universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

"Shimura Reciprocity and Prime Idèles"

verfasst von / submitted by

Balint Rago, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2022 / Vienna, 2022

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik UG2002
Betreut von / Supervisor:	ao. Univ.-Prof. Dr. Joachim Mahnkopf

Abstract

The aim of this thesis is to provide an understanding of the mechanisms involved in Shimura's reciprocity law. The reciprocity law is a direct consequence of the theory of complex multiplication, which essentially is class field theory for imaginary quadratic number fields. As such, it provides a connection between the norm residue symbol, an important component of class field theory, and the automorphism group of the modular function field. After presenting the necessary concepts, as well as the reciprocity law itself, we will rigorously examine its workings with a certain class of idèles, the so-called prime idèles, and explicitly determine the resulting automorphisms and their actions on modular functions. The benefits of examining prime idèles are twofold. They give rise to a much larger class of idèles and are deeply connected with the Artin symbol, a prominent map in algebraic number theory. Additionally, we will present two concrete applications of Shimura's reciprocity law. The determination of the higher ramification groups of certain ray class fields and the computation of the conjugates of certain elements of ring class fields.

Zusammenfassung

Das Ziel der vorliegenden Arbeit ist es, ein Verständnis der Mechanismen zu liefern, die an Shimuras Reziprozitätsgesetz beteiligt sind. Das Reziprozitätsgesetz ist eine direkte Konsequenz der Theorie der komplexen Multiplikation, die im Wesentlichen Klassenkörpertheorie für imaginär quadratische Zahlkörper ist. Als solches stellt es eine Verbindung zwischen dem Normrestsymbol, einer wichtigen Komponente der Klassenkörpertheorie, und der Automorphismengruppe des modularen Funktionenkörpers her. Nachdem wir die notwendigen Konzepte, sowie das Reziprozitätsgesetz selbst vorgestellt haben, untersuchen wir gründlich seine Funktionsweise mit einer bestimmten Klasse von Idèlen, den sogenannten Primidèlen, und bestimmen explizit die resultierenden Automorphismen und ihre Wirkungen auf Modulformen. Die Untersuchung von Primidèlen hat zwei Vorteile. Sie erzeugen eine weitaus größere Klasse von Idèlen und sind eng mit dem Artin-Symbol, einer wichtigen Abbildung in der algebraischen Zahlentheorie, verbunden. Zusätzlich stellen wir zwei konkrete Anwendungen des Reziprozitätsgesetzes vor. Die Bestimmung der höheren Verzweigungsgruppen gewisser Strahlklassenkörper und die Berechnung der Konjugierten gewisser Elemente von Ringklassenkörpern.

Contents

1 Concepts in Number Theory and Class Field Theory

In this section we will revise some important concepts in algebraic number theory and class field theory. To approach the latter, we will first focus on local class field theory by working with $\mathfrak{p}$-adic number fields, where we will also summarize some properties of the p-adic numbers and integers. Moving on to global class field theory, we will introduce the idèle group and the norm residue map, which are integral components of Shimura's reciprocity law. Moreover, the alternative ideal-theoretic formulation of class field theory will be needed to define ring class fields.

1.1 Algebraic Number Theory

A *number field* K is a finite extension of $\mathbb{Q}$. We call the subring $\mathcal{O}_K \subseteq K$, which contains all $x \in K$, that are roots of monic polynomials with coefficients in $\mathbb{Z}$, *the ring of integers of* K. Some important properties of the ring $\mathcal{O}_K$ are the following.

(i) $\mathcal{O}_K$ is a Noetherian ring

(ii) $\mathcal{O}_K$ is integrally closed

(iii) Every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is a maximal ideal.

Rings satisfying (i)-(iii) are called *Dedekind domains*. The most important property of Dedekind domains is the unique factorization of ideals.

Theorem 1.1. *Any nonzero ideal* $\mathfrak{a}$ *of* $\mathcal{O}_K$ *can be written as a product*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

where the $\mathfrak{p}_i$ *are prime ideals in* $\mathcal{O}_K$ *and* $n_i \in \mathbb{N}$. *This decomposition is unique up to ordering.*

For a proof, see [Neu99, Chapter I, Theorem 3.3]. □

This factorization does not only hold for ideals, but also for certain $\mathcal{O}_K$-submodules of K, called *fractional ideals*. These can be written in the form $x\mathfrak{a}$ for $x \in K$ and an ideal

$\mathfrak{a}$ of $\mathcal{O}_K$.

The collection of all fractional ideals I_K forms a group under multiplication of ideals. This means that for each $\mathfrak{b} \in I_K$ there is an inverse $\mathfrak{b}^{-1} \in I_K$ for which $\mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}_K$. This motivates the following

Theorem 1.2. *Any fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ can be written as*

$$\mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{\ell_i}$$

for prime ideals $\mathfrak{p}_i$ and $\ell_i \in \mathbb{Z}$. This decomposition is unique up to ordering.

For a proof, see [Neu99, Chapter I, Corollary 3.9]. □

For any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we define its *norm* to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. This definition makes sense, since the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. In particular, this means that for a prime ideal $\mathfrak{p}$ the residue field $\mathcal{O}_K/\mathfrak{p}$ is a finite field.

Let K be a number field, $\mathfrak{p}$ a prime of K, i.e. a prime ideal of $\mathcal{O}_K$ and L a finite extension of K. Then L is a number field and $\mathfrak{p}\mathcal{O}_L$ is an ideal of L. We are interested in the decomposition

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_g^{e_g},$$

where the $\mathfrak{P}_i$'s are primes of L, containing $\mathfrak{p}$.

The exponent e_i is called the *ramification index* of $\mathfrak{p}$ in $\mathfrak{P}_i$ and we say that $\mathfrak{p}$ is *unramified* in L if $e_i = 1$ for all i. If $e_i > 1$ for some i, we say that $\mathfrak{p}$ *ramifies* in L.

