# Notes on class field theory and complex multiplication

Kartik Prasanna
University of California, Los Angeles, CA

July 5, 2005

Disclaimer: These notes are in draft form and have not been carefully proofread. Please use at your own risk !

## Contents

# 1 Introduction

These notes are meant to be an introduction to class field theory, the theory of complex multiplication and some aspects of the theory of Shimura curves for participants of a summer school in Hangzhou. There is absolutely nothing original in these notes, either in terms of content or presentation. Indeed, we have often simply copied from standard texts, notably Lang's book for class field theory, and Shimura's books and articles for the rest of the notes. The only virtue of these notes then is (hopefully) that they provide to a beginning student clear statements of the main theorems and motivation to read the more comprehensive books and articles cited.

# 2 Class field theory

## 2.1 Number fields and their completions

### 2.1.1 Number fields, prime ideals

A number field is a finite extension of $\mathbb{Q}$. The ring of integers of $L$, $\mathfrak{o}_L$ is defined to be the subring of $L$ consisting of $x \in L$ that satisfy a monic polynomial with coefficients in $\mathbb{Z}$. $\mathfrak{o}_L$ is an integrally closed integral domain of dimension 1 i.e. all the nonzero prime ideals of $\mathfrak{o}_L$ are maximal. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathfrak{o}_L$. Then $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime number $p$. The prime ideal $\mathfrak{p}$ is said to lie over $p$. Conversely, for any integer prime $p$, the set of prime ideals $\mathfrak{p}$ of $\mathfrak{o}_L$ that lie over $\mathfrak{p}$ is finite. If $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$ denotes the set of these primes, one has

$$p\mathfrak{o}_L = \prod_i \mathfrak{p}_i^{e_{\mathfrak{p}_i}} \tag{1}$$

for some integers $e_{\mathfrak{p}_i}$. If $f_{\mathfrak{p}_i} := [\mathfrak{o}/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ is the degree of the finite field $\mathfrak{o}/\mathfrak{p}_i$ over $\mathbb{F}_p$, one has also

$$[L : \mathbb{Q}] = \sum_i e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}$$

More generally, let $K/L$ be an extension of number fields, and $\mathfrak{p}$ a prime ideal in $\mathfrak{o}_L$. Then the set of primes $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$ of $\mathfrak{o}_K$ lying over $\mathfrak{p}$ (i.e. such that $\mathfrak{p}_i \cap \mathfrak{o}_L = \mathfrak{p}$) is finite. We have

$$\mathfrak{p}\mathfrak{o}_K = \prod_i \mathfrak{p}_i^{e_{\mathfrak{p}_i/\mathfrak{p}}} \tag{2}$$

for some integers $e_{\mathfrak{p}_i/\mathfrak{p}}$, generalising (1) above. If $f_{\mathfrak{p}_i/\mathfrak{p}} := [\mathfrak{o}_K/\mathfrak{p}_i : \mathfrak{o}_L/\mathfrak{p}]$ is the degree of the finite field $\mathfrak{o}_K/\mathfrak{p}_i$ over $\mathfrak{o}_L/\mathfrak{p}$, one has also

$$[K : L] = \sum_i e_{\mathfrak{p}_i/\mathfrak{p}} f_{\mathfrak{p}_i/\mathfrak{p}} \tag{3}$$

generalising (2) above.

**Definition 2.1** *A prime $\mathfrak{p}$ in $L$ is said to be ramified in $K$ if $e_{\mathfrak{p}_i/\mathfrak{p}} > 1$ for some $\mathfrak{p}_i$ lying over $\mathfrak{p}$.*

It is known that only finitely many primes of $L$ ramify in $K$. In fact one may define an ideal in $L$ called the discriminant ideal $\mathfrak{d}_{K/L}$ such that $\mathfrak{p}$ ramifies in $K$ if and only if $\mathfrak{p}|\mathfrak{d}_{K/L}$. $\mathfrak{p}$ is said to be unramified in $K$ if it is not ramified.

### 2.1.2 Fractional Ideals

A fractional ideal $\mathfrak{a}$ in $L$ is an $\mathfrak{o}_L$-submodule of $L$, such that $x\mathfrak{a} \subseteq \mathfrak{o}_L$ for some $x \in L^\times$. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals,

$$\mathfrak{a}\mathfrak{b} := \{\sum_i a_i b_i, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\} \tag{4}$$

is also a fractional ideal. Likewise, if $\mathfrak{a} \neq 0$,

$$\mathfrak{a}^{-1} = \{\alpha \in L, \alpha\mathfrak{a} \subseteq \mathfrak{o}_L\} \tag{5}$$

is also a fractional ideal. The set of fractional ideals in $L$ then forms a group under the multiplication law (4), with inverses being defined as in (5). We denote this group by the symbol $I_L$ or just by $I$ if the field $L$ is fixed. Associated to every $\alpha \in L$ is the principal fractional ideal $(\alpha) := \alpha\mathfrak{o}$. Since $(\alpha)(\beta) = (\alpha\beta)$ and $(\alpha)^{-1} = (\alpha^{-1})$, the set of principal fractional ideals forms a subgroup $P$ of $I$.

**Theorem 2.2** *(Unique factorization) Every fractional ideal $\mathfrak{a}$ factors uniquely as*

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i}$$

*for some set of distinct prime ideals $\mathfrak{p}_i$ and non-zero integers $n_i$.*

**Theorem 2.3** *The quotient group $I/P$ is finite.*

$I/P$ is called the class group of $L$.

### 2.1.3 Completions

There are two kinds of completions that one wishes to study corresponding to two different kinds of metrics (places) on $L$. Let us denote $\mathfrak{o}_L$ just by the symbol $\mathfrak{o}$.

**Non-archimedean places.** Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathfrak{o}$. One may define on $L$ a norm $|\cdot|_\mathfrak{p}$ in the following way:

$$|a|_\mathfrak{p} = (\frac{1}{p^{1/e_\mathfrak{p}}})^{v_\mathfrak{p}(a)} \tag{6}$$

where $v_\mathfrak{p}(a)$ is defined to be the largest integer $m$ such that $a \in \mathfrak{p}^m$. Let $L_\mathfrak{p}$ denote the completion of $L$ for the metric defined by $|\cdot|_\mathfrak{p}$. Then $L \subseteq L_\mathfrak{p}$ and the norm $|\cdot|_\mathfrak{p}$ extends naturally to a norm on $L_\mathfrak{p}$, also denoted by the same symbol $|\cdot|_\mathfrak{p}$. $L_\mathfrak{p}$ is a topological field with respect to the associated metric. Let $\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{p}^i\mathfrak{o}_\mathfrak{p}$ denote the closures of $\mathfrak{o}$ and $\mathfrak{p}^i$ in $L_\mathfrak{p}$ respectively. Then $\mathfrak{o}_\mathfrak{p}$ is a topological ring in which $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$ is the unique nonzero prime ideal and $\mathfrak{p}^i\mathfrak{o}_\mathfrak{p} = (\mathfrak{p}\mathfrak{o}_\mathfrak{p})^i$. The ideal $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$ is principal and every non-zero ideal in $\mathfrak{o}_\mathfrak{p}$ is a power of $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$. In other words, $\mathfrak{o}_\mathfrak{p}$ is a discrete valuation ring with maximal ideal $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$. The formula (6) continues to hold for $a \in L_\mathfrak{p}$, except that $v_\mathfrak{p}(a)$ must now be defined to be the largest integer $m$ such that $a \in \mathfrak{p}^m\mathfrak{o}_\mathfrak{p}$.

The additive group $(L_\mathfrak{p}, +)$ is locally compact, and the filtration of additive subgroups $\ldots \subseteq \mathfrak{p}^{i+1}\mathfrak{o}_\mathfrak{p} \subseteq \mathfrak{p}^i\mathfrak{o}_\mathfrak{p} \subseteq \ldots$ gives a fundamental system of compact open neighborhoods of 0. Let $U_\mathfrak{p}$ denote the units of $\mathfrak{o}_\mathfrak{p}$ i.e. $U_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \backslash \mathfrak{p}\mathfrak{o}_\mathfrak{p}$. Define $U_{\mathfrak{p},i} = 1+\mathfrak{p}^i\mathfrak{o}_\mathfrak{p}$. Each $U_{\mathfrak{p},i}$ is a multiplicative subgroup of $L_\mathfrak{p}^\times$. The multiplicative group $L_\mathfrak{p}^\times$ is also locally compact, with the filtration $\ldots \subseteq U_{\mathfrak{p},i+1} \subseteq U_{\mathfrak{p},i} \subseteq \ldots$ being a fundamental system of open neighborhoods of 1.

**Archimedean places.** These correspond to metrics obtained by embedding $L$ in $\mathbb{C}$ and restricting the usual absolute value on $\mathbb{C}$. The number of distinct embeddings of $L$ in $\mathbb{C}$ is well known to equal the degree $[L : \mathbb{Q}]$. An embedding $\sigma$ is said to be real if $\sigma(L) \subseteq \mathbb{R}$ and imaginary otherwise. The imaginary embeddings clearly occur in pairs of complex conjugate embeddings that induce the same absolute value. Thus if $r$ is the number of real embeddings and $2s$ the number of imaginary embeddings, there are $r + s$ distinct metrics thus obtained. Correspondingly the completions $L_\sigma = \mathbb{R}$ for the real embeddings and $= \mathbb{C}$ for the imaginary ones.

We denote by $\Sigma_{L,f}$ (resp. $\Sigma_{L,\infty}$, resp. $\Sigma_L$) the set of non-archimedean places (resp. the set of archimedean places of $L$, resp. the set of all places) of $L$.

### 2.1.4 Adeles and ideles

For many purposes it turns out to be useful to bundle together all the completions of a number field $L$ into a single object, called the adele ring of $L$.

