Complex multiplication constructions of abelian extensions of quartic fields

Asuncion, J.G.

Introduction

The Kronecker-Weber Theorem is a classical result in number theory. It is a statement concerning *abelian extensions*, Galois extensions of a number field with abelian Galois group.

> **Theorem 0.1** (Kronecker-Weber Theorem)**.** Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$ with $\zeta_m = \exp(2\pi i/m)$ for some $m \in \mathbb{Z}_{>0}$.
>
> The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ via the map
>
> $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a + m\mathbb{Z} &\mapsto (\zeta_m \mapsto \zeta_m^a).\end{aligned}$$

This theorem, combined with Galois theory, tells us that every abelian extension of $\mathbb{Q}$ can be expressed as $\mathbb{Q}(\boldsymbol{\alpha})$ where $\boldsymbol{\alpha}$ is a polynomial in an mth root of unity for some positive integer m. For example, the abelian extension

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

is contained in the cyclotomic field $\mathbb{Q}(\zeta_9)$. Indeed, the field L is equal to

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

While L is also contained in other cyclotomic fields $\mathbb{Q}(\zeta_n)$ for other positive integers n, the integer 9 is the smallest integer satisfying this condition. Such an integer is called the *conductor of the extension* $L/\mathbb{Q}$.

The twelfth of Hilbert's 23 problems, also known as Kronecker's Jugendtraum[1], asks to

[1] Kronecker's dream of his youth

find an analogue of the Kronecker-Weber Theorem when the base field $\mathbb{Q}$ is replaced by another number field.

Class field theory (Section 1.1) tells us that, for every number field K and for every positive integer m there exists a bijection between the set of subgroups of a so-called ray class group $\mathrm{Cl}_K(m)$ of K and the set of abelian extensions L/K of conductor[2] dividing m. However, given a subgroup of $\mathrm{Cl}_K(m)$, the corresponding bijection does not necessarily give an explicit description of the abelian extension.

Not all hope is lost as there exists a case for which an explicit analogue of Theorem 0.1 is known. This is the case where the base field K is an imaginary quadratic number field, instead of Kronecker-Weber's $\mathbb{Q}$. Complex Multiplication (CM) theory (Section 1.2) for elliptic curves provides this analogue. Using CM theory, one may find defining polynomials of any abelian extension of any imaginary quadratic number field K.

A generalization of CM theory to higher dimensional principally polarized abelian varieties was developed by Shimura and Taniyama during the 1950s. Like its elliptic curve counterpart, the theory explicitly describes abelian extensions of so-called CM fields in terms of special values of modular functions. However, the theory does not cover *all* abelian extensions of a CM field hence it does not give an analogue of the Kronecker-Weber theorem on its own.

In this thesis, however, we show that we can use Shimura's CM theory to explicitly compute the largest unramified[3] abelian extension, called the Hilbert class field, of *any* primitive quartic CM field. With this thesis, we hope to encourage further exploration on how to utilize CM theory to advance research on abelian extensions.

This thesis is divided into the following chapters.

In Chapter 1, we review how CM theory is used to find all abelian extensions of an imaginary quadratic number field. In Chapter 2, we review the more general CM theory.

An adaptation of Shimura's [30, Theorem 2] shows that for some positive integer m, the Hilbert class field $H_{K^r}(1)$ of a primitive quartic CM field K^r with real quadratic subfield K_0^r is contained in the compositum Ξ_m of the ray class field $H_{K_0^r}(m)$ of K_0^r

[2] See the definition of conductor on page 22

[3] An abelian extension is unramified if and only if its conductor is 1.

and an abelian extension $\mathrm{CM}_{K^r,\Phi^r}(m)$ of K^r, defined in Section 2.1.3, given by CM theory.

In Chapter 3, we do several things related to this result of Shimura. First, we prove a theorem that gives us an integer m for which Shimura's result is true. Then we define, for every positive integer m, the Shimura ray class group $\mathfrak{C}_K(m)$ of a CM field K related to K^r. Using this Shimura ray class group, we give an algorithm, which takes as input a positive integer m' and outputs whether or not the Hilbert class field is contained in $\Xi_{m'}$. This algorithm enables us to find the smallest positive integer m for which Shimura's result is true.

The aforementioned result of Shimura is useful for computational purposes because both parts of the compositum can be explicitly computed. In Chapter 4, we show how to compute the abelian extension $\mathrm{CM}_{K^r,\Phi^r}(m)$. Ray class fields of real quadratic fields, such as $H_{K_0^r}(m)$, can be computed efficiently in practice and we cite the relevant articles in the introduction of the chapter.

In order to make the above theory really explicit, we have implemented most of the algorithms discussed in this thesis.

The algorithm to compute the Shimura ray class group uses algorithms to compute kernels, images, quotients and group extensions involving finitely generated abelian groups and morphisms between them. These algorithms are known and found in [6, Chapter 4]. In Chapter 5, we restate these algorithms in detail, carefully taking note of which information is needed to compute which groups.

To our knowledge, these algorithms have not been implemented as built-in functions in any computer algebra system. Hence, we have implemented these algorithms and made them available as a pair of PARI/GP [21] scripts – `fgag.gp` and `fgagshimuray.gp`. The former implements the required algorithms found in [6, Chapter 4] and the latter uses the former to implement the algorithm which computes the Shimura ray class group.

We use our code and other built-in functions from PARI/GP [21] and SAGE [27] in order to show how our method of constructing CM fields works. In Chapter 6, we give explicit examples using our CM theory algorithm, compare how our method fares against the well-known generic Kummer theory algorithms, and discuss the limitations of both approaches.