For any of the primes $\mathfrak{P}_i$, there is a finite extension of residue fields $\mathcal{O}_L/\mathfrak{P}_i/\mathcal{O}_K\mathfrak{p}$ and its degree f_i is called the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{P}_i$. We say that $\mathfrak{p}$ *splits completely* in L if $e_i = f_i = 1$ for all i and $\mathfrak{p}$ is *inert* in L if $g = 1$ and $\mathfrak{p}$ is unramified in L, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$, where $\mathfrak{P}$ is the unique prime of L containing $\mathfrak{p}$.

The integers e_i, f_i and g satisfy the following equality.

Theorem 1.3. *Let e_i, f_i and g be given as above. Then*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

For a proof, see [Neu99, Chapter I, Proposition 8.2]. □

In the case of a Galois extension L, these results become much simpler. The Galois group $\mathrm{Gal}(L/K)$ acts transitively on the primes of L, which contain $\mathfrak{p}$. This implies that $e_i = e_j = e$ and $f_i = f_j = f$ for all i, j. The equality from Theorem 1.3. simplifies to

$$efg = [L : K].$$

The *decomposition group* and *inertia group* of a prime $\mathfrak{P}$ are defined as

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and

$$I_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \mod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}$$

and we immediately see that $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$.

Another important result is the following

Proposition 1.4. *Let L/K be an extension of number fields with $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for an element $\alpha \in \mathcal{O}_L$. Let $\mathfrak{p}$ be a prime of K and let $f(X)$ be the minimal polynomial of α over K, i.e. $f(X) \in \mathcal{O}_K[X]$. If*

$$f \equiv \prod_{i=1}^{g} f_i^{e_i} \mod \mathfrak{p},$$

where the f_i are pairwise distinct and irreducible modulo $\mathfrak{p}$, then we have the decomposition

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where $\mathfrak{P}_i = (\mathfrak{p}, f_i(\alpha))$ are distinct primes of L.

For a proof, see [Neu99, Chapter I, Proposition 8.3]. □

In the following we will restrict to the case of quadratic field extensions $K/\mathbb{Q}$, which can be written uniquely as $K = \mathbb{Q}(\sqrt{n})$ for a squarefree integer n.

Definition 1.5. The *discriminant* d_K of $K = \mathbb{Q}(\sqrt{n})$ is defined as

$$d_K = \begin{cases} n & \text{if } n \equiv 1 \bmod 4 \\ 4n & \text{otherwise} \end{cases}$$

There is a concrete description of the ring of integers of a quadratic field.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\dfrac{1+\sqrt{n}}{2}\right] & \text{if } n \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{n}] & \text{else} \end{cases}$$

Finally, we are interested in the decomposition of prime numbers p in the field K. For an odd prime p and $d \in \mathbb{Z}$, let $\left(\frac{d}{p}\right)$ denote the Legendre symbol. For $p = 2$ we set

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{if } d \equiv 0 \bmod 2 \\ 1 & \text{if } d \equiv 1, 7 \bmod 8 \\ -1 & \text{if } d \equiv 3, 5 \bmod 8. \end{cases}$$

We now give a complete characterisation of the decomposition of prime numbers in K.

Theorem 1.6. *Let K be a quadratic field, $p \in \mathbb{Z}$ a prime and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be the nontrivial automorphism.*

(i) *p is ramified in K, i.e. of the form $p\mathcal{O}_K = \mathfrak{p}^2$ if and only if $\left(\frac{d_K}{p}\right) = 0$.*

(ii) *p splits completely in K, i.e. is of the form $p\mathcal{O}_K = \mathfrak{p}\sigma(\mathfrak{p})$ if and only if $\left(\frac{d_K}{p}\right) = 1$.*

(iii) *p is inert in K, i.e. $p\mathcal{O}_K$ is prime in K, if and only if $\left(\frac{d_K}{p}\right) = -1$.*

For a proof, see [Cox13, Proposition 5.16.]. □

1.2 Completion and p-adic numbers

In the following, we will look at completions of fields with respect to $\mathfrak{p}$-adic norms and their extensions. Later on, this will lead us to the notion of idèles, which are important tools for class field theory and consequently Shimura's reciprocity law. We will also summarize the main properties of the field of p-adic numbers $\mathbb{Q}_p$ and the ring of p-adic integers $\mathbb{Z}_p$.

Let K be a field. A *discrete valuation* is a surjective homomorphism

$$v : K^* \to \mathbb{Z}$$

with the property

$$v(x + y) \geq \min(v(x), v(y))$$

and it is customary to extend v to K by setting $v(0) = \infty$.

Discrete valuations are closely related with *discrete valuation rings*, i.e. principal ideal domains with a single prime ideal. It is easy to show that for a discrete valuation ring R

with unique prime ideal $\mathfrak{p}$ we have

$$R^* = R - \mathfrak{p}.$$

The generating element of $\mathfrak{p} = \varpi R$ is simply called *prime element* and every nonzero element x of R is associate to a power ϖ^n for a nonnegative integer n. Let $v(x)$ denote this unique integer. Extending to the field of fractions K of R, the map v becomes a discrete valuation. In particular, we have

$$R = \{x \in K : v(x) \geq 0\},$$

$$R^* = \{x \in K : v(x) = 0\},$$

$$\mathfrak{p} = \{x \in K : v(x) > 0\}.$$

We can define an *absolute value* on K with respect to the discrete valuation v as follows. For $x \in K^*$

$$\|x\| = a^{v(x)},$$

where a is any real number in the interval $(0, 1)$ and

$$\|0\| = 0.$$

We are interested in the completion $\hat{K}$ with respect to the topology induced by this absolute value, which is independent of the choice of the number a.

Proposition 1.7. *Let K be a field with a discrete valuation v and valuation ring A. Assume that K is complete in the topology induced by v. Let L/K be a finite extension and let B be the integral closure of A in L. Then*

(i) *B is a discrete valuation ring with valuation w.*

(ii) *B is a free A-module of rank $[L : K]$.*

(iii) *L is complete in the topology induced by w.*

For a proof, see [Ser79, Chapter II, §2, Proposition 3]. □

In the setting of number fields, we have the following example.