**Definition 2.4** *The Adele ring of $L$, denoted $\mathbb{A}_L$, is defined to be the subring of $\prod_{v\in\Sigma_L} L_v$ consisting of those $(a_v)_{v\in\Sigma_L}$ such that $a_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}$ for almost all $\mathfrak{p} \in \Sigma_{L,f}$ (i.e. for all but finitely many $\mathfrak{p}$.) We also denote by $\mathbb{A}_{L,f}$ the subring of $\mathbb{A}_L$ consisting of those $(a_v)_{v\in\Sigma_L}$ such that $a_\sigma = 1$ for all $\sigma \in \Sigma_{L,\infty}$ and $\mathbb{A}_{L,\infty}$ the subring of $\mathbb{A}_L$ consisting of those $(a_v)_{v\in\Sigma_L}$ such that $a_\mathfrak{p} = 1$ for all $\mathfrak{p} \in \Sigma_{L,f}$.*

Addition and multiplication on $\mathbb{A}_L$ is defined component-wise. It will also be important to put a topology on $\mathbb{A}_L$ in the following way. For each finite subset $S \subseteq \Sigma_L$ containing $\Sigma_{L,\infty}$, define $\mathbb{A}_{L,S}$ to be the subring of $\mathbb{A}_L$ consisting of those $(a_v)_{v\in\Sigma_L}$ such that $a_\mathfrak{p} \in \mathfrak{o}_\mathfrak{p}$ for $\mathfrak{p} \notin S$. Since $\mathbb{A}_{L,S} = \prod_{\mathfrak{p}\notin S} \mathfrak{o}_\mathfrak{p} \times \prod_{v\in S} L_v$, and each $\mathfrak{o}_\mathfrak{p}$ is compact, we can make $\mathbb{A}_{L,S}$ into a locally compact group by giving it the product topology. Now we make $\mathbb{A}_L$ into a topological group by declaring each $\mathbb{A}_{L,S}$ to be an open subgroup. One may check that with this definition $\mathbb{A}_L$ is a topological ring. Note that the topology on $\mathbb{A}_L$ is not the subspace topology inherited from $\prod_{v\in\Sigma_L} L_\sigma$.

Next we consider the unit group of $\mathbb{A}_L$. This is called the idele group of $L$ and is denoted $\mathbb{A}_L^\times$. Likewise we denote the unit group of $\mathbb{A}_{L,S}$ by $\mathbb{A}_{L,S}^\times$. Clearly

$$\mathbb{A}_L^\times = \{(a_v) \in \prod_{v\in S} L_v^\times : a_\mathfrak{p} \in U_\mathfrak{p} \text{ for almost all } \mathfrak{p} \in \Sigma_{L,f}\} = \bigcup_S \mathbb{A}_{L,S}^\times, \text{ and}$$

$$\mathbb{A}_{L,S}^\times = \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \times \prod_{v\in S} L_v^\times$$

We give $\mathbb{A}_{L,S}^\times$ the product topology and make $\mathbb{A}_L^\times$ into a topological group by ordaining each $\mathbb{A}_{L,S}^\times$ to be an open subgroup. Note that the topology on $\mathbb{A}_L^\times$ is not the subspace topology inherited from $\mathbb{A}_L$.

The multiplicative group $L^\times$ embeds diagonally (and discretely) in $\mathbb{A}_L^\times$, via $\alpha \rightsquigarrow (\ldots, \alpha, \alpha, \alpha, \ldots,)$. We will view $L^\times$ as a subgroup of $\mathbb{A}_L^\times$ via this embedding.

**Definition 2.5** *Let $x \in \mathbb{A}_L^\times$. We associate to $x$ a fractional ideal $\mathfrak{i}(x)$ in $L$ by requiring that $\mathfrak{i}(x)_\mathfrak{p} = \mathfrak{p}^n$ where $v_\mathfrak{p}(x_\mathfrak{p}) = n$.*

Since $x$ is an idele, $v_\mathfrak{p}(x_\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$, so this definition makes sense. $\mathfrak{i}$ is a surjective homomorphism from $\mathbb{A}_L^\times$ to $I$.

### 2.1.5 Cycles

**Definition 2.6** *A cycle in $L$ is a a formal product*

$$\mathfrak{c} = \prod_{\mathfrak{p}\in\Sigma_{L,f}} \mathfrak{p}^{m(\mathfrak{p})} \times \prod_{\sigma\in\Sigma_{L,\infty}} \sigma^{m(\sigma)}$$

*for integers $m(\mathfrak{p})$ and $m(\sigma)$ where all but finitely many of the $m(\mathfrak{p})$ are 0 and $m(\sigma) = 0$ or 1. Here $m(\mathfrak{p})$ (resp. $m(\sigma)$) is called the multiplicity of $\mathfrak{c}$ at $\mathfrak{p}$ (resp. $\sigma$.) We say $v \mid \mathfrak{c}$ if $m(v) > 0$ and $v \nmid \mathfrak{c}$ otherwise.*

Suppose $\mathfrak{c}$ is a cycle in $L$. For each place $v \in \Sigma_L$, we define subgroups $U_v$ and $W_{\mathfrak{c}}(v)$ of $L_v^\times$ as follows. For $v = \mathfrak{p}$ non-archimedean, $U_{\mathfrak{p}}=$ the group of units in $\mathfrak{o}_{\mathfrak{p}}$, $W_{\mathfrak{c}}(\mathfrak{p}) = \{\alpha \in U_{\mathfrak{p}}, \alpha - 1 \in \mathfrak{p}^{m(\mathfrak{p})}\}$. For $v = \sigma$ archimedean, $U_\sigma = L_\sigma^\times$; $W_{\mathfrak{c}}(\sigma) = L_\sigma^\times$ if $m_\sigma(\mathfrak{c}) = 0$ or if $\sigma$ is a complex embedding, $W_{\mathfrak{c}}(\sigma) = \mathbb{R}^+$ if $\sigma$ is real and $m_\sigma(\mathfrak{c}) \geq 0$. Finally we define $W_{\mathfrak{c}}$ and $\mathbb{A}_{L,\mathfrak{c}}^\times$ as follows:

$$\begin{aligned} W_{\mathfrak{c}} &= \prod_{v \in \Sigma_L} W_{\mathfrak{c}}(v) \\ \mathbb{A}_{L,\mathfrak{c}}^\times &= (\prod_{v \mid \mathfrak{c}} W_{\mathfrak{c}}(v) \times \prod_{v \nmid \mathfrak{c}} L_v^\times) \cap \mathbb{A}_L^\times \end{aligned}$$

Note that $W_{\mathfrak{c}}$ is an open subgroup of $\mathbb{A}_L^\times$.

Define $I(\mathfrak{c})$ to be the subgroup of $I$ consisting of fractional ideals $\mathfrak{a}$ that are prime to $\mathfrak{c}$ i.e. $\mathfrak{p} \nmid \mathfrak{a}$ if $\mathfrak{p} \mid \mathfrak{c}$. Likewise, define $P_{\mathfrak{c}}$ to be the subgroup of principal fractional ideals $(\alpha)$ such that $\alpha \in \mathbb{A}_{L,\mathfrak{c}}^\times$. Note that the map $\mathfrak{i}$ defined in the previous section maps $\mathbb{A}_{L,\mathfrak{c}}^\times$ surjectively onto $I(\mathfrak{c})$.

**Theorem 2.7** *The quotient group $I(\mathfrak{c})/P_{\mathfrak{c}}$ is finite*

$I(\mathfrak{c})/P_{\mathfrak{c}}$ may be called a generalized ideal class group.

### 2.1.6 The trace and the norm

For $\alpha \in L$, the trace and norm of $\alpha$, denoted $tr(\alpha)$ and $N(\alpha)$ are defined respectively to be the trace and norm of the linear map $\alpha : L \to L$ given by left multiplication by $\alpha$, where we think of $L$ as a $\mathbb{Q}$ vector space. If $\sigma_1, \ldots, \sigma_n, n = [L : \mathbb{Q}]$, denote the distinct embeddings of $L$ in $\mathbb{C}$, one has

$$Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \qquad N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \tag{7}$$

More generally, if $K/L$ is a finite extension and $\alpha \in K$, we define $Tr_{K/L}(\alpha)$ and $N_{K/L}(\alpha)$ to be the trace and determinant of $\alpha : K \to K$, thinking of $K$ as an $L$-vector space. Similarly, if $v$ is a place of $L$ and $w$ is a place of $K$ lying over $v$, one may define maps $Tr_{K_w/L_v} : K_w \to L_v$ and $N_{K_w/L_v} : K_w \to L_v$. From the description (7) one sees that $Tr$ is an additive homomorphism and $N$ is a multiplicative homomorphism on the multiplicative group of non-zero elements. It is not hard to check then that the trace and norm extend to maps

$$Tr_{K/L} : \mathbb{A}_K \to \mathbb{A}_L, \qquad N_{K/L} : \mathbb{A}_K^\times \to \mathbb{A}_L^\times$$

that are respectively additive and multiplicative continuous homomorphisms.

Finally, let $\mathfrak{b}$ be a fractional ideal in $K$. Then

$$N_{K/L}\mathfrak{b} := \text{the ideal generated by } \{N_{K/L}(x), x \in \mathfrak{b}\}$$

is a fractional ideal in $L$. One has $N_{K/L}(\mathfrak{b}_1\mathfrak{b}_2) = N_{K/L}(\mathfrak{b}_1)N_{K/L}(\mathfrak{b}_2)$. It is easy to check that if $\mathfrak{q}$ is a prime of $K$, $\mathfrak{q} \cap L = \mathfrak{p}$, then $N\mathfrak{q} = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$.

## 2.2 Main theorems of class field theory

Let $L$ be a number field. Class field theory concerns the study of abelian extensions of $L$, i.e. extension fields $K/L$ that are Galois over $L$ with abelian Galois group. The main theorems gives a description of the Galois groups of such extensions purely in terms of objects attached to the base field, namely certain subgroups of the idele group $\mathbb{A}_L^\times$ or equivalently certain generalised ideal class groups of $L$. As a consequence one also gets information on how primes of $L$ split in the extension $K$. Roughly speaking, the way an unramified prime $\mathfrak{p}$ of $L$ splits in a finite abelian extension $K$ (in other words the structure of $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$) depends only on the class of $\mathfrak{p}$ in a certain generalised ideal class group of $L$. This consequence is thus a very general reciprocity law and is called *Artin reciprocity*. Indeed all of the more familiar reciprocity laws (eg. quadratic or cubic reciprocity) may be deduced as corollaries of Artin reciprocity (albeit with some work in each case !)

Our description of the main theorems follows the approach (and some of the notation) of [1], where the reader may also find proofs of all the theorems stated. We start with a description of the Artin map. Suppose $K/L$ is a finite abelian extension with Galois group $G$. Let $\mathfrak{p}$ be a prime of $L$ that is unramified in $K$, and $\mathfrak{q}$ a prime of $K$ lying over $L$. The decomposition group $G_\mathfrak{q} := \{\sigma \in G, \sigma\mathfrak{q} = \mathfrak{q}\}$ is canonically isomorphic to the Galois group $Gal(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$. This latter group has a canonical generator $\bar{\sigma}$ given by $\bar{\sigma}(x) = x^{N\mathfrak{p}}$. If $\sigma$ is the corresponding element of $G_\mathfrak{q} \subseteq G$, then $\sigma$ is independent of the choice of $\mathfrak{q}$ and is denoted by the symbol $(\mathfrak{p}, K/L)$ (also called the *Artin symbol*.) By extending multiplicatively we get a homomorphism called the *Artin map* or *reciprocity map*,

$$rec_{L/K} : I(\mathfrak{d}_{L/K}) \to G$$

where $\mathfrak{d}_{K/L}$ is the relative discriminant of $K/L$. For any fractional ideal $\mathfrak{a} \in I(\mathfrak{d})$, we write $(\mathfrak{a}, L/K)$ for $rec_{L/K}(\mathfrak{a})$.

