EXPLICIT CLASS FIELD THEORY: COMPLEX MULTIPLICATION

GEORGE MITCHELL

In this report we develop the theory of complex multiplication and sketch proofs of the main theorems. We then look at applications of the theorems. Analogous to how the theory of cyclotomic fields provide an explicit description of abelian extensions of $\mathbb{Q}$, the theory of complex multiplication provides an explicit description of abelian extensions for K, an imaginary quadratic extension of $\mathbb{Q}$. Our main references are [1] and [2].

1. Introduction

Our main goals are to understand and apply the following theorems:

Theorem (Main Theorem of CM, Part I)**.** *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let E be an elliptic curve with complex multiplication by $\mathcal{O}$. Then the j-invariant $j(E)$ is an algebraic number and $K(j(E))$ is the ring class field of $\mathcal{O}$.*

The main application of this theorem will be when $\mathcal{O} = \mathcal{O}_K$, the ring of integers of K. In that case, the theorem gives an explicit construction of the Hilbert Class Field of K.

Theorem (Main Theorem of CM, Part II)**.** *Let K be a imaginary quadratic field and let E be an elliptic curve with complex multiplication by K. Let $h : E \to \mathbb{P}^1$ be a Weber function for E. Then $K^{ab} = K(j(E), h(E_{tors}))$.*

This result gives an explicit description of the maximal abelian extension of K. The next few sections will be dedicated to defining the required terms in the above theorems and then sketching proofs of both.

This is analogous to the case with cyclotomic fields, as follows. For $\mathbb{Q}$, it is known that $\mathbb{Q}^{ab} = \cup_N \mathbb{Q}(\zeta_N)$, that is, we adjoin to $\mathbb{Q}$ all roots of unity. This is the famous Kronecker-Weber Theorem. We can view these roots of unity as torsion values of an analytic function, namely they are values of $e^{2\pi iz}$ evalutated at $1/N$ for positive integers N.

What the above theorems show, is that for $K/\mathbb{Q}$ quadratic imaginary, we can find a suitable analytic function such that adjoining torsion values of this function to K will generate all abelian extensions. In our case, we simply have to adjoin $j(E)$ and also $h(E_{\text{tors}})$. As we will see later, the Weber function at these points is essentially the x-coordinate of the torsion point (except in two cases). If we were to adjoin all torsion points of E, and not just the x-coordinate, then we would obtain abelian extensions of H_K, the Hilbert Class Field, but these are not necessarily abelian over K. Hence the Weber function picks out a suitable subfield.

Date: April 2019.

2. Elliptic Curves, Lattices and Class Field Theory

In this section we define and build the relevant theory in order to understand and prove the two main theorems. In particular, we define the j-invariant for lattices and we give a brief discussion of the ideal-theoretic formulation of Class Field Theory (CFT).

2.1. **Elliptic Curves and Lattices.** Let E be an elliptic curve over $\mathbb{C}$. By Uniformization, we can view $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, for some lattice Λ in the complex plane. An endomorphism $\varphi \in \mathrm{End}(E)$ corresponds to a complex number α such that $\alpha\Lambda \subseteq \Lambda$. In many cases, $\mathrm{End}(E) \cong \mathbb{Z}$, but when the endomorphism ring is stricly larger, one can show that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} := K$ is an imaginary quadratic extension of $\mathbb{Q}$ and that $\mathrm{End}(E) := \mathcal{O}$ is an order in that field. In this case, we say that E *has complex multiplication by* $\mathcal{O}$. If $\mathcal{O} = \mathcal{O}_K$ then we say that E *has complex multiplication by* K.

Given a lattice $\Lambda \subset \mathbb{C}$, we can define an elliptic function on Λ, called the *Weierstrass* $\wp$*-function*:

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

which satisfies the differential equation $\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$, where

$$g_2(\Lambda) := 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad g_3(\Lambda) := 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}.$$

We further define $\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_2(\Lambda)^2$ and finally $j(\Lambda) := 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}$.

If $E/\mathbb{C}$ is an elliptic curve, then $j(E) := j(\Lambda)$, where Λ is the corresponding lattice in the complex plane. It is well known that the j-invariant categorizes elliptic curves up to isomorphism and lattices up to homothety.

If $\tau \in \mathbb{H}$, the complex upper half plane, then we define $j(\tau) := j(\Lambda)$ where $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$.