Let K be a number field and let $\mathfrak{p}$ be a prime of K. Let $x \in K$. Then the fractional ideal $x\mathcal{O}_K$ has a unique decomposition

$$x\mathcal{O}_K = \mathfrak{p}^{\ell} \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i},$$

where all the $\mathfrak{p}_i$ are different from $\mathfrak{p}$. The map $v_\mathfrak{p}(x) = \ell$ defines a discrete valuation. We denote the completion of K with respect to this valuation by $K_\mathfrak{p}$.

Let L/K be a finite extension and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. Let $e_\mathfrak{P}$ and $f_\mathfrak{P}$ be the ramification and inertia indices of $\mathfrak{p}$ in $\mathfrak{P}$ respectively. It is easy to check that for every $x \in K$ we have

$$v_\mathfrak{P}(x) = e_\mathfrak{P} v_\mathfrak{p}(x)$$

and by continuity, this holds for every $x \in K_\mathfrak{p}$, by extending this relation to $L_\mathfrak{P}/K_\mathfrak{p}$. We say that $v_\mathfrak{P}$ *extends* the valuation $v_\mathfrak{p}$ with index $e_\mathfrak{P}$ and one can show that $L_\mathfrak{P}/K_\mathfrak{p}$ is a finite extension of degree $e_\mathfrak{P} f_\mathfrak{P}$. From Theorem 1.3. we obtain

$$\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] = [L : K].$$

Moreover, let $\hat{\mathfrak{p}}$ and $\hat{\mathfrak{P}}$ denote the unique primes in $K_\mathfrak{p}$ and $L_\mathfrak{P}$ respectively. Then $e_{\hat{\mathfrak{P}}} = e_\mathfrak{P}$ and $f_{\hat{\mathfrak{P}}} = f_\mathfrak{P}$.

Assume that L/K is a Galois extension of number fields and let $\mathfrak{P}$ and $\mathfrak{P}'$ be primes dividing $\mathfrak{p}$. Then there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Extending σ continuously, we obtain an isomorphism $L_\mathfrak{P} \cong L_{\mathfrak{P}'}$, which fixes $K_\mathfrak{p}$ pointwise. One can even show that every $K_\mathfrak{p}$-automorphism of $L_\mathfrak{P}$ arises in such a way.

Proposition 1.8. *Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ and $\mathfrak{P}'$ be primes of L dividing $\mathfrak{p}$. Then $L_\mathfrak{P}$ is isomorphic to $L_{\mathfrak{P}'}$. Moreover, the decomposition group $D_\mathfrak{P}$ is isomorphic to* $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$.

For a proof, see [Neu13, Chapter III, pp. 114-115]. □

We can also describe the valuation $v_\mathfrak{P}$ in terms of $v_\mathfrak{p}$.

Proposition 1.9. *For $x \in L_\mathfrak{P}$, we have*

$$v_\mathfrak{P}(x) = \frac{v_\mathfrak{p}(N_{L_\mathfrak{P}/K_\mathfrak{p}}(x))}{f_\mathfrak{P}}.$$

For a proof, see [Ser79, Chapter II, §2, Corollary 4]. □

To conclude, we will give a short summary of the main properties of the p-adic integers $\mathbb{Z}_p$ and the p-adic numbers $\mathbb{Q}_p$ for a prime number p.

Let v_p denote the valuation with respect to the prime number p in $\mathbb{Q}$. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ in the topology induced by v_p. The ring of p-adic integers $\mathbb{Z}_p$ is defined as the valuation ring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ can be

uniquely written as

$$\sum_{i=0}^{\infty} a_i p^i,$$

where $a_i \in \{0, 1, ..., p-1\}$ for all i.

Since $\mathbb{Z}_p$ is a discrete valuation ring, an element $x \in \mathbb{Z}_p$ is a unit if and only if $v_p(x) = 0$, which is equivalent to $a_0 \neq 0$. Otherwise x is contained in the unique prime ideal $p\mathbb{Z}_p$. In particular, p is the unique prime element up to associates.

Since $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$, we have for every element of $\mathbb{Q}_p$ a unique representation

$$\sum_{i=k}^{\infty} a_i p^i,$$

where $a_i \in \{0, 1, ..., p-1\}$ for all i and $k \in \mathbb{Z}$, not necessarily positive.

It is possible to approximate every element of $\mathbb{Z}_p$ arbitrarily close with integers. Indeed, if one takes

$$\sum_{i=0}^{n} a_i p^i,$$

the difference will have an arbitrarily high valuation and thus an arbitrarily low absolute value. The same holds for $\mathbb{Q}_p$ and rational numbers.

An equivalent definition of $\mathbb{Z}_p$ is given by the inverse limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Every element of this inverse limit can be uniquely written as

$$(s_1, s_2, ...) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z},$$

where for every i, j with $i < j$, we have

$$s_j \equiv s_i \mod \mathbb{Z}/p^i\mathbb{Z}.$$

We have a canonical isomorphism

$$\varphi : \mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

$$\sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{0} a_i p^i, \sum_{i=0}^{1} a_i p^i, \sum_{i=0}^{2} a_i p^i, ... \right).$$

Another important result, that we will need later on is the following

Theorem 1.10. (Hensel's Lemma for $\mathbb{Q}_p$)
Let $f \in \mathbb{Z}_p[X]$ be a monic polynomial and let $\bar{f} \in \mathbb{F}_p[X]$ be its reduction modulo p. If $\bar{f}$ is the product of two relatively prime polynomials g' and h', then $f = gh$ such that $g' = \bar{g}$ and $h' = \bar{h}$.

For a proof, see [Gou97, Theorem 3.4.1]. □

1.3 Class Field Theory

The goal of class field theory is the classification of abelian extensions L/K with certain properties of a given number field or local field K in terms of data intrinsic to K, for example ideal-theoretic or topological properties of K or certain groups, which are closely related to K. For all abelian extensions L/K with certain specific properties, one finds in most cases surjective group homomorphisms of the form

$$\theta_{L/K} : G_K \to \mathrm{Gal}(L/K),$$

where the definition of G_K is independent of L, together with an explicit description of the kernels, which depend on L. The collection of the resulting isomorphisms is called a "Reciprocity Law".

With the help of a reciprocity law, one can find a map

$$\left\{\begin{matrix}\text{Abelian extensions } L/K \text{ with} \\ \text{certain specific properties}\end{matrix}\right\} \longrightarrow \left\{\text{Certain subgroups of } G_K\right\},$$

which is an inclusion-preserving or reversing bijection.