**Definition 2.8** *A cycle $\mathfrak{c}$ in $L$ is said to be admissible for the extension $K/L$ if $W_\mathfrak{c}(v) \subseteq N_{K_w/L_v}(K_w^\times)$ for all places $w$ of $K$ lying over $v$.*

It is not hard to show that $U_v \subseteq N_{K_w/L_v}(K_w^\times)$ if $w$ is unramified over $v$. Thus any $\mathfrak{c}$ which is sufficiently divisible at the primes ramified in $K/L$ will be admissible for $K/L$.

**Definition 2.9** *Let $\mathfrak{c}$ be a cycle in $L$ and $K/L$ a finite extension. We define $\mathfrak{N}(\mathfrak{c})$ to be the group of fractional ideals in $L$ which are obtained as $N(\mathfrak{b})$ for $\mathfrak{b}$ a fractional ideal in $K$, with $\mathfrak{b}$ prime to $\mathfrak{c}$.*

**Theorem 2.10** *(a) Let $\mathfrak{c}$ be any cycle divisible by all the primes ramified in $L/K$. Then the reciprocity map*

$$rec_{L/K} : I(\mathfrak{c}) \to G \tag{8}$$

*restricted to $I(\mathfrak{c})$ is surjective.*

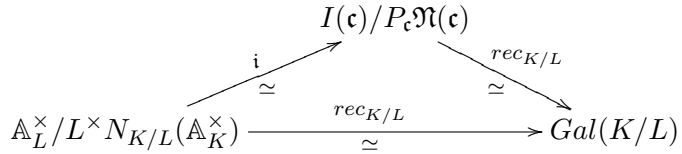
*(b) (Artin reciprocity) There exists an admissible cycle $\mathfrak{c}$ for $L/K$ such that $P_\mathfrak{c}$ is contained in the kernel of the map (8). For such a $\mathfrak{c}$, one has an isomorphism*

$$rec_{L/K} : I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}) \simeq G \tag{9}$$

We now define a map $\varphi : \mathbb{A}_L^\times \to I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c})$ as follows: for $x \in \mathbb{A}_L^\times$, pick (by the approximation theorem) $\alpha \in L^\times$ such that $\alpha x \in \mathbb{A}_{L,\mathfrak{c}}^\times$. Then $\mathfrak{i}(\alpha x) \in I(\mathfrak{c})$. We define $\varphi(x) =$ the image of $\mathfrak{i}(\alpha x)$ in $I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c})$. If $\beta \in L^\times$ is such that $\beta x \in \mathbb{A}_{L,\mathfrak{c}}^\times$, then $\alpha\beta^{-1} \in \mathbb{A}_{L,\mathfrak{c}}^\times \cap L$, hence $\mathfrak{i}(\alpha\beta^{-1}) \in P_\mathfrak{c}$. Thus the class of $\mathfrak{i}(\alpha x)$ in $I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c})$ is independent of the choice of $\alpha$, so $\varphi$ is indeed well defined. Now composing the map $rec_{L/K}$ of (9) with $\varphi$ we get a map, also denoted

$$rec_{L/K} : \mathbb{A}_L^\times \to G \tag{10}$$

**Theorem 2.11** *The map (10) is surjective with kernel $L^\times N_{K/L}(\mathbb{A}_K^\times)$. We thus get isomorphisms*




*Further, if $\mathfrak{p}$ is a prime ideal in $L$, unramified in $K$, $\pi$ is a uniformiser at $\mathfrak{p}$, and $\xi_\pi := (\ldots, 1, 1, \pi, 1, 1, \ldots)$ is the idele whose $\mathfrak{p}$ component is $\pi$ and all whose other components are 1, then*

$$rec_{K/L}(\xi_\pi) = (\mathfrak{p}, K/L) \tag{11}$$

As the field $K$ varies, so does the cycle $\mathfrak{c}$ and the group $I(\mathfrak{c})$. One reason the idele group $\mathbb{A}_L^\times$ is so useful is that we can use it to study all abelian extensions $K$ at one go (and in fact even infinite abelian extensions, as we shall see later.) Further, formulated adelically, it is easy to compare the reciprocity map as the base field $L$ varies. The following two theorems serve to illustrate this point.

**Theorem 2.12** *(Formal properties of the Artin map) (a) Suppose $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the following diagram commutes*

$$\begin{array}{ccc} \mathbb{A}_L^\times / L^\times N_{K/L}(\mathbb{A}_K^\times) & \xrightarrow[\simeq]{rec_{K/L}} & Gal(K/L) \\ \downarrow \sigma & & \downarrow \sigma\cdot\sigma^{-1} \\ \mathbb{A}_{L^\sigma}^\times / (L^\sigma)^\times N_{K^\sigma/L^\sigma}(\mathbb{A}_{K^\sigma}^\times) & \xrightarrow[\simeq]{rec_{K^\sigma/L^\sigma}} & Gal(K^\sigma/L^\sigma) \end{array}$$

*(b) Suppose $L \subseteq K \subseteq K'$. Then the following diagram commutes*

$$\begin{array}{ccc} \mathbb{A}_L^\times / L^\times N_{K'/L}(\mathbb{A}_{K'}^\times) & \xrightarrow[\simeq]{rec_{K'/L}} & Gal(K'/L) \\ \downarrow proj & & \downarrow res \\ \mathbb{A}_L^\times / L^\times N_{K/L}(\mathbb{A}_K^\times) & \xrightarrow[\simeq]{rec_{K/L}} & Gal(K/L) \end{array}$$

*(c) Suppose $K/L$ is abelian and $L'/L$ is a finite extension. Let $K' = KL'$, so that $K'/L'$ is abelian. Then the following diagram commutes*

$$\begin{array}{ccc} \mathbb{A}_{L'}^\times / L'^\times N_{K'/L'}(\mathbb{A}_{K'}^\times) & \xrightarrow[\simeq]{rec_{K'/L'}} & Gal(K'/L') \\ \downarrow N_{L'/L} & & \downarrow res \\ \mathbb{A}_L^\times / L^\times N_{K/L}(\mathbb{A}_K^\times) & \xrightarrow[\simeq]{rec_{K/L}} & Gal(K/L) \end{array}$$

**Theorem 2.13** *Let $\mathcal{H}_K := L^\times N_{K/L}(\mathbb{A}_K^\times)$. The assignment $K \rightsquigarrow \mathcal{H}_K$ gives a bijection between finite abelian extensions $K$ of $L$ and open subgroups of $\mathbb{A}_L^\times$ containing $L^\times$. We say that $\mathcal{H}_K$ belongs to $K$ or that $K$ is the class field corresponding to $\mathcal{H}_K$. This assignment has the following properties (analogous to the main theorem of Galois theory):*

*(a) $\mathcal{H}_K \supseteq \mathcal{H}_{K'} \iff K \subseteq K'$*

*(b) $\mathcal{H}_{KK'} = \mathcal{H}_K \cap \mathcal{H}_{K'}$*

*(c) $\mathcal{H}_{K\cap K'} = \mathcal{H}_K \mathcal{H}_{K'}$*

**Definition 2.14** *(Ray class fields) The class field corresponding to the subgroup $L^\times W_{\mathfrak{c}}$ is called the ray class field of conductor $\mathfrak{c}$.*

Note that any open subgroup $\mathcal{H}$ of $\mathbb{A}_L^\times$ contains $W_{\mathfrak{c}}$ for some $\mathfrak{c}$. Since $W_{\mathfrak{c}_1} \cap W_{\mathfrak{c}_2} = W_{min(\mathfrak{c}_1,\mathfrak{c}_2)}$, there is always a smallest cycle $\mathfrak{c}$ (or equivalently, largest subgroup $W_{\mathfrak{c}}$) such that $\mathcal{H} \supseteq W_{\mathfrak{c}}$. In this case $\mathfrak{c}$ is called the conductor of the Abelian extension $K/L$ corresponding to $\mathcal{H}$.

**Definition 2.15** *(Hilbert class field) The ray class field of conductor* (1) *is called the Hilbert class field of $L$.*

The Hilbert class field is usually denoted by the symbol $H$. It is the maximal everywhere unramified Abelian extension of $L$. From Thm. 2.11 we see that $Gal(H/L) \simeq I/P$, the class group of $L$.

By Thm. 2.12, part (b), we get a well defined homomorphism

$$rec_L : \mathbb{A}_L^\times \to Gal(L^{ab}/L) \tag{12}$$

where $L^{ab}$ denotes the maximal abelian extension of $L$.

**Theorem 2.16** *The homomorphism (12) is surjective. In fact we have an exact sequence*

$$1 \to \overline{L^\times (L_\infty^\times)^+} \to \mathbb{A}_L^\times \xrightarrow{rec_L} Gal(L^{ab}/L) \to 1 \tag{13}$$

## 2.3 Examples

### 2.3.1 Cyclotomic fields and the Kronecker-Weber theorem

Let $m$ be a positive integer, $\zeta_m$ a primitive $m$th root of unity and $K = \mathbb{Q}(\zeta_m)$. Without loss we may assume that $m$ is either odd or a multiple of 4 (since for odd $m$, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. In what follows we omit the subscript $m$ and write just $\zeta$ for $\zeta_m$. It is well known that $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. Indeed one has a natural map from $\psi : (\mathbb{Z}/m\mathbb{Z})^\times \to Gal(K/\mathbb{Q})$ given by $\psi([n])(\zeta) = \zeta^n$ for any integer $n$ coprime to $m$, and this map is an isomorphism. Thus $K$ is an abelian extension of $\mathbb{Q}$. We show now that $\mathcal{H}_K = \mathbb{Q}^\times W_{m\sigma_\infty}$, where $\sigma_\infty$ is the unique archimedean place of $\mathbb{Q}$. In other words, $\mathbb{Q}(\zeta)$ is the ray class field of conductor $m\sigma_\infty$.

We recall some well-known facts about cyclotomic fields that may be found in any basic book on algebraic number theory. The ring of integers $\mathfrak{o}_K = \mathbb{Z}[\zeta]$. A prime $p$ is ramified in $K$ if and only if $p \mid m$. If $p \nmid m$, $f_p$ is equal to the smallest integer $f$ such that $p^f \equiv 1(\mod m)$ i.e. the order of $[p]$ as an element of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Let $p$ be a prime unramified in $K$. Since $(p, K/\mathbb{Q})$ can be characterised as the unique $\sigma \in Gal(K/\mathbb{Q})$ such that $\sigma\mathfrak{p} = \mathfrak{p}$ and $\sigma\zeta \equiv \zeta^p \mod \mathfrak{p}$ for any prime $\mathfrak{p}$ in $K$ over $p$, and since $\psi([p])$ also has this property (why ?), we must have $(p, K/\mathbb{Q}) = \psi([p])$. We now show that $W_{m\sigma_\infty}$ is contained in the kernel of the Artin map. Let $x = (x_v) \in W_{m\sigma_\infty}$. Pick a positive integer $a$ such that for all $p \mid m$, $ax_p \equiv 1(p^{max(n_p, v_p(m))})$ where $\prod_{p|m} p^{n_p}$ is the conductor of $K/\mathbb{Q}$. By the definition of the Artin map, $rec(x) = \psi([a])$. Since $x_p \equiv 1(p^{v_p(m)})$, we have $a \equiv 1(p^{v_p(m)})$. Thus $a \equiv 1(m)$ and $\psi([a]) = 1$ as required, so indeed $\mathbb{Q}^\times W_{m\sigma_\infty} \subseteq \mathcal{H}_K$.

