Une généralisation de la théorie CM aux variétés abéliennes principalement polarisées de dimension supérieure a éte développée par Shimura et Taniyama pendant les années 1950. Comme la théorie pour les courbes elliptiques, la généralisation de la théorie CM décrit explicitement les extensions abéliennes des corps CM en termes de valeurs spéciales de fonctions modulaires. Toutefois, la théorie ne couvre pas toutes les extensions abéliennes d'un corps CM, de sorte que ce n'est pas exactement un analogue du théorème de Kronecker-Weber.

Cette thèse est composée des chapitres suivants.

Dans le Chapitre 1, nous rappelons comment la théorie CM est utilisée pour trouver toutes les extensions d'un corps de nombres quadratique imaginaire. Dans le Chapitre 2, nous rappelons la théorie CM plus générale.

Une adaption de [30, Theorem 2] de Shimura nous montre que pour un certain entier positif m, le corps de classes de Hilbert $H_{K^r}(1)$ d'un corps CM K^r avec un sous-corps quadratique réel K_0^r est contenu dans le compositum Ξ_m du corps de classes de rayon $H_{K_0^r}(m)$ de K_0^r et d'une extension abélienne $\mathrm{CM}_{K^r,\Phi^r}(m)$ de K^r, définie dans la Section 2.1.3 et donnée par la théorie CM.

Dans le Chapitre 3, nous réalisons quelques travaux en rapport avec ce résultat de Shimura. Tout d'abord, nous donnons un théorème qui nous fournit un entier m pour lequel le résultat de Shimura est vrai. Ensuite, nous définissons, pour tout entier positif m, le groupe de classes de rayon de Shimura $\mathfrak{C}_K(m)$ d'un corps CM K lié à K^r. En utilisant ce groupe de classes de rayon de Shimura, nous donnons un algorithme qui prend en entrée un entier positif m et qui indique si le corps de classes de Hilbert est oui ou non contenu dans Ξ_m. Cet algorithme nous permet de trouver le plus petit entier positif m pour lequel le résultat de Shimura est vrai.

Le résultat sus-mentionné de Shimura est utile à des fins de calcul car les deux parties du compositum peuvent être explicitement calculées. Au Chapitre 4, nous montrons comment calculer l'extension abélienne $\mathrm{CM}_{K^r,\Phi^r}(m)$. Les corps de classes de rayon des corps reéls quadratiques, tels que $H_{K_0^r}(m)$, peuvent être calculés efficacement en pratique, et nous citons les articles pertinents dans l'introduction du chapitre.

Afin de rendre la théorie ci-dessus vraiment explicite, nous avons mis en oeuvre la plupart des algorithmes discutés dans cette thèse.

L'algorithme pour calculer le groupe de classes de rayon de Shimura utilise des algorithmes pour calculer des noyaux, des images, des quotients et des extensions de groupes abéliens finiment engendrés et les morphismes entre eux. Ces algorithmes sont connus et se trouvent dans [6, Chapter 4]. Dans le Chapitre 5, nous reformulons ces algorithmes en détail en relevant soigneusement lesquelles des informations sont nécessaires pour calculer tel ou tel groupe.

À notre connaissance, ces algorithmes n'ont éte implantés en tant que fonction intégrée dans aucun logiciel de calcul formel. Par conséquent, nous avons mis en œuvre ces algorithmes et nous les avons rendus disponibles sous la forme de deux scripts PARI/GP [21] – `fgag.gp` et `fgagshimuray.gp`. Le premier script implant les algorithmes requis trouvés dans [6] et le second utilise le premier pour implanter l'algorithme qui calcule le groupe de classes de rayon de Shimura.

Nous utilisons notre code et d'autres fonctions intégrées à PARI/GP et SAGE pour montrer comment fonctionne notre méthode de construction de corps de classes. Au Chapitre 6, nous donnons explicitement des exemples utilisant notre algorithme issu de la théorie CM, nous comparons les performances de notre méthode par rapport aux algorithmiques génériques bien connus reposant sur la théorie de Kummer, et nous discutons les limites des deux approches.