Before stating the main theorems of general class field theory of abelian extensions, we will give a concrete example of class field theory of *unramified extensions*.

We call the prime ideals of a field K *finite primes*. A *real infinite prime* of K is an embedding $\sigma : K \to \mathbb{R}$ and a *complex infinte prime* is an embedding $\sigma : K \to \mathbb{C}$, where $\sigma \neq \overline{\sigma}$. We say that an infinite prime σ ramifies in an extension L if σ is real and has a complex extension to L.

A field extension L/K is said to be *unramified*, if every finite and infinite prime of K is unramified in L.

Proposition 1.11. *Let L/K be a Galois extension of number fields, $\mathfrak{p}$ a prime of K, unramified in L and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. There is a unique $\sigma \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P},$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ *is the norm of* $\mathfrak{p}$.

For a proof, see [Cox13, Lemma 5.19.]. □

We denote this unique automorphism, called the *Artin symbol*, by

$$\left(\frac{L/K}{\mathfrak{P}}\right).$$

The conjugates of the Artin symbol satisfy an important property. For any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

In the case of an abelian extension, this simplifies to

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \left(\frac{L/K}{\mathfrak{P}}\right),$$

which means

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

is well defined and we can define the Artin symbol in terms of $\mathfrak{p}$. In particular, if L/K is an unramified abelian extension, the symbol is defined for every prime $\mathfrak{p}$.

Extending multiplicatively to all fractional ideals, we obtain the *Artin map*, a homomorphism

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K),$$

where I_K is the group of fractional ideals of K. An important subgroup of I_K is the group of *principal fractional ideals* P_K. These are of the form $\alpha\mathcal{O}_K$ for $\alpha \in K^*$. The quotient $I_K/P_K = C(\mathcal{O}_K)$ is called the *ideal class group* and is a finite group.

The reciprocity law for unramified abelian extensions can now be stated with a single isomorphism and a distinguished extension, the *Hilbert class field of* K, which is the maximal unramified abelian extension of K. Its existence can be proven for every number field K. In particular, the Hilbert class field contains every unramified abelian extension of K.

Theorem 1.12. (Artin Reciprocity for the Hilbert Class Field)
Let L *be the Hilbert class field of a number field* K. *Then the Artin map*

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K),$$

is surjective and its kernel is the subgroup of principal fractional ideals P_K. *Thus there is an isomorphism*

$$C(\mathcal{O}_K) \cong \mathrm{Gal}(L/K).$$

For a proof, see [Cox13, Theorem 5.23.]. □

Applying Galois Theory we get the immediate

Corollary 1.13. *There is an inclusion-reversing bijection*

$$\left\{\text{Unramified abelian extensions } L/K\right\} \longrightarrow \left\{\text{Subgroups of } C(\mathcal{O}_K)\right\}.$$

If an extension M/K is mapped to the subgroup H, then we have an isomorphism

$$C(\mathcal{O}_K)/H \cong \mathrm{Gal}(M/K)$$

induced by the Artin map. □

Thus, it is enough to study the fractional ideals of the base field to get information on the unramified abelian extensions.

In the case of arbitrary abelian extensions one has to work with the topology induced by the $\mathfrak{p}$-adic valuations. This is done in two steps. The first is the study of abelian extensions of $\mathfrak{p}$-adic number fields, called *local class field theory*.

A $\mathfrak{p}$-adic number field K is a complete field of characteristic 0, equipped with a discrete valuation, such that the residue field $A_K/\mathfrak{p}$ is finite, with $\mathfrak{p}$ being the unique prime ideal of the valuation ring A_K.

Let K be a number field or a $\mathfrak{p}$-adic number field and let L/K be a Galois extension. An important component of class field theory is the norm map $N_{L/K} : L^* \to K^*$ and its image $N_{L/K}L^*$, called a *norm group*.

To prove the reciprocity law of local class field theory, one has to work with unramified extensions first, similar to the example above, and then generalize to obtain the following

Theorem 1.14. (Reciprocity Law of Local Class Field Theory)
Let K be a $\mathfrak{p}$-adic number field. For every Galois extension L/K we have an isomorphism

$$K^*/N_{L/K}L^* \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

For a proof, see [Neu13, Chapter II, Theorem 5.9]. □

The surjective homomorphism

$$(\quad, L/K) : K^* \to \mathrm{Gal}(L/K)^{\mathrm{ab}},$$

which induces the above isomorphism, is called the *norm residue symbol*. By taking projective limits, the norm residue symbols of abelian extensions induce an injective homomorphism

$$(\quad, K) : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where K^{ab} is the maximal abelian extension of K.

So far, the reciprocity law only tells us that the abelian extensions are related to the norm groups of K^*, i.e. the groups of the form $N_{L/K}L^*$ for an abelian extension L/K. The following theorem characterises the norm groups in terms of K^*, endowed with the $\mathfrak{p}$-adic topology.

Theorem 1.15. (Existence Theorem of Local Class Field Theory)
The norm groups of K^* are in bijection with the open subgroups of finite index. In particular, there is an inclusion reversing bijection between the abelian extensions of K and the open subgroups of K^* of finite index, given by

$$L \mapsto N_{L/K}L^*,$$

for any abelian extension L/K.

For a proof, see [Neu13, Chapter II, Theorem 6.1 and Theorem 6.2]. □

The second step is to establish a connection between $\mathfrak{p}$-adic number fields and number fields, moving from local to *global class field theory*. This is achieved by the *idèle group*, i.e. the restricted product

$$\mathbf{I}_K = \prod_{\mathfrak{p}}^{*} K_{\mathfrak{p}}^*,$$

where $\mathfrak{p}$ runs over all finite and infinite primes of the field K and for a tuple $(x_{\mathfrak{p}}) \in \mathbf{I}_K$, we have $x_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}^*$ for all but finitely many $\mathfrak{p}$. There is a natural embedding of K^* into the idèles. Let $\alpha \in K^*$ and consider the tuple $x = (\alpha, \alpha, ...)$. Then $x \in \mathbf{I}_K$, since only finitely many prime ideals appear in the decomposition of $\alpha\mathcal{O}_K$. Thus we can identify K^* as a subgroup of $\mathbf{I}_K$. The quotient

$$\mathbf{C}_K = \mathbf{I}_K/K^*$$

is called the *idèle class group* and is the main object of study in global class field theory.