Since $W_{m\sigma_\infty} = \prod_{p\nmid m} \mathbb{Z}_p^\times \times \prod_{p|m}(1 + p^{v_p(m)}\mathbb{Z}_p) \times (\mathbb{R}^+)^\times$ and since $\mathbb{A}_\mathbb{Q}^\times = \mathbb{Q}^\times \cdot (\prod_p \mathbb{Z}_p^\times \times (\mathbb{R}^+)^\times)$, we see that the index of $\mathbb{Q}^\times W_{m\sigma_\infty}$ in $\mathbb{A}_\mathbb{Q}^\times$ is exactly $\phi(m)$, the cardinality of $\prod_{p|m} \mathbb{Z}_p^\times/(1 + p^{v_p(m)}\mathbb{Z}_p) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. On the other hand $[\mathbb{A}_\mathbb{Q}^\times : \mathbb{Q}^\times W_{m\sigma_\infty}] \geq [\mathbb{A}_\mathbb{Q}^\times : \mathcal{H}_K] = \#Gal(K/\mathbb{Q}) = \phi(m)$ by Thm. 2.11. Thus $\mathcal{H}_K = \mathbb{Q}^\times W_{m\sigma_\infty}$.

Now let $K'$ be any abelian extension of $q$. We may pick an integer $m$ such that $\mathcal{H}_{K'} \supseteq W_{m\sigma_\infty}$. By Thm. 2.13, we must have $K' \subseteq \mathbb{Q}(\zeta_m)$. This yields the celebrated

**Theorem 2.17** *(Kronecker-Weber theorem) Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

### 2.3.2 Quadratic fields and quadratic reciprocity

Let $K = \mathbb{Q}(\sqrt{m})$ where $m$ is a square-free integer. The primes ramified in $K$ are exactly those dividing $m$ if $m \equiv 1(4)$ and those dividing $4m$ if $m \equiv 2, 3(4)$. We may identify $Gal(K/\mathbb{Q})$ with the group $\{\pm 1\}$; then for $p$ any prime unramified in $K$, it is easy to see that $(p, K/\mathbb{Q}) = \left(\frac{m}{p}\right)$.

We now show how one might derive (some cases of) quadratic reciprocity from Artin reciprocity. For instance, let us suppose that $m = q$, a prime, $\equiv 1(4)$. Let $K' = \mathbb{Q}(\zeta_q)$. Since $[K' : \mathbb{Q}] = q-1$, $K'$ contains a unique quadratic subfield. This subfield, being unramified outside $q$ (since $K'$ is unramified outside $q$) must be $K$. Thus $cond(K) = q$. Now Artin reciprocity tells us that $(p, K/\mathbb{Q})$ depends only on $p$ modulo the conductor of $K$, i.e. only on $p \mod q$. Thus the Artin symbol gives a surjective homomorphism $rec : (\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\}$, with $rec([a]) = \left(\frac{q}{a}\right)$. If $a \equiv b^2 \mod q$, we have $rec(a) = rec(b)^2 = 1$. Hence the kernel of $rec$ must consist exactly of the square classes mod $q$. In other words $\left(\frac{a}{q}\right) = \left(\frac{q}{a}\right)$ for all $(a, q) = 1$.

# 3 Complex Multiplication

## 3.1 Introduction

In the last section we saw how one can generate class fields of $\mathbb{Q}$ and even the maximal abelian extension by adjoining roots of unity. Now one might think of roots of unity as being special values of the exponential function ($z \rightsquigarrow e^{2\pi i z}$) at points of finite order on the unit circle group. A natural question then is whether one can generate abelian extensions of other fields in a similar manner, by suitable special values of transcendental functions. By the early 20th century, due to the efforts of many mathematicians, this was essentially accomplished for imaginary quadratic fields. In the latter half of the 20th century, beginning with work of Shimura and Taniyama, this theory was generalized to a wider class of fields, called CM fields. It also became the foundation on which the theory of Shimura varieties was built. Our goal now is to describe the statements of main theorems and their consequences, first in the imaginary quadratic case (CM elliptic curves) and then in the general CM case. In

the next section we shall apply these to study the simplest kinds of Shimura varieties, namely Shimura curves.

## 3.2 Imaginary quadratic fields

### 3.2.1 Elliptic curves

We refer the reader to Brian Conrad's talks for the basics of the analytic and algebraic theory of elliptic curves (and later, abelian varieties.) We shall however recall some facts about elliptic curves below, which will also serve the purpose of fixing notation.

We will only be concerned with elliptic curves over fields of characteristic zero and even among those, only fields that can be embedded in the complex numbers. (This is okay since we are only interested in statements of the main results and not proofs. The proofs very much require working over fields of finite characteristic.)

**Definitions:** Recall that an elliptic curve over $\mathbb{C}$ can be equally thought of in any one of the following ways:
A. As $\mathbb{C}/\Lambda$ for $\Lambda$ a lattice in $\mathbb{C}$ i.e. $\Lambda$ is a discrete subgroup of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$.
B. As being the projective curve associated to the affine curve

$$y^2 = 4x^3 - g_2x - g_3, g_2, g_3 \in \mathbb{C} \tag{14}$$

with $\Delta := g_2^3 - 27g_3^2 \neq 0$.
C. As being a projective algebraic curve $E/\mathbb{C}$ that also has the structure of a group variety.

Here is how one goes between these descriptions. To go from A to B, one considers the Weierstrass functions

$$\begin{aligned} \wp(u) : &= \frac{1}{u^2} + \sum_{\omega\in\Lambda,\omega\neq 0} [\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}] \\ \wp'(u) : &= \frac{d}{du}\wp(u) = -\frac{2}{u^3} - \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{(u-\omega)^3} \end{aligned}$$

These are periodic functions with respect to $\Lambda$ with poles of order 2 and 3 respectively at points in $\Lambda$, that satisfy a relation of the form

$$\wp'^2 = 4\wp^3 - g_2(L)x - g_3(L) \tag{15}$$

Then one associates to $\mathbb{C}/\Lambda$ the projective curve $E_L$ associated to the affine curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ in $\mathbb{C}^2$. The map $u \rightsquigarrow (\wp(u), \wp'(u))$ gives a complex analytic isomorphism from $\mathbb{C}/\Lambda$ to $E_L$ sending 0 to the point at infinity, $[0, 1, 0]$, on $E_L$.

To go from B to C, one must define a group law on $E$, given by the equation (14). Let $O$ be the point at infinity, $[0,1,0]$, on $E$. Given points $P$ and $Q$ on $E$, construct the line joining $P$ and $Q$ (or if $P = Q$, take the tangent line to $E$ at $P$.) This line meets $E$ at exactly one other point, say $R$. Next construct the line through $O$ and $R$, which meets $E$ again at exactly one other point, which we define to be the sum $P \oplus Q$. Then one may verify that $\oplus$ is a group law on $E$ with $O$ as the identity element. The constructions involved being clearly algebraic, $E$ is then a group variety.

Finally, to go from C to A, one may consider the tangent space $V$ at the origin $O$ of $E$, and the exponential map $exp : V \to E$ since $E$ has the structure of a compact complex Lie group. One shows that $exp$ is surjective with kernel equal to a lattice $U$ in $V$. Now picking an isomorphism of $V$ with $\mathbb{C}$, $U$ corresponds to a lattice $\Lambda$ in $\mathbb{C}$ and $E \simeq \mathbb{C}/\Lambda$.

**Homomorphisms, isogenies and endomorphisms:** Given two elliptic curves $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$, a homomorphism from $E_1$ to $E_2$ is any complex analytic map from $E_1$ to $E_2$ that is a group homomorphism. It turns out that any complex analytic map from $E_1$ to $E_2$ sending $O_{E_1}$ to $O_{E_2}$ is given by a linear map $u \rightsquigarrow \mu u$ such that $\mu\Lambda_1 \subseteq \Lambda_2$. Equivalently, in terms of definitions $B$ and $C$, a homomorphism from $E_1$ to $E_2$ is an algebraic map that is a group homomorphism. Again, it turns out that any algebraic map that sends the identity to the identity is automatically a group homomorphism.

An isogeny is a homomorphism from $E_1$ to $E_2$ that equivalently, (i) is a non-zero map, (ii) has finite kernel, and (iii) is surjective.

An endomorphism of $E$ is a homomorphism from $E$ to itself. Let $End(E)$ denote endomorphism ring of $E$, where we add endomorphisms by $(\phi+\psi)(x) = \phi(x) + \psi(x)$, and multiply endomorphisms by $(\phi \cdot \psi)(x) = (\phi \circ \psi)(x)$. Also let $End^0(E) = End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. If $E = \mathbb{C}/\Lambda$,

$$\begin{aligned} End(E) &= \{\mu \in \mathbb{C}, \mu\Lambda \subseteq \Lambda\} \\ End^0(E) &= \{\mu \in \mathbb{C}, \mu \cdot (\mathbb{Q}\Lambda) \subseteq (\mathbb{Q}\Lambda)\} \end{aligned}$$

where $\mathbb{Q}\Lambda$ denotes the $\mathbb{Q}$-linear span of $\Lambda$.

### 3.2.2 Elliptic curves with complex multiplication

Clearly, $\mathbb{Z} \subseteq End(E)$ for any elliptic curve $E$.

**Definition 3.1** *An elliptic curve $E/\mathbb{C}$ is said to have complex multiplication (or simply CM) if $End(E) \neq \mathbb{Z}$.*

Now suppose $E = \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_1$ and $\omega_2$ being chosen such that $\omega_1/\omega_2 \in \mathfrak{H}$, the complex upper half plane. Set $z = \omega_1/\omega_2$.