2.2. **Class Field Theory.** We now want to formulate CFT using ideals. We assume that $\mathcal{O} = \mathcal{O}_K$. Let Cl_K be the class group of $\mathcal{O}_K$ and let El_K be the set of $\mathbb{C}$-isomorphism classes of elliptic curves with complex multiplication by K. Then for a non-zero fractional ideal $\mathfrak{a}$ of K, the operation:

$$[\mathfrak{a}] \star E_\Lambda := E_{\mathfrak{a}^{-1}\Lambda}$$

is a well defined action of Cl_K on El_K. In fact, the action is simply transitive (see [[2], II.1]). Thus we see that $|El_k| = |Cl_K| < \infty$.

There is a natural action of $G = \mathrm{Gal}(\bar{K}/K)$ on El_K where $\sigma \star E := E^\sigma$. But since the action of Cl_K is simply transitive, it follows that there is a unique $[\mathfrak{a}] \in Cl_K$, depending on σ, such that $[\mathfrak{a}] \star E = E^\sigma$. In this way we get a well defined homomorphism

$$F : G \to Cl_K$$

characterized by the property that $E^\sigma = F(\sigma) \star E$ for all $\sigma \in G$. It is a nontrivial fact that this map does not depend on the representative $E \in El_K$ we chose.

Now let L/K be a finite abelian Galois extension, let $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_K$ that is divisible by all the ramified primes. We make the following definitions:

$$\begin{aligned} I(\mathfrak{c}) &= \text{group of fractional ideals of } K \text{ coprime to } \mathfrak{c}. \\ P(\mathfrak{c}) &= \{(\alpha) \mid \alpha \in K^\times,\ \alpha \equiv 1 \bmod \mathfrak{c}\} \\ E[\mathfrak{c}] &= \{P \in E \mid [\gamma]P = 0 \text{ for all } \gamma \in \mathfrak{c}\}. \end{aligned}$$

Let $\sigma_\mathfrak{p}$ be the unique *Frobenius* element over the prime $\mathfrak{p} \subset \mathcal{O}_K$ in $\mathrm{Gal}(L/K)$. We can define the *Artin map*

$$\begin{aligned} (\cdot, L/K) : I(\mathfrak{c}) &\longrightarrow \mathrm{Gal}(L/K) \\ (\mathfrak{a}, L/K) = (\prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}, L/K) &\longmapsto \prod_\mathfrak{p} \sigma_\mathfrak{p}^{n_\mathfrak{p}}. \end{aligned}$$

Then CFT gives the following "weak" version of Artin Reciprocity, which is all that we will require.

Theorem 2.1. *There exists an integral ideal $\mathfrak{c} \subset \mathcal{O}_K$, divisible by precisely primes that ramify in L/K, such that $((\alpha), L/K) = 1$ for all $\alpha \in K^\times$, with $\alpha \equiv 1$ mod $\mathfrak{c}$.*

There is a largest ideal $\mathfrak{c}_{L/K}$ for which the above theorem is true, which we call the *conductor* of L/K. We finally quote a proposition that characterizes the map F earlier described, essentially showing that for half of the Frobenius elements, the map F is an inverse to the Artin map.

Proposition 2.2. *There is a finite set of rational primes $S \subset \mathbb{Z}$ such that if $p \notin S$ is a prime that splits in K, say $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ then $F(\sigma_\mathfrak{p}) = [\mathfrak{p}]$ in Cl_K.*

3. Main Theorem of CM, Part I

We can now prove the first main theorem, restated here for completeness.

Theorem 3.1. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let E be an elliptic curve with complex multiplication by $\mathcal{O}$. Then the j-invariant $j(E)$ is an algebraic number and $K(j(E))$ is the ring class field of $\mathcal{O}$.*

Proof. We prove the theorem in the case that $\mathcal{O} = \mathcal{O}_K$, the ring of integers of K.

We first prove that $j(E) \in \bar{\mathbb{Q}}$. To this end, let $\sigma \in \mathrm{Aut}(\mathbb{C})$. It is clear that $j(E^\sigma) = j(E)^\sigma$ and that $\mathrm{End}(E^\sigma) = \mathcal{O}_K$. Since El_K is a finite set, and each isomorphism class therein is determined by its j-invariant, we have that $j(E)^\sigma$ takes on finite values as σ varies. Hence $[\mathbb{Q}(j(E)) : \mathbb{Q}] < \infty$, and $j(E)$ is algebraic over $\mathbb{Q}$.