Theorem 1.16. (Artin's Reciprocity Law)
Let L/K be an extension of number fields. There is an isomorphism

$$\theta_{L/K} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathbf{C}_K/N_{L/K}\mathbf{C}_L.$$

For a proof, see [Neu13, Chapter III, Theorem 6.12]. □

The map $\theta_{L/K}$ is called the *reciprocity map* and its inverse is induced by the surjective homomorphism

$$(\quad, L/K) : \mathbf{C}_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}},$$

again called the *norm residue symbol*. By taking projective limits, we obtain the surjective homomorphism

$$(\quad, K) : \mathbf{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

called the *universal norm residue map*. As before, the groups $N_{L/K}\mathbf{C}_L$ are called *norm groups* and they are completely characterised in terms of K. Endowing $\mathbf{C}_K$ with a topology assembled from the $\mathfrak{p}$-adic topologies of the idelic components, called the *idèle topology*, we obtain the following

Theorem 1.17. (Existence Theorem of Global Class Field Theory)
The norm groups of $\mathbf{C}_K$ are precisely the closed subgroups of finite index. In particular, there is an inclusion reversing bijection between the abelian extensions of K and the closed subgroups of finite index of $\mathbf{C}_K$, given by

$$L \mapsto N_{L/K}\mathbf{C}_L,$$

for any abelian extension L/K.

For a proof, see [Neu13, Chapter III, Theorem 7.8]. □

There is an alternative approach to class field theory, omitting idèles entirely. Instead, one relates abelian extensions L/K to so-called *moduli*. However, the resulting theorems depend on the particular choice of the modulus. To conclude this section, we will quickly summarize the main theorems using this ideal-theoretic approach.

A *modulus* in a field K is a formal product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. Let $I_K(\mathfrak{m})$ be the group of all fractional ideals, relatively prime to $\mathfrak{m}_0$. The subgroup $P_{K,1}(\mathfrak{m}) \subseteq I_K(\mathfrak{m})$ generated by the set

$$\{\alpha\mathcal{O}_K : \alpha \in \mathcal{O}_K, \alpha \equiv 1 \mod \mathfrak{m}_0 \text{ and } \sigma(\alpha) > 0 \text{ for every } \sigma \text{ dividing } \mathfrak{m}_\infty\}$$

has finite index in $I_K(\mathfrak{m})$. A subgroup $H \subseteq I_K(\mathfrak{m})$ containing $P_{K,1}(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ and the quotient $I_K(\mathfrak{m})/H$ is a *generalized ideal class group* for $\mathfrak{m}$.

Let L/K be an abelian extension and let all ramified primes of K divide the modulus $\mathfrak{m}$. Let $\mathfrak{p}$ be a prime of K, unramified in L. Recall that the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$$

is the unique automorphism such that

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_L$ and $\mathfrak{P}$ dividing $\mathfrak{p}$. In particular, the Artin symbol is defined for every prime $\mathfrak{p}$, relatively prime to $\mathfrak{m}_0$ and by extending multiplicatively, we obtain a well-defined and surjective homomorphism

$$\Phi_{L/K,\mathfrak{m}} := \left(\frac{L/K}{\cdot}\right) : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K),$$

again called the *Artin map*.

Theorem 1.18. (Artin Reciprocity Theorem)
Let L/K be an abelian extension. Then there is a modulus $\mathfrak{m}$, divisible by all ramified primes of K, such that $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. We have an isomorphism

$$I_K(\mathfrak{m})/\ker(\Phi_{L/K,\mathfrak{m}}) \cong \mathrm{Gal}(L/K)$$

and $\mathrm{Gal}(L/K)$ is a generalized ideal class group for $\mathfrak{m}$.

For a proof, see [Jan73, Chapter V, Theorem 5.7]. □

Theorem 1.19. (Existence Theorem)
Let $\mathfrak{m}$ be a modulus and let H be a congruence subgroup for $\mathfrak{m}$. There is a unique abelian extension L/K, with all ramified primes of K dividing $\mathfrak{m}$, such that $H = \ker(\Phi_{L/K,\mathfrak{m}})$, yielding the isomorphism

$$I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K).$$

For a proof, see [Jan73, Chapter V, Theorem 9.16]. □

Remark 1.20. We call the unique abelian extension $K_\mathfrak{m}/K$, corresponding to the congruence subgroup $P_{K,1}(\mathfrak{m})$, the *ray class field for the modulus* $\mathfrak{m}$. In particular, if $\mathfrak{m} = 1$, i.e. no prime divides $\mathfrak{m}$, then the ray class field for $\mathfrak{m}$ is the Hilbert class field of K.

2 Ring Class Fields and Complex Multiplication

In this section, we will present the main theorems of complex multiplication. To prepare the way, we will introduce ring class fields and certain subrings of the ring of integers $\mathcal{O}_K$ of a quadratic field K, called orders. The two are related by the ideal-theoretic version of class field theory.

The second important component of the theory of complex multiplication are lattices in the complex plane and their j-invariants. We will see that the j-function is a powerful tool to generate ring class fields. Moreover, it is also related to the field of modular functions, as we will observe in the following section.

2.1 Orders and Ring Class Fields

Throughout this subsection, let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic number field, i.e. $n < 0$ and squarefree, with discriminant

$$d_K = \begin{cases} n & \text{if } n \equiv 1 \mod 4 \\ 4n & \text{otherwise} \end{cases}.$$

Definition 2.1. An *order* $\mathcal{O}$ in K is a free $\mathbb{Z}$-module of rank 2 and a subring of $\mathcal{O}_K$, containing 1.