**Proposition 3.2** *E has CM if and only if $\mathbb{Q}(z)$ is an imaginary quadratic field.*

**Proof:** Any non zero element of $End(E)$ is given by $\mu \in \mathbb{C}, \mu \neq 0$ such that $\mu\Lambda \subseteq \Lambda$. Then there exist integers $a, b, c, d$, such that

$$\begin{aligned} \mu\omega_1 &= a\omega_1 + b\omega_2 \\ \mu\omega_2 &= c\omega_1 + d\omega_2 \end{aligned}$$

with $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ being an invertible matrix. Thus $\mu z = az + b, \mu = cz + d$, and $\bar{\mu}\overline{z} = a\overline{z} + b, \bar{\mu} = c\overline{z} + d$. We can write these equations as a single matrix equation

$$\begin{pmatrix} z & \overline{z} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z & \overline{z} \\ 1 & 1 \end{pmatrix}$$

or equivalently

$$\begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} = \begin{pmatrix} z & \overline{z} \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z & \overline{z} \\ 1 & 1 \end{pmatrix}$$

Now two possibilities may occur: if $A$ is a diagonal matrix, then $\mu = \bar{\mu}$ and necessarily $\mu \in \mathbb{Z}$. If $A$ is not diagonal, then either $c \neq 0$ or $b \neq 0$. In either case, $\mu \neq \bar{\mu}$, since $\mu = cz + d = a + b/z$ and hence in fact both $b, c \neq 0$. Thus $\mu \notin \mathbb{R}$. Since $\mu$ satisfies the polynomial $(X - \mu)(X - \bar{\mu}) =$ char. polynomial of $A$, $\mu$ generates an imaginary quadratic field $K$ over $\mathbb{Q}$, and $\mathbb{Q}(z) = \mathbb{Q}(\mu) = K$. This proves one direction, namely, if $E$ has CM, then $\mathbb{Q}(z)$ is imaginary quadratic.

In the other direction, suppose $\mathbb{Q}(z)$ is imaginary quadratic. Then $\mathbb{Q}\Lambda = \mathbb{Q}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_2(\mathbb{Q}z + \mathbb{Q}) = \omega_2 K$. Thus

$$End^0(E) = \{\mu \in \mathbb{C}, \mu\omega_2 K \subseteq \omega_2 K\} = K$$

Hence $End(E) \neq \mathbb{Z}$ and $E$ has CM. $\square$

We see then that to any CM elliptic curve $E/\mathbb{C}$, we have associated an imaginary quadratic field $K$ along with an embedding $i : K \hookrightarrow \mathbb{C}$. Abstractly, $K = End^0(E)$ and $i$ is the embedding induced by the action of $K$ on the tangent space at the origin.

Conversely, let us now start with an imaginary quadratic field $K$ and describe all isomorphism classes of CM elliptic curves $E/\mathbb{C}$ with $End^0(E) \simeq K$. To begin with, we will need some definitions.

**Definition 3.3** *Let $L$ be a number field. A* **$\mathbb{Z}$-lattice** *(or simply lattice) in $L$ is a free $\mathbb{Z}$-submodule of $L$ of rank $= [L : \mathbb{Q}]$. Equivalently, a lattice is a free $\mathbb{Z}$-submodule of $L$ that generates $L$ over $\mathbb{Q}$. An* **order** *in $L$ is a lattice that is also a subring (containing 1.)*

The ring of integers $\mathfrak{o}_L$ is clearly an order. In fact every order in $L$ must be contained in $\mathfrak{o}_L$ (Why?). One can construct other orders in $L$ in the following way. Start with $\mathfrak{a}$, a lattice in $L$, and consider $\mathfrak{o} := \{\mu \in L, \mu\mathfrak{a} \subseteq \mathfrak{a}\}$. Then $\mathfrak{o}$ is an order in $L$. We say that $\mathfrak{o}$ is the order of $\mathfrak{a}$ or that $\mathfrak{a}$ is a **proper $\mathfrak{o}$-ideal**. Of course, in the case $\mathfrak{o} = \mathfrak{o}_L$, the proper $\mathfrak{o}_L$ ideals are just the usual fractional ideals in $L$. It turns out that for an arbitrary order $\mathfrak{o}$ in $L$, one can define an analog of the class group by taking the group of proper $\mathfrak{o}$-ideals $\mathfrak{a}$ modulo the equivalence relation $\mathfrak{a}_1 \sim \alpha\mathfrak{a}_2$ for $\alpha \in L^\times$. The group so obtained is called the **class group of** $\mathfrak{o}$ and can be shown to be finite.

We now return to the discussion about CM elliptic curves $E$ with $End^0(E) \simeq K$. We have seen before that $E \simeq \mathbb{C}/\Lambda = \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \simeq \mathbb{C}/(\mathbb{Z}z + \mathbb{Z})$. Since $K \simeq End^0(E) = \mathbb{Q}(z)$, we see that $E \simeq \mathbb{C}/\mathfrak{a}$ for some lattice $\mathfrak{a}$ in $K$ and some embedding $i : K \hookrightarrow \mathbb{C}$. If $\mathfrak{o} := \{\mu \in K, \mu\mathfrak{a} \subseteq \mathfrak{a}\}$ is the order of $\mathfrak{a}$, we have $End(E) \simeq \mathfrak{o}$. Of course, $\mathfrak{a}$ will depend on the choice of isomorphism $\varphi : K \simeq End^0(E)$. However, since for any $x \in \mathfrak{o}$, $tr(x) = x + \bar{x} \in \mathbb{Z} \subset \mathfrak{o}$, we have $\bar{\mathfrak{o}} = \mathfrak{o}$ and the order $\mathfrak{o}$ associated to $E$ is independent of the choice of isomorphism $\varphi$.

Conversely, let $\mathfrak{o}$ be any order in $K$, $\mathfrak{a}$ a proper $\mathfrak{o}$-ideal and $i : K \hookrightarrow \mathbb{C}$ an embedding of $K$ in $\mathbb{C}$. Then $\mathbb{C}/\mathfrak{a}$ is an elliptic curve with $End(E) \simeq \mathfrak{o}$. It is easy to see that if $\mathfrak{b}$ is another proper $\mathfrak{o}$-ideal, the curves $\mathbb{C}/\mathfrak{a}$ and $\mathbb{C}/\mathfrak{b}$ are isomorphic iff $\mathfrak{a} \sim \mathfrak{b}$. Thus we have

**Proposition 3.4** *Let $\mathfrak{o}$ be any order in $K$. There is a bijection between isomorphism classes of $E/\mathbb{C}$ with $End(E) \simeq \mathfrak{o}$, and equivalence classes of proper $\mathfrak{o}$-ideals $\mathfrak{a}$ in $K$. Thus the number of isomorphism classes of elliptic curves $E$ with $End(E) \simeq \mathfrak{o}$ is equal to the class number of the order $\mathfrak{o}$. In particular, the number of isomorphism classes of elliptic curves $E$ with $End(E) \simeq \mathfrak{o}_K$ is equal to the class number of $K$.*

**Proposition 3.5** *Let $E_1$ and $E_2$ be two CM elliptic curves over $\mathbb{C}$. Then $E_1$ is isogenous to $E_2 \iff End^0(E_1) \simeq End^0(E_2)$.*

Indeed, if $E_1 \simeq \mathbb{C}/\mathfrak{a}$ and $E_2 \simeq \mathbb{C}/\mathfrak{b}$ for some embedding $i : K \hookrightarrow \mathbb{C}$, $\mathfrak{a} \cap \mathfrak{b}$ is also a lattice in $K$ and both $E_1$ and $E_2$ are isogenous to $\mathbb{C}/(\mathfrak{a} \cap \mathfrak{b})$.

### 3.2.3 Idelic actions on lattices

In this section we explain some generalities on lattices and idelic actions on lattices that will be necessary to formulate the main theorem. In the last section we defined $\mathbb{Z}$-lattices in a number field. More generally,

**Definition 3.6** *Let $V$ be a finite dimensional vector space over a number field $\mathbb{Q}$. An $\mathbb{Z}$-lattice (or simply lattice) in $V$ is a finitely generated $\mathbb{Z}$-submodule of $V$ that generates $V$ over $\mathbb{Q}$.*

Note: More generally, one could consider $\mathfrak{o}_L$ lattices in vector spaces $V$ over a number field $L$. All the propositions stated below can then be generalized in the obvious way to this situation.

**Proposition 3.7** *Suppose* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two lattices in* $V$*. Then* $\mathfrak{a}+\mathfrak{b}, \mathfrak{a}\cap\mathfrak{b}$ *and* $\mathfrak{a}\mathfrak{b}$ *are lattices in* $V$*.*

**Proof:** Exercise.

If $\mathfrak{a}$ is a lattice we define $\mathfrak{a}_p$ to be the closure of $\mathfrak{a}$ in $V_p := V \otimes \mathbb{Q}_p$. i.e. $\mathfrak{a}_p = \mathfrak{a} \otimes \mathbb{Z}_p$.

**Proposition 3.8** *Suppose* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two lattices in* $V$*. Then*
*(i) If* $\mathfrak{a} \subseteq \mathfrak{b}$ *and* $\mathfrak{a}_p = \mathfrak{b}_p$ *for all* $p$*, then* $\mathfrak{a} = \mathfrak{b}$*.*
*(ii)* $\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}_p \subseteq \mathfrak{b}_p$ *for all primes* $p$*.*
*(iii)* $\mathfrak{a} = \mathfrak{b} \iff \mathfrak{a}_p = \mathfrak{b}_p$ *for all* $p$

**Proof:** (i) Consider the exact sequence

$$0 \to \mathfrak{a} \to \mathfrak{b} \to (\mathfrak{b}/\mathfrak{a}) \to 0$$

Since $\mathfrak{a}_p = \mathfrak{b}_p$, $(\mathfrak{b}/\mathfrak{a})_p = 0$ for all $p$, hence $\mathfrak{a}/\mathfrak{b} = 0$ and $\mathfrak{a} = \mathfrak{b}$.
(ii) One implication is obvious. In the other direction, let $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$. Then $\mathfrak{b} \subseteq \mathfrak{c}$ and $\mathfrak{b}_p = \mathfrak{c}_p$ for all $p$, hence by part (i) $\mathfrak{b} \subseteq \mathfrak{c}$. i.e. $\mathfrak{b} = \mathfrak{c}$, so $\mathfrak{a} \subset \mathfrak{b}$ as required.
(iii) Apply part (ii) to the inclusions $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{b} \subseteq \mathfrak{a}$. $\square$

**Proposition 3.9** *Suppose* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two lattices in* $V$*. Then* $\mathfrak{a}_p = \mathfrak{b}_p$ *for almost all* $p$*, i.e. for all but finitely many* $p$*. Converely, suppose* $\mathfrak{a}$ *is a lattice and we are given for each* $p$*, a lattice* $\mathfrak{c}_p$ *in* $V_p$ *(i.e. a finitely generated sub-*$\mathbb{Z}_p$ *module that generates* $V_p$ *over* $\mathbb{Z}_p$*) such that for almost all* $p$*,* $\mathfrak{c}_p = \mathfrak{a}_p$*. Then there exists a unique lattice* $\mathfrak{b}$ *in* $V$*, with* $\mathfrak{b}$ *in* $V$ *with* $\mathfrak{b}_p = \mathfrak{c}_p$ *for all* $p$*.*

**Proof:** For the first part, let $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$. Then $\mathfrak{a} \subseteq \mathfrak{c}$, and $\mathfrak{c}/\mathfrak{a}$ has finite order, hence $(\mathfrak{c}/\mathfrak{a})_p = 0$ for all but finitely many $p$. Thus for all but finitely many $p$, $\mathfrak{a}_p = \mathfrak{c}_p$ and likewise $\mathfrak{b}_p = \mathfrak{c}_p$, whence $\mathfrak{a}_p = \mathfrak{b}_p$.