Now we prove the statement regarding H_K, the Hilbert Class Field of K. We first show that $K(j(E))/K$ is unramified by showing that the conductor is trivial. We then use our knowledge of the conductor to show that in this case, the map F is an isomorphism, which gives the result. Let L be the fixed field of the kernel of

the homomorphism F. Then we have

$$\begin{aligned}\mathrm{Gal}(\bar{K}/L) &= \ker F \\ &= \{\sigma \in G \ : \ F(\sigma) = 1\} \\ &= \{\sigma \in G \ : \ F(\sigma) \star E = E\} \\ &= \{\sigma \in G \ : \ E^\sigma = E\} \\ &= \{\sigma \in G \ : \ j(E^\sigma) = j(E)\} \\ &= \{\sigma \in G \ : \ j(E)^\sigma = j(E)\} = \mathrm{Gal}(\bar{K}/K(j(E)).\end{aligned}$$

This gives that $L = K(j(E))$. This shows that $K(j(E))/K$ is abelian, since F is injective on $\mathrm{Gal}(L/K)$ by definition of L. Let $\mathfrak{c}_{L/K}$ be the conductor and consider the composition

$$I(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot, L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} Cl_K.$$

Then it follows from Proposition 2.2 and use of the Dirichlet Theorem on primes that $F((\mathfrak{a}, L/K)) = [\mathfrak{a}]$ for all $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$. This immediately gives that

$$F(((\alpha), L/K)) = 1$$

for all principal $(\alpha) \in I(\mathfrak{c}_{L/K})$. Injectivity of F gives that $((\alpha), L/K) = 1$ for all $(\alpha) \in I(\mathfrak{c}_{L/K})$. By definition of the conductor we must have that $\mathfrak{c}_{L/K} = (1)$ and thus L/K is unramified. Thus $K(j(E)) \subseteq H_K$. But now, since $\mathfrak{c}_{L/K} = (1)$, we have that $I(\mathfrak{c}_{L/K}) \to Cl_K$ is surjective, and by the above characterisation of F, it follows that F is surjective, thus an isomorphism. Thus

$$[L : K] = |\mathrm{Gal}(L/K)| = |Cl_K| = [H_K : K].$$

Hence $L = H_K$. □

It can actually be shown that in this case, $j(E)$ is an algebraic *integer*. This is proven in three different ways in [[2], II], but was not needed for our purposes.

As an application of this result, lets consider an example given in class.

Example. We want to write $p = x^2 + 14y^2$. In this case $K = \mathbb{Q}(\sqrt{-14})$. Here we have $Cl_K \cong \mathbb{Z}/4\mathbb{Z}$. Then

$$p \text{ splits in } K \iff \left(\frac{-14}{p}\right) = 1.$$

Since Cl_K is not trivial, this criterion is not enough to conclude that $p = x^2 + 14y^2$. However, using the Principal Ideal Theorem, we know that the primes that split in H_K are those which can be written as $x^2 + 14y^2$, so knowing H_K more explicitly is key. Theorem 3.1 gives that $H_K = K(j(\sqrt{-14}))$. In ([1], §14), it is shown that

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right)^3$$

from which it follows that $H_K = K(\sqrt{2\sqrt{2} - 1})$. Knowing H_K so explicitly allows one to conclude that

$$p = x^2 + 14y^2 \iff \left(\frac{-14}{p}\right) \text{ and } (x^2 + 1)^2 \equiv 8 \bmod p \text{ has a solution.}$$

This second condition is related to the minimal polynomial of $\sqrt{2\sqrt{2} - 1}$ and its derivation can be found in [[1], Ch.2].

4. Main Theorem of CM, Part II

In order to define the second main theorem, we require the notion of a Weber function. Incidentally, these Weber functions are also used in the computation of $j(\sqrt{-14})$ from earlier. Weber computed many j-invariants which lead to some very beautiful numerical equations, much like the one quoted above.

We wish to show that the torsion points of an elliptic curve E with complex multiplication by K generate abelian extensions of K. Weber functions are used to pick out the required subfield to make this so.

4.1. **Weber Functions.** Let H_K be the Hilbert Class Field of K and let E be an elliptic curve defined over H_K with CM by K. A *Weber function* is a finite map

$$h : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1.$$

We give an example of a Weber function to illustrate their purpose.