It is easy to see that $\mathcal{O}_K$ is an order, more precisely the *maximal order* of K and we can write $\mathcal{O}_K = [1, w_K]$, where

$$w_K = \frac{d_K + \sqrt{d_K}}{2}.$$

We can describe any order $\mathcal{O}$ in such a way. Since $\mathcal{O}$ and $\mathcal{O}_K$ both have rank 2, the index $f = [\mathcal{O}_K : \mathcal{O}]$ is finite and we call f the *conductor* of $\mathcal{O}$.

Lemma 2.2. *Let $\mathcal{O}$ be an order with conductor f. Then*

$$\mathcal{O} = [1, f w_K].$$

For a proof, see [Cox13, Lemma 7.2.]. □

Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. The *norm* of $\mathfrak{a}$ is defined as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ and it can be easily shown that it is a finite number, as we have already discussed for $\mathcal{O}_K$ in the previous section. However, the lack of a crucial property makes the treatment of $\mathcal{O}$ more difficult than the one of $\mathcal{O}_K$.

If $\mathcal{O}$ is a proper subring of $\mathcal{O}_K$, then $\mathcal{O}$ is not integrally closed, since $\sqrt{n} \notin \mathcal{O}$, but $X^2 - n \in \mathcal{O}[X]$. Then $\mathcal{O}$ is not a Dedekind domain and we may not have unique factorization of ideals. To solve this problem, we will consider ideals with the following property.

Definition 2.3. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is called a *proper ideal*, if

$$\mathcal{O} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\},$$

or in other words, if for every $\alpha \in K$ we have

$$\alpha\mathfrak{a} \subseteq \mathfrak{a} \iff \alpha \in \mathcal{O}.$$

Note that the implication $\alpha \in \mathcal{O} \Rightarrow \alpha\mathfrak{a} \subseteq \mathfrak{a}$ is always satisified. We can extend this definition to *fractional ideals* of $\mathcal{O}$. These are nonzero finitely generated $\mathcal{O}$-modules, contained in K and it can be shown that every fractional ideal of $\mathcal{O}$ is of the form $\alpha\mathfrak{a}$ for some $\alpha \in K^*$ and an ideal $\mathfrak{a}$ of $\mathcal{O}$. We also define invertibility of fractional ideals in the same way as we did for $\mathcal{O}_K$.

Lemma 2.4. *If $K = \mathbb{Q}(\tau)$ and $aX^2 + bX + c$ is the minimal polynomial of τ, with $(a, b, c) = 1$, then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$.*

For a proof, see [Cox13, Lemma 7.5.]. □

Now we can characterise all invertible fractional ideals of $\mathcal{O}$.

Proposition 2.5. *A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is invertible if and only if it is proper.*

For a proof, see [Cox13, Proposition 7.4.]. □

We denote the set of all proper fractional ideals of $\mathcal{O}$ by $I(\mathcal{O})$ and Proposition 2.5. tells us that $I(\mathcal{O})$ is a group under multiplication. It is easily checked that any principal ideal is proper, which means the set $P(\mathcal{O})$, generated by the principal ideals of $\mathcal{O}$ is a subgroup of $I(\mathcal{O})$.

Definition 2.6. The *ideal class group* of the order $\mathcal{O}$ is the quotient

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

and its cardinality is the *class number*

$$h(\mathcal{O}) = |C(\mathcal{O})|.$$

Unfortunately, the ideal class group is not enough to relate orders with class field theory. Hence we need to introduce ideals *prime to the conductor*.

Definition 2.7. Let $\mathcal{O}$ be an order of conductor f and let k be an integer. Then a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$ is *prime to* k if

$$\mathfrak{a} + k\mathcal{O} = \mathcal{O}.$$

In particular, $\mathfrak{a}$ is *prime to the conductor* if it is prime to f.

Two important properties of such ideals are given by the following

Lemma 2.8. *Let $\mathcal{O}$ be an order of conductor f, let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$ and let $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ denote the norm of $\mathfrak{a}$. If $m \in \mathbb{N}$, then*

(i) *$\mathfrak{a}$ is prime to m if and only if $N(\mathfrak{a})$ is relatively prime to m.*

(ii) *If $\mathfrak{a}$ is prime to f, then it is proper.*

For a proof, see [Cox13, Lemma 7.18.]. □

Lemma 2.9. *Let $\mathcal{O}$ be an order and let $\mathfrak{a}$ and $\mathfrak{b}$ be two proper ideals of $\mathcal{O}$. Then*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ are prime to f, then so is $\mathfrak{ab}$.

For a proof, see [Cox13, Lemma 7.14. (ii)]. □

The previous results tell us that the set of ideals, which are prime to f, is contained in $I(\mathcal{O})$ and closed under multiplication. Let $I(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O})$, generated by this set. We also obtain the subgroup $P(\mathcal{O}, f) \subseteq I(\mathcal{O}, f)$, generated by all principal ideals, which are prime to f. These groups are closely related to the ideal class group.

Proposition 2.10. *There is an isomorphism*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong C(\mathcal{O}),$$

induced by the inclusion $I(\mathcal{O}, f) \hookrightarrow I(\mathcal{O})$.

For a proof, see [Cox13, Proposition 7.19.]. □

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and let $m \in \mathbb{N}$. Recall that I_K is the group of fractional ideals of $\mathcal{O}_K$. By Lemma 2.8., we obtain a subgroup $I_K(m)$, generated by all ideals of $\mathcal{O}_K$, prime to m. The following proposition describes the relation between the groups $I(\mathcal{O}, f)$ and $I_K(f)$.