For the second part, we may assume without loss that $\mathfrak{c}_p \subseteq \mathfrak{a}_p$ for all $p$ (by multiplying $\mathfrak{a}$ by a scalar.) Now we can pick an integer $n$ such that $(n\mathfrak{a})_p \subseteq \mathfrak{c}_p$ for all $p$. Thus $(n\mathfrak{a})_p \subseteq \mathfrak{c}_p \subseteq \mathfrak{a}_p$ for all $p$. Now there is a natural isomorphism

$$\psi : \mathfrak{a}/n\mathfrak{a} \simeq \oplus_{p|n} \mathfrak{a}_p/(n\mathfrak{a})_p$$

Let $\mathfrak{b} = \{x \in \mathfrak{a}, \psi([x])_p \in \mathfrak{c}_p \text{ for all } p\}$. Then it is clear that $\mathfrak{b}$ is a lattice with the required property. $\square$

Let us now apply the above in the following situation. Let $K$ be an imaginary quadratic field and consider $K$ as a vector space over $\mathbb{Q}$. Suppose $\mathfrak{a}$ is a lattice in $K$. Let $x \in \mathbb{A}_K^\times$. We wish to define a new lattice which will be called $x\mathfrak{a}$. For each rational prime $p$, consider the $p$ component $x_p \in (K_p)^\times$. Then $x_p\mathfrak{a}_p$ is a $\mathbb{Z}_p$-lattice in $K_p$. For almost all $p$, $x_p$ is a unit in $K_p^\times$, hence $x_p\mathfrak{a}_p = \mathfrak{a}_p$. Then by Prop. 3.9 above, there exists a unique lattice $\mathfrak{b}$ in $K$ with $\mathfrak{b}_p = x_p\mathfrak{a}_p$ for all $p$. We denote such a $\mathfrak{b}$ by the symbol $x\mathfrak{a}$.

We would also like to associate to $x$ a canonical isomorphism from $K/\mathfrak{a}$ to $K/x\mathfrak{a}$. Since

$$\begin{aligned} K/\mathfrak{a} &\simeq \oplus_p K_p/\mathfrak{a}_p, \\ \text{and } K/x\mathfrak{a} &\simeq \oplus_p K_p/(x\mathfrak{a})_p \end{aligned}$$

it suffices to construct a canonical isomorphism from $K_p/\mathfrak{a}_p$ to $K_p/(x\mathfrak{a})_p$ for each $p$. But multiplication by $x_p$ gives such an isomorphism, so we are done. We denote the isomorphism just constructed by the symbol $x$. If $u \in K$, then $x([u]) = [v]$ in $K/x\mathfrak{a}$ where $v \in K$ satisfies $v \equiv x_p u \mod (x\mathfrak{a})_p$ for all $p$.

### 3.2.4 Main theorem for CM elliptic curves

We are now in a position to state the main theorem. Let $E/\mathbb{C}$ be an elliptic curve with CM by $K$, an imaginary quadratic field. By the discussion in a previous section, we can find a $\mathbb{Z}$-lattice $\mathfrak{a}$ in $K$ and an embedding $i : K \hookrightarrow \mathbb{C}$ such that $E \simeq \mathbb{C}/\mathfrak{a}$. Let us fix an isomorphism $\xi : \mathbb{C}/\mathfrak{a} \to E$. Clearly, $\xi$ restricts to an isomorphism $\xi : K/\mathfrak{a} \to E_{tors}$.

Let $\sigma \in Aut(\mathbb{C}/\mathbb{Q})$ and consider the curve $E^\sigma$ (obtained for instance by applying $\sigma$ to the coefficients of any Weierstrass model of $E$.) If $\varphi \in End(E)$, then $\varphi^\sigma \in End(E^\sigma)$ (where $\varphi^\sigma$ may be defined by applying $\sigma$ to the coefficients of the polynomials involved in the description of $\varphi$) and the assignment $\varphi \rightsquigarrow \varphi^\sigma$ gives an isomorphism $End(E) \simeq End(E^\sigma)$. Thus $E^\sigma$ also has CM by $K$. Hence $E^\sigma$ also admits a description as $\xi' : \mathbb{C}/\mathfrak{a}' \simeq E^\sigma$ for a lattice $\mathfrak{a}'$ in $K$. The main theorem is motivated by the following question: can one find such a $\xi'$, in terms of which the action of $\sigma$ on the torsion subgroup admits a particularly simple description ? The following theorem solves this problem for certain $\sigma$, namely those that fix $K$.

**Theorem 3.10** *Suppose $\sigma \in Aut(\mathbb{C}/K)$. Let $s \in \mathbb{A}_K^\times$ be any element such that $rec(s) = \sigma|_{Gal(\bar{K}/K)}$. Then there exists a unique complex analytic uniformization $\xi' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma$ such that $\sigma(\xi(u)) = \xi'(s^{-1}u)$ for all $u \in K/\mathfrak{a}$ i.e. the following diagram commutes*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E_{tors} \subset E \\ \downarrow{\scriptstyle s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E^{\sigma}_{tors} \subset E^{\sigma} \end{array}$$

### 3.2.5 The $j$-invariant, automorphisms and Weber functions

Before we derive consequences of the main theorem, we need to digress a little and review some more basic facts about elliptic curves. We begin with the following proposition for which the reader can find a proof in [2], Prop. 3.1.

**Proposition 3.11** *Suppose $E$ and $E'$ are two elliptic curves given by Weierstrass equations*

$$E : y^2 = 4x^3 - g_2x - g_3 \text{ and } E' : y^2 = 4x^3 - g_2'x - g_3'$$

*Suppose $E$ and $E'$ are isomorphic, and $\lambda : E \to E'$ is an isomorphism. Then there exists an element $\mu \in \mathbb{C}$, such that*

$$g_2' = \mu^4 g_2, g_3' = \mu^6 g_3, \text{ and } \lambda(x, y) = (\mu^2 x, \mu^3 y)$$

The following is an immediate corollary to the proposition.

**Corollary 3.12** *For $E$ given by $y^2 = 4x^3 - g_2x - g_3$, define*

$$j(E) := \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}$$

*Then $j(E)$ depends only on the isomorphism class of $E$. Further $j(E) = j(E') \iff E \simeq E'$.*

Next we consider the automorphism group of $E$. Since $Aut(E)$ = group of units in $End(E)$, if $E$ has no CM, $Aut(E) = \{\pm 1\}$. Even if $E$ has CM by an order $\mathfrak{o}$ in an imaginary quadratic field $K$, the only cases in which $Aut(E) = \mathfrak{o}^\times$ has more than two elements are the following:

(i) $K = \mathbb{Q}(i), \mathfrak{o} = \mathfrak{o}_K, \mathfrak{o}^\times = \{\pm 1, \pm i\}$

(ii) $K = \mathbb{Q}(\omega)$, $\omega$ a primitive cube root of unity, $\mathfrak{o} = \mathfrak{o}_K$, $\mathfrak{o}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.

In each of these cases, the order $\mathfrak{o}$ is the maximal order, which happens to have class number 1. Thus there is a unique curve up to isomorphism of each of the two types (i) and (ii).

**Exercise:** Write down a Weierstrass model in each of the cases (i) and (ii) and identify the extra automorphisms. What are the corresponding $j$-invariants ?

Now define for any elliptic curve given in Weierstrass form, a function on the points of $E$ as follows.

$$\begin{aligned} h(x,y) &= \frac{g_2 g_3}{\Delta} x, \text{ if } E \text{ is not of the type (i) or (ii) above} \\ &= \frac{g_2^2}{\Delta} x^2 \text{ if } E \text{ is of type (i)} \\ &= \frac{g_3}{\Delta} x^3 \text{ if } E \text{ is of type (ii)} \end{aligned}$$

The proof of the following proposition is left as an exercise for the reader.

**Proposition 3.13** *(a) Let $E$ be an elliptic curve given in Weierstrass form. If $t$ and $t'$ are points on $E$, $h(t) = h(t') \iff t' = \lambda(t)$ for $\lambda \in Aut(E)$.*

*(b) Let $E$ and $E'$ be two elliptic curves given in Weierstrass form and $\lambda : E \to E'$ an isomorphism. Then $h_E = h_{E'} \circ \lambda$.*

The function $h(x,y)$ is called a Weber function.

### 3.2.6 Class fields of imaginary quadratic fields as an application of the main theorem

As an application of the main theorem, we now discuss how one can generate abelian extensions of imaginary quadratic fields.

**Theorem 3.14** *Let $E, K, \mathfrak{a}, \xi$ be as in the main theorem, and $h$ the Weber function defined on a Weierstrass model of $E$. Let $u \in K/\mathfrak{a}$(so that $\xi(u) \in E_{tors}$.) Also let $W$ be the open subgroup of $\mathbb{A}_K^\times$ defined by*

$$W = \{s \in \mathbb{A}_K^\times, s\mathfrak{a} = \mathfrak{a}, su = u\} \tag{16}$$

*Then the field $K(j(E), h(\xi(u)))$ is the class field corresponding to the subgroup $K^\times W$ of $\mathbb{A}_K^\times$.*

**Proof** (of Thm. 3.14): Let $F$ be the class field corresponding to the open subgroup $K^\times W$ and $L$ the field $K(j(E), h(\xi(u)))$. Let $\sigma \in Aut(\mathbb{C}/K)$. We show that $\sigma|_F = 1 \iff \sigma|_L = 1$, which in turn implies $F = L$.
(i) $\sigma|_F = 1 \Rightarrow \sigma|_L = 1$.