Example. If we write E is the form

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in H_K$$

then we can define a Weber function:

$$h(P) = h(x, y) = \begin{cases} x & \text{if } AB \neq 0, \\ x^2 & \text{if } B = 0, \\ x^3 & \text{if } A = 0. \end{cases}$$

In this example we see that except for the two exceptional cases ($j = 0$ and $j = 1728$) the Weber function just gives the x-coordinate of the point.

One can define a Weber function analytically using $\wp(z, \Lambda)$ in a way that doesn't depend on fields of definiton. This can be found in [[2],II.5].

4.2. **Second Main Theorem.** We can now state the second main theorem of CM.

Theorem 4.1. *Let K be a imaginary quadratic field and let E be an elliptic curve with complex multiplication by K. Let $h : E \to \mathbb{P}^1$ be a Weber function for E. Then $K^{ab} = K(j(E), h(E_{tors}))$.*

Proof. For brevity, we do not prove in detail but instead give a brief overview of how the proof goes. The theorem is a consequence of the following:

Fact: $L = K(j(E), h(E[\mathfrak{c}]))$ is the ray class field of K modulo $\mathfrak{c}$.

This is shown by proving that $(\mathfrak{p}, L/K) = 1$ if and only if $\mathfrak{p} \in P(\mathfrak{c})$ and by using the invariance of h. For a proof of this (very nontrivial) fact see [[2], II.5].

Given this fact, let L/K be a finite abelian extension and let $\mathfrak{c}_{L/K}$ be the conductor. By CFT and the above fact, we have

$$L \subseteq K(j(E), h(E[\mathfrak{c}_{L/K}])).$$

Taking the compositum over all conductors gives that $L \subseteq K(j(E), h(E_{\mathrm{tors}}))$ and then taking the union over all such fields L gives $K^{ab} \subseteq K(j(E), h(E_{\mathrm{tors}}))$.

But the above fact gives that $K(j(E), h(E_{\mathrm{tors}}))$ is a compositum of abelian extensions, and is therefore abelian. This gives the result. □

As an application of the second main theorem, we consider an example in the special case that K has class number 1.

Example. One can show that E_{tors} generates abelian extensions of H_K, but not necessarily of K, that is why the Weber function is necessary. However, if K has class number 1, then we have that $H_K = K$ and

$$K^{ab} = H_K(h(E_{\text{tors}})) \subset H(E_{\text{tors}}) \subset H^{ab} = K^{ab}.$$

Thus if K has class number 1 then $K^{ab} = K(E_{\text{tors}})$. The j-invariants of these elliptic curves will be in $\mathbb{Q}$, and in fact $\mathbb{Z}$.

This last result is analogous to the Kronecker-Weber Theorem, whereby the maximal abelian extension of $\mathbb{Q}$ was obtained by adjoining all "torsion" points to $\mathbb{Q}$.

5. A Third Main Theorem of CM

There is a *third* Main Theorem of CM which we state without proof. For this, we fix the following notation:

Let $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}_K$, the ring of integers of a quadratic imaginary field $K/\mathbb{Q}$. Let $\sigma \in \text{Aut}(\mathbb{C})$ and $s \in \mathbb{I}_K$ satisfying $[s, K] = \sigma|_{K^{ab}}$. Finally, fix a complex analytic isomorphism

$$f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$$

where $\mathfrak{a}$ is a fractional ideal of K.

Theorem (Main Theorem of CM, Part III)**.** *There exists a unique complex analytic isomorphism*

$$f' : \mathbb{C}/s^{-1}\mathfrak{a} \longrightarrow E^{\sigma}(\mathbb{C})$$

so that the following diagram commutes:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{s^{-1}} & K/s^{-1}\mathfrak{a} \\ \downarrow f & & \downarrow f' \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^{\sigma}(\mathbb{C}). \end{array}$$

We only say that this theorem is of note because it translates the algebraic action of σ on the torsion subgroup $f(K/\mathfrak{a}) = E_{\text{tors}}$ into the analytic action of multiplication by s^{-1}. The theorem then allows one to associate a *Grossencharacter* to the elliptic curve E, which then has consequences for the L-series of E (see [[2], II.9-II.10]).

References

[1] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, Second Edition, John Wiley and Sons, 2014

[2] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Third Edition, Springer, 2013