Proposition 2.11. *Let $\mathcal{O}$ be an order of conductor f. Then*

(i) *If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, prime to f, then $\mathfrak{a} \cap \mathcal{O}$ is an ideal of $\mathcal{O}$, also prime to f. Furthermore $N(\mathfrak{a}) = N(\mathfrak{a} \cap \mathcal{O})$.*

(ii) *If $\mathfrak{a}$ is an ideal of $\mathcal{O}$, prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, also prime to f. Furthermore $N(\mathfrak{a}) = N(\mathfrak{a}\mathcal{O}_K)$.*

(iii) *The maps $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ are mutually inverse, inducing an isomorphism*

$$I_K(f) \cong I(\mathcal{O}, f).$$

For a proof, see [Cox13, Proposition 7.20.]. □

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$, prime to f. The inclusion $\mathcal{O} \subseteq \mathcal{O}_K$ induces a homomorphism $\varphi : \mathcal{O} \to \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$. Note that $f\mathcal{O}_K \subseteq \mathcal{O}$ and so $f\alpha + \mathfrak{a}\mathcal{O}_K$ is contained in the image of φ for every $\alpha \in \mathcal{O}_K$. But by Proposition 2.11. $\mathfrak{a}\mathcal{O}_K$ is prime to f and so φ is surjective with kernel $\mathfrak{a}$. From the resulting isomorphism

$$\mathcal{O}/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$$

we can deduce that $\mathfrak{a}$ is a prime ideal if and only if $\mathfrak{a}\mathcal{O}_K$ is a prime ideal. This means in particular, that every ideal $\mathfrak{a}$ of $\mathcal{O}$, prime to f, has a unique decomposition as a product of prime ideals, which are prime to f. The decomposition is given by the factorization of $\mathfrak{a}\mathcal{O}_K$ in $\mathcal{O}_K$.

We can now describe the ideal class group $C(\mathcal{O})$ in terms of $\mathcal{O}_K$. Let $P_{K,\mathbb{Z}}(f)$ denote the subgroup of $I_K(f)$ generated by all principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ and $\alpha \equiv a \mod f\mathcal{O}_K$ for an integer $a \in \mathbb{Z}$, relatively prime to f.

Proposition 2.12. *Let $\mathcal{O}$ be an order of conductor f. Then there are isomorphisms*

$$I_K(f)/P_{K,\mathbb{Z}}(f) \cong C(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f).$$

For a proof, see [Cox13, Proposition 7.22.]. □

One application of this proposition is the following formula for the class number of $\mathcal{O}$.

Theorem 2.13. *Let $\mathcal{O}$ be an order of conductor f. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

For a proof, see [Cox13, Theorem 7.24.]. □

We now have the necessary tools to define ring class fields. Recall the group $I_K(\mathfrak{m})$ of all fractional ideals of $\mathcal{O}_K$, relatively prime to $\mathfrak{m}_0$ for a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, introduced in the discussion preceding Theorem 1.18. and its subgroup $P_{K,1}(\mathfrak{m})$, generated by the set

$$\{\alpha\mathcal{O}_K : \alpha \in \mathcal{O}_K, \alpha \equiv 1 \mod \mathfrak{m}_0 \text{ and } \sigma(\alpha) > 0 \text{ for every } \sigma \text{ dividing } \mathfrak{m}_\infty\}.$$

If we take the modulus $\mathfrak{m} = f\mathcal{O}_K$, we immediately see that

$$P_{K,1}(f\mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f) = I_K(f\mathcal{O}_K).$$

This implies that $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for the modulus $f\mathcal{O}_K$ or in other words, $C(\mathcal{O})$ is a generalized ideal class group for $f\mathcal{O}_K$.

Definition 2.14. Let $\mathcal{O}$ be an order of conductor f. The *ring class field* of $\mathcal{O}$ is the unique abelian extension L/K, all of whose ramified primes divide $f\mathcal{O}_K$, such that

$$C(\mathcal{O}) \cong \mathrm{Gal}(L/K).$$

The existence and uniqueness of such an extension are guaranteed by Theorem 1.19., since $C(\mathcal{O})$ is a generalized ideal class group. Note also that in an imaginary quadratic field, all infinite primes are unramified.

2.2 Lattices and the j-Invariant

We now turn to the second component of complex multiplication, the j-invariant of a lattice.

Definition 2.15. A *lattice* L is an additive subgroup of $\mathbb{C}$, generated by two complex numbers $\omega_1, \omega_2 \in \mathbb{C}$, linearly independent over $\mathbb{R}$. We write $L = [\omega_1, \omega_2]$.

We associate with a lattice L the *Weierstrass $\wp$-function* for L which is defined for any complex number z outside of L as

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

We will just write $\wp(z)$, whenever the lattice L is clear from the context.

As we will see in the following theorem, $\wp(z)$ is an *elliptic function for* L, which means it is meromorphic on $\mathbb{C}$ and for all $\omega \in L$ and $z \in \mathbb{C} - L$, we have $\wp(z + \omega) = \wp(z)$.

Here are some important properties of $\wp(z)$.

Theorem 2.16. *Let $\wp(z)$ be the Weierstrass $\wp$-function for the lattice L.*

(i) *$\wp(z)$ is an elliptic function for L, with double poles at every $\omega \in L$.*

(ii) *Let*

$$g_2(L) = 60 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^4}$$

and

$$g_3(L) = 140 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^6}.$$

Then $\wp(z)$ satisifes the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

(iii) *The equality*

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

holds for all $z, w \notin L$ with $z + w \notin L$.

For a proof, see [Cox13, Theorem 10.1.]. □

We can now define an equivalence relation on the set of lattices.

Definition 2.17. Two lattices L and L' are equivalent or *homothetic*, if there is a nonzero $\lambda \in \mathbb{C}$, such that $L' = \lambda L$.

Note that the Weierstrass $\wp$-function satisfies

$$\wp(z, L) = \lambda^2 \wp(\lambda z, \lambda L)$$

and it can be shown that for every elliptic function $f(z)$ for L, $f(\lambda^{-1} z)$ is an elliptic function for λL.

Proposition 2.18. *Let L be a lattice. Then*

$$\Delta(L) = g_2(L)^3 - 27 g_3(L)^2 \neq 0$$

for the constants $g_2(L)$ and $g_3(L)$, defined in Theorem 2.16. (ii).

For a proof, see [Cox13, Proposition 10.7.]. □

Definition 2.19. The *j-Invariant* $j(L)$ of a lattice L is the number

$$j(L) = 1728\frac{g_2(L)^3}{\Delta(L)}.$$

Proposition 2.18. guarantees that $j(L)$ is defined for every lattice L. The name j-invariant can be justified by the following fact.

Theorem 2.20. *Let L and L' be two lattices. Then $j(L) = j(L')$ if and only if L and L' are homothetic.*

For a proof, see [Cox13, Theorem 10.9.]. □

We can now relate lattices to orders in the following way.