Since $\sigma|_F = 1$, we may pick $s \in W$ such that $\sigma|_{K^{ab}} = rec(s)$. Thus $s\mathfrak{a} = \mathfrak{a}$ and also $s^{-1}\mathfrak{a} = \mathfrak{a}$. By the main theorem, there is an isomorphism $\xi' : \mathbb{C}/s^{-1}\mathfrak{a} = \mathbb{C}/\mathfrak{a} \to E^\sigma$ making the following diagram commute:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E_{tors} \subset E \\ \downarrow{\scriptstyle s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/\mathfrak{a} & \xrightarrow{\xi'} & E^\sigma_{tors} \subset E^\sigma \end{array}$$

Since $E^\sigma \simeq \mathbb{C}/s^{-1}\mathfrak{a} = \mathbb{C}/\mathfrak{a} \simeq E$, we have $j(E) = j(E^\sigma) = j(E)^\sigma$. Now let $\lambda : E^\sigma \to E$ be the unique isomorphism making the following diagram commute:

$$\begin{array}{ccc} & \mathbb{C}/\mathfrak{a} & \\ {\scriptstyle \xi'}\swarrow & & \searrow{\scriptstyle \xi} \\ E^\sigma & \xrightarrow{\quad\lambda\quad} & E \end{array}$$

Then $h(\xi(u))^\sigma = h((\xi(u))^\sigma) = h(\xi'(s^{-1}u)) = h(\xi'(u)) = h(\lambda(\xi'(u))) = h(\xi(u))$ by two applications of Prop. 3.13 (b). Thus $\sigma|_L = 1$.

(ii) $\sigma|_L = 1 \Rightarrow \sigma|_F = 1$.

Let $s \in \mathbb{A}_K^\times$ such that $rec(s) = \sigma|_{K^{ab}}$, and $\xi'$ be given by the main theorem so that the following diagram commutes.

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\quad\xi\quad} & E_{tors} \subset E \\ \downarrow{\scriptstyle s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\quad\xi'\quad} & E^\sigma_{tors} \subset E^\sigma \end{array}$$

Since $j(E^\sigma) = j(E)^\sigma = j(E)$, $E^\sigma$ is isomorphic to $E$. Hence we can pick an element $\mu \in K^\times$ such that $\mu s^{-1}\mathfrak{a} = \mathfrak{a}$. Let $\lambda$ be the unique isomorphism making the following diagram commute:

$$\begin{array}{ccc} \mathbb{C}/s^{-1}\mathfrak{a} & \xrightarrow{\quad\xi'\quad} & E^\sigma \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \lambda} \\ \mathbb{C}/\mathfrak{a} & \xrightarrow{\quad\xi\quad} & E \end{array}$$

Now $h(\lambda(\xi(u)^\sigma)) = h(\xi(u)^\sigma) = (h(\xi(u)))^\sigma = h(\xi(u))$. Hence there exists $\alpha \in \mathfrak{o}^\times$ such that $i(\alpha) \cdot \lambda(\xi(u)^\sigma) = \xi(u)$ where $i(\alpha)$ denotes the endomorphism defined by $\alpha$. But now, $\lambda(\xi(u)^\sigma) = \lambda(\xi'(s^{-1}u)) = \xi(\mu s^{-1}u)$. Thus $\alpha\mu s^{-1}u = u$. Now setting $s' = \alpha\mu s^{-1}$, we see that $s'\mathfrak{a} = \mathfrak{a}$ and $s'u = u$. Hence $s' \in W$ an consequently $s \in K^\times W = \mathcal{H}_F$. Thus $\sigma|_F = 1$ as required. $\square$

**Corollary 3.15** *Suppose that $E$ above is chosen to have CM by $\mathfrak{o}_K$.*
*(i) Let $\mathfrak{c}$ be an integral ideal in $K$ and let $E[\mathfrak{c}]$ denote the $\mathfrak{c}$-torsion subgroup of $E$. Then the field $K(j(E), h(E[\mathfrak{c}]))$ is the ray class field of $K$ of conductor $\mathfrak{c}$.*
*(ii) $K(j(E), h(E_{tors}))$ is the maximal abelian extension of $K$.*

**Proof:** (i) We may assume that $E \simeq \mathbb{C}/\mathfrak{a}$ for a fractional ideal $\mathfrak{a}$ in $K$. Let $u \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$ be such that $\{\alpha \in \mathfrak{o}_K, \alpha u = 0\} = \mathfrak{c}$. Then it is easy to check that the group $W$ of (16) is nothing but $W_\mathfrak{c}$. Thus $K_\mathfrak{c} = K(j(E), h(\xi(u))) \subseteq K(j(E), h(E[\mathfrak{c}]))$. On the other hand, for every $v \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$,

$$W_\mathfrak{c} \subseteq \{s \in \mathbb{A}_K^\times, s\mathfrak{a} = \mathfrak{a}, sv = v\}$$

hence $K_{\mathfrak{c}} \supseteq K(j(E), h(\xi(v)))$. since this is true for all $v \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$, $K_{\mathfrak{c}} \supseteq K(j(E), h(E[\mathfrak{c}]))$. Thus $K_{\mathfrak{c}} = K(j(E), h(E[\mathfrak{c}]))$ as required.
(ii) Follows immediately from (i).

For $E$ as in the previous corollary we write $j(\mathfrak{a})$ for $j(E)$.

**Corollary 3.16** *For every fractional ideal $\mathfrak{a}$ in $K$, the field $K(j(\mathfrak{a}))$ is the maximal everywhere unramified abelian extension of $K$ i.e. is equal to the Hilbert class field $H$ of $K$. Further for $\sigma \in Gal(H/K)$, if $\sigma = (\mathfrak{b}, H/K)$ for some fractional ideal $\mathfrak{b}$, then*

$$j(\mathfrak{a})^{\sigma} = j(\mathfrak{b}^{-1}\mathfrak{a})$$

## 3.3 CM fields

In this section we explain how the results of the previous section may be generalized to the higher dimensional case.

### 3.3.1 Abelian Varieties

Again, we refer the reader to Brian Conrad's lectures for more details. Here we simply provide a brief overview.

An abelian variety over $\mathbb{C}$ may be thought of equally in any one of the two ways:

(i) As a projective group variety, i.e. a projective variety $A$ equipped with maps $m : A \times A \to A$ and $i : A \to A$ satisfying the usual group axioms.

(ii) As a complex torus $V/U$, where $V$ is a $g$ dimensional $\mathbb{C}$-vector space, $U$ is a lattice in $V$ (i.e. a subgroup of rank $2g$) such that there exists a **positive definite** Hermitian form $H : V \times V \to \mathbb{C}$ that is integral valued on $U$. In this case, we write $E = Im(H)$. $E$ is said to be a Riemann form on $V/U$.

Notice two differences from the definition in the elliptic curve case: firstly in the case $g = 1$, a Hermitian form $H$ with the required properties always exists on any complex torus, but this is not the case for $g > 1$. Secondly, for higher dimensional abelian varieties, there is no nice description using equations unlike the Weierstrass equation for elliptic curves.

The existence of the form positive definite form $H$ is equivalent to the existence of an ample line bundle on $V/U$. Indeed we have

**Proposition 3.17** *For any complex torus $V/U$, there is a bijection between isomorphism classes of line bundles $\mathcal{L}$ on $V/U$ and collections of data consisting of a Hermitian form $H : V \times V \to \mathbb{C}$, such that $E = Im(H)$ is $\mathbb{Z}$-valued on $U$ and a map $\alpha : U \to S^1 = \{z \in \mathbb{C}^{\times}\}, |z| = 1, \alpha(u_1+u_2) = \alpha(u_1)\alpha(u_2)e^{\pi i E(u_1,u_2)}$. We denote the line bundle associated to $H$ and $\alpha$ by the symbol $L(H, \alpha)$. $L(H, \alpha)$ is ample $\iff$ $H$ is positive definite. $L(H, \alpha)$ is topologically trivial $\iff$ $H = 0$.*

Now let us assume that $A = V/U$ is an abelian variety. There is associated to $A$ another abelian variety $\hat{A}$ called the dual abelian variety, whose points parametrize isomorphism classes of line bundles on $A$ that are topologically trivial. $\hat{A}$ is isogenous to $A$ and $\hat{\hat{A}}$ is canonically isomorphic to $A$. To every line bundle $\mathcal{L}$ on $A$, one may attach a map $\phi_{\mathcal{L}} : A \to \hat{A}$, which at the level of points is $x \rightsquigarrow T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, where $T_x$ denotes translation by $x$. $\mathcal{L}$ is said to be non-degenerate if $\phi_{\mathcal{L}}$ is an isogeny. Any ample line bundle is non-degenerate.

**Definition 3.18** *A* **polarization** $\lambda$ *on* $A$ *is an isogeny* $\lambda : A \to \hat{A}$ *such that* $\lambda = \phi_{\mathcal{L}}$ *for some choice of ample* $\mathcal{L}$*.*

Of course $\mathcal{L}$ and $\mathcal{L}'$ could be non-isomorphic line bundles such that $\phi_{\mathcal{L}} = \phi_{\mathcal{L}'}$. This happens precisely when $\mathcal{L}\mathcal{L}'^{-1} \in Pic^0(A)$, the group of topologically trivial line bundles.

A polarization on $A$ gives rise to an involution on $End^0(A)$, via $\phi \rightsquigarrow \lambda^{-1}\phi\lambda$. This involution is called the Rosati involution, and we denote it by the symbol $'$. If $\lambda = \phi_{\mathcal{L}}$ with $\mathcal{L}$ ample and $E$ is the Riemann form associated to $\mathcal{L}$, then $E(\phi x, y) = E(x, \phi' y)$. Note that, by the remarks above, the Riemann form $E$ depends only on the polarization, not the choice of $\mathcal{L}$.

### 3.3.2 CM fields and CM Abelian varieties

**Definition 3.19** *A CM field is a totally imaginary quadratic extension of a totally real number field.*

Let $K$ be a CM field of degree $2g$ over $\mathbb{Q}$ and $F$ its maximal totally real subfield. Denote by $\rho$ the non trivial element of $Gal(K/F)$.

**Definition 3.20** *An abelian variety* $A$ *of dimension* $g$ *is said to have CM by* $K$ *if there exists an embedding* $i : K \hookrightarrow End^0(A)$*.*

It can be shown that in such a case, $i(K)$ is its own centralizer in $End^0(A)$.

Suppose now that $A$ has CM by $K$ and fix an embedding $i : K \hookrightarrow End^0(A)$. Let $\sigma$ denote the representation of $K$ on the tangent space of $A$ at the origin. Then $\sigma \oplus \bar{\sigma}$ is equivalent to the representation of $K$ on $H_1(A, \mathbb{C})$. Since this last representation is defined $/\mathbb{Q}$ and has dimension equal to the degree $[K : \mathbb{Q}]$, it must equal the regular representation of $K$ (tensored up to $\mathbb{C}$.) Thus $\sigma = \sigma_1 \oplus \ldots \oplus \sigma_g$, for some collection $\Phi = \{\sigma_1, \ldots, \sigma_g\}$ of embeddings of $K$ in $\overline{\mathbb{Q}}$ (or $\mathbb{C}$) such that $\{\sigma_1, \ldots, \sigma_g, \sigma_1\rho, \ldots, \sigma_g\rho\}$ is the complete set of embeddings of $K$ in $\mathbb{C}$. We call such a $\Phi$ a CM type of $K$, and in the situation above we say that $\Phi$ is the CM type of the pair $(A, i)$.

Now let $0 \to U \to V \to A \to 0$ be the analytic uniformization of $A$. We may pick a basis of $V$ such that the action of $K$ is by $a \rightsquigarrow d(a^{\sigma_1}, a^{\sigma_2}, \ldots, a^{\sigma_g})$,

so that $V$ is now identified with $\mathbb{C}^g$ and $U$ with a lattice $L$ in $\mathbb{C}^g$. Since the action of $K$ on $\mathbb{Q}L$ is equivalent to the regular representation of $K$, we may pick $w \in \mathbb{Q}L$ such that $\mathbb{Q}L = i(K)w$. Since $\mathbb{R}L = \mathbb{C}^g$, no coordinate of $w$ is 0. Then changing coordinates on $\mathbb{C}^g$ again, we may assume that $\mathbb{Q}L = i(K)$. If $\Phi : K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{C}^g$ is the isomorphism given by $\Phi$ and $\mathfrak{a} = \Phi^{-1}(L)$, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & K \otimes_{\mathbb{Q}} \mathbb{R} & \longrightarrow & (K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{a} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L & \longrightarrow & \mathbb{C}^g & \xrightarrow{\xi} & A & \longrightarrow & 0 \end{array}$$

that realises $A$ as a quotient $(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{a}$ for a lattice $\mathfrak{a}$ in $K$. Conversely, given a CM type $\Phi$ and a lattice $\mathfrak{a}$ in $K$, the complex torus $(K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{a}$ is algebraizable. In fact one has

**Proposition 3.21** *Let $\zeta \in K$ be such that $-\zeta^2 \in F$ and is a totally positive element of $F$, and such that $Im(\zeta^{\sigma_i}) > 0$ for all $i$. Define for $z, w \in \mathbb{C}^g$,*

$$E'(z,w) = \sum_i \zeta^{\sigma_i}(z_i \bar{w}_i - \bar{z}_i w_i)$$

*Then for some integer $g$, $E := gE'$ is a Riemann form on $\mathbb{C}^g/\Phi(\mathfrak{a})$ satisfying*

$$E(ax, y) = E(x, a^\rho y) \tag{17}$$

*for all $a \in K$, and whose associated Hermitian form is positive definite. Conversely all Riemann forms on $\mathbb{C}^g/\Phi(\mathfrak{a})$ satisfying (17) and whose associated Hermitian form is positive definite arise in this way.*

The proposition above shows the existence of (and even classifies) polarizations on $A$ such that the associated Rosati involution on $End^0(A)$ restricts to the involution $\rho$ on $K$. Note that the form $E'$ defined above satisfies

$$E'(\Phi(x), \Phi(y)) = Tr_{K/\mathbb{Q}}(\zeta x y^\rho)$$

for all $x, y \in K$.

To summarize, suppose we are given an abelian variety $A$ with CM by $K$, an embedding $i : K \hookrightarrow End^0(A)$ and a polarization $\lambda$ on $A$ whose associated Rosati involution preserves $K$ and acts as $\rho$ on $K$. Then we may associate to such data $(A, i, \lambda)$ a CM type $\Phi$, an analytic uniformization $\xi : \mathbb{C}^g \to A$, a lattice $\mathfrak{a}$ in $K$ and an element $\zeta \in K$ such that $\xi : \mathbb{C}^g/\Phi(\mathfrak{a}) \simeq A$ and via this isomorphism one has
(i) the embedding $i : K \hookrightarrow End^0(A)$ corresponds to the action of $K$ on $\mathbb{C}^g$ by $\Phi$, and

(ii) the Riemann form $E$ associated to $\lambda$ satisfies

$$E(\Phi(x), \Phi(y)) = Tr_{K/\mathbb{Q}}(\zeta x y^{\rho})$$

for all $x, y \in K$.

We say then that $(A, i, \lambda)$ is of type $(K, \Phi, \mathfrak{a}, \zeta)$ with respect to $\xi$. Clearly the type determines $A$ up to isomorphism. Note that while $K$ and $\Phi$ are uniquely determined by the data $(A, i, \lambda)$, $\mathfrak{a}$, $\xi$ and $\zeta$ are not. However, since $K$ is its own centralizer in $End^0(A)$, the indeterminacy is only up to changing basis in $\mathbb{C}^g$ by the action of an element of $K^{\times}$ i.e. for any $\alpha \in K^{\times}$, we could replace $\mathfrak{a}$, $\xi$ and $\zeta$ by $\mathfrak{a}' = \alpha^{-1}\mathfrak{a}$, $\xi' = \xi \circ \Phi(\alpha), \zeta' = (\alpha\alpha^{\rho})\zeta$.

### 3.3.3 Properties of CM fields : the reflex field

We begin with the following useful proposition.

**Proposition 3.22** *Let $K \subset \mathbb{C}$ be a number field. Then $K$ is a CM field if and only if*
*(i) $\rho$ induces a non-trivial automorphism of $K$ (here $\rho$ is complex conjugation.)*
*(ii) $\rho\tau = \tau\rho$ for all embeddings $\tau : K \hookrightarrow \mathbb{C}$. (Here $\rho\tau$ is defined to be $\tau \circ \rho$.)*

**Proof:** Suppose $K$ satisfies (i) and (ii). Let $F$ be the subfield of $K$ fixed by $\rho$. Then $K/F$ is a quadratic extension. The condition (ii) implies that for every embedding $\tau : K \hookrightarrow \mathbb{C}$, $\tau(K) \not\subset \mathbb{R}$ and $\tau(F) \subset \mathbb{R}$. Thus $F$ is totally real and $K$ is totally imaginary, so $K$ is a CM field. Conversely, if $K$ is a CM field, (i) is obviously true and (ii) follows easily by using that $K = F(\alpha)$ for some element $\alpha$ with $\alpha^2 \in F$. $\square$

**Corollary 3.23** *The composite of two (and hence finitely many) CM fields is a CM field. In particular, the Galois closure of a CM field is a CM field.*

**Proof:** Indeed suppose $K, L$ are CM fields in $\mathbb{C}$. Then (i) and (ii) follow for the field $KL$ since they hold separately for $K$ and for $L$, so $KL$ is a CM field. $\square$

Now suppose $\Phi = \{\sigma_1, \ldots, \sigma_r\}$ is a CM type attached to a CM field $K$ of degree $2r$ over $\mathbb{Q}$. Define

$$N_{\Phi}(x) = \prod_i x^{\sigma_i}, \qquad Tr_{\Phi}(x) = \sum_i x^{\sigma_i}$$

Then define the reflex field of $(K, \Phi)$ to be the field $K^*$ generated by $Tr_{\Phi}(x)$ for all $x \in K$. For any $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$,

**Proposition 3.24** *$K^*$ is a CM field.*

**Proof:** We check that $K^*$ satisfies (i) and (ii) of Prop. 3.22. Firstly, if $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$Tr_\Phi(x)^{\tau\rho} = \sum_i x^{\sigma_i\tau\rho} = \sum_i x^{\rho\sigma_i\tau} = \sum_i x^{\sigma_i\rho\tau} = Tr_\Phi(x)^{\rho\tau}$$

so (ii) is satisfied. Next, note that since $(Tr_\Phi(x))^\rho = Tr_\Phi(x^\rho)$, $\rho$ induces an involution of $K^*$. If this involution is trivial, then $(Tr_\Phi(x))^\rho = Tr_\Phi(x)^\rho$ for all $x$, which is impossible by linear independence of $\Phi \cup \Phi^\rho$. Thus $\rho$ induces a non-trivial involution of $K^*$ as required. $\square$

Next we construct a CM type of $K^*$ called the reflex type. First let $K'$ be the Galois closure of $K$ and let $G$ denote the group $Gal(K'/K)$. Let $H$ and $H^*$ denote the subgroups of $G$ corresponding to $K$ and $K^*$ respectively. Extend each $\sigma_i$ to an embedding of $K'$ in $\mathbb{C}$ and consider union of cosets $S := \cup H\sigma_i$. By linear independence of characters,

$$H^* = \{\gamma \in G, S\gamma = S\}$$

Since for all $\gamma \in H^*$, $\gamma S^{-1} = S^{-1}$, $S^{-1}$ is a union of cosets of $H^*$, say $S^{-1} = \cup_j H^*\tau_j$. Now one can check that $\Phi^* = \{\tau_1, \ldots, \tau_m\}$ is a CM type of the CM field $K^*$, and we call it the reflex type associated to $(K, \Phi)$. Now, since

$$H = \{\gamma \in G, S^{-1}\gamma = S^{-1}\}$$

it follows that $N_{\Phi^*}(x) \in K$ for every $x \in K^*$. In fact, one can show that $N_{\Phi^*}$ can be extended to a continuous homomorphism

$$N_{\Phi^*} : \mathbb{A}_{K^*}^\times \to \mathbb{A}_K^\times$$

### 3.3.4 Examples

### 3.3.5 The main theorem for CM Abelian varieties

We can now state the main theorem as originally given by Shimura and Taniyama.

**Theorem 3.25** *Suppose $(A, i, \lambda)$ is of type $(K, \Phi, \mathfrak{a}, \zeta)$ with respect to $\xi : \mathbb{C}^g \to A$. Let $\sigma \in Aut(\mathbb{C}/K^*)$ and suppose that $s \in \mathbb{A}_{K^*}^\times$ is such that $rec(s) = \sigma|_{K^*}$. Then there exists a unique analytic uniformization $\xi' : \mathbb{C}^g \to E^\sigma$ satisfying*

*(i) $(A^\sigma, i^\sigma, \lambda^\sigma)$ is of type $(K, \Phi, N_{\Phi^*}(s)^{-1}\mathfrak{a}, N_{K^*/\mathbb{Q}}(s\mathfrak{o})\zeta)$ with respect to $\xi'$ (where $\mathfrak{o}$ denotes the ring of integers of $K^*$.)*
*(ii) $(\xi(\Phi(u)))^\sigma = \xi'(\Phi(N_\Phi(s)^{-1}u))$ for all $u \in K/\mathfrak{a}$. i.e. the following diagram commutes*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi\circ\Phi} & A_{tors} \subset A \\ \downarrow{\scriptstyle N_{\Phi^*}(s)^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/N_{\Phi^*}(s)^{-1}\mathfrak{a} & \xrightarrow{\xi'\circ\Phi} & A^\sigma_{tors} \subset A^\sigma \end{array}$$

# References


[1] Lang, Serge *Algebraic number theory*
[2] Silverman, Joseph *The Arithmetic of Elliptic curves*
[3] Shimura, Goro *Introduction to the arithmetic theory of automorphic functions*
[4] Shimura, Goro *Abelian varieties with complex multiplication and Modular functions*