Proposition 2.21. *Let K be an imaginary quadratic field. Then every proper fractional ideal of an order $\mathcal{O}$ is a lattice and conversely, any lattice contained in K is a proper fractional ideal of $\mathcal{O}$ for some order $\mathcal{O}$ in K.*

For a proof, see [Cox13, p. 190]. □

The following theorem tells us the main idea behind complex multiplication.

Theorem 2.22. *Let L be a lattice with Weierstrass $\wp$-function $\wp(z)$ and let $\alpha \in \mathbb{C} - \mathbb{Z}$. Then the following statements are equivalent.*

(i) *$\wp(\alpha z)$ is a rational function in $\wp(z)$.*

(ii) $\alpha L \subseteq L$.

(iii) *There is an imaginary quadratic field K and an order $\mathcal{O}$ in K, such that $\alpha \in \mathcal{O}$ and L is homothetic to a proper fractional ideal of $\mathcal{O}$.*

For a proof, see [Cox13, Theorem 10.14.]. □

We say that the lattice L has *complex multiplication* with α or equivalently with the entire order $\mathcal{O}$ if the statements of Theorem 2.22. hold. To be precise, this means that we have $\alpha L \subseteq L$ for all $\alpha \in \mathcal{O}$ and so $\mathcal{O}L = L$, since $1 \in \mathcal{O}$. Note also that for homothetic lattices L and L', the statements hold for L if and only if they do for L'.

For a fixed order $\mathcal{O}$, any proper fractional ideal of $\mathcal{O}$ trivially has complex multiplication with $\mathcal{O}$. Since multiplication of a fractional ideal with a number $\alpha \in K^*$ is

equivalent with multiplication with the principal fractional ideal $\alpha\mathcal{O}$, we see that two proper fractional ideals are homothetic as lattices, if and only if their ideal classes are equal in $C(\mathcal{O})$. Thus we obtain

Corollary 2.23. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Then there is a bijection between the ideal class group $C(\mathcal{O})$ and the homothety classes of lattices, having complex multiplication with $\mathcal{O}$.* □

Let $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the upper half plane. For every $\tau \in \mathfrak{h}$, the $\mathbb{Z}$-module $[1, \tau]$ is a lattice and so the j-invariant of a lattice induces a map

$$j : \mathfrak{h} \to \mathbb{C}$$

$$\tau \mapsto j([1, \tau]),$$

called the j-function.

An interesting property of the j-function is related to the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane, given by the Möbius transformation

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}$$

for $\tau \in \mathfrak{h}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Theorem 2.24.

(i) *$j(\tau)$ is holomorphic on $\mathfrak{h}$.*

(ii) *Let $\tau, \tau' \in \mathfrak{h}$. Then $j(\tau) = j(\tau')$ if and only if τ and τ' lie in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. We say that $j(\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant.*

(iii) *The j-function is surjective.*

For a proof, see [Cox13, Theorem 11.2.]. □

From the surjectivity of the j-function, we obtain the

Corollary 2.25. *Let $g_2, g_3 \in \mathbb{C}$, satisfying $g_2^3 - 27g_3^2 \neq 0$. Then there is a lattice L, such that $g_2(L) = g_2$ and $g_3(L) = g_3$.*

For a proof, see [Cox13, Corollary 11.7.]. □

Before moving on to the main theorems of complex multiplication, we will give a quick description of *elliptic curves* over $\mathbb{C}$ and how they are related to the contents of this section.

Definition 2.26. An *elliptic curve* E over $\mathbb{C}$ is an equation of the form

$$y^2 = 4x^3 - g_2x - g_3,$$

where $g_2, g_3 \in \mathbb{C}$ and $g_2^3 - 27g_3^2 \neq 0$. We denote the set of solutions

$$\{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$$

by $E(\mathbb{C})$.

Given a lattice L, we obtain the elliptic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L)$$

and since the $\wp$-function of L satisfies the differential equation of Theorem 2.16. (ii), we see that for any $z \in \mathbb{C} - L$, we have $(\wp(z), \wp'(z)) \in E(\mathbb{C})$. Due to the periodicity of the $\wp$-function, we obtain a map

$$\mathbb{C}/L \to E(\mathbb{C}),$$

sending 0 to ∞ and it can be shown that this map is a bijection.

There is a canonical way to endow $E(\mathbb{C})$ with a group structure. We take ∞ to be the identity element and we define additon by the addition law of the $\wp$-function given in Theorem 2.16. (iii). Then the map

$$\mathbb{C}/L \to E(\mathbb{C})$$

becomes a group isomorphism.

Conversely, given an elliptic curve

$$y^2 = 4x^3 - g_2x - g_3,$$

we know by Corollary 2.25., that there is a lattice L with $g_2(L) = g_2$ and $g_3(L) = g_3$. Given another lattice L' with the same constants, we have $j(L) = j(L')$ and so L and L' are homothetic. Now, if $L' = \lambda L$, a straightforward computation shows that

$$g_2(L) = \lambda^4 g_2(\lambda L)$$

and

$$g_3(L) = \lambda^6 g_3(\lambda L).$$

Thus, homothetic lattices with the same constants have to be equal and so there is a unique lattice L associated with E.

This means, we can translate any property of lattices to a property of elliptic curves over $\mathbb{C}$ and vice versa. For example, two elliptic curves

$$y^2 = 4x^3 - g_2x - g_3$$

$$y^2 = 4x^3 - g_2'x - g_3'$$

are said to be *isomorphic over* $\mathbb{C}$ if there is $\lambda \in \mathbb{C}^*$ such that

$$g_2' = \lambda^4 g_2$$

$$g_3' = \lambda^6 g_3.$$

We immediately see that two elliptic curves E and E' are isomorphic over $\mathbb{C}$ if and only if their asscoiated lattices L and L' are homothetic and we can define the j-invariant for elliptic curves in an obvious way.

The *endomorphism ring* of an elliptic curve E is the set

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\},$$

where L is the lattice, assoicated to E and we see that $\alpha \in \mathrm{End}_{\mathbb{C}}(E)$ if and only if L has complex multiplication with α.

2.3 The Main Theorems of Complex Multiplication

We are now ready to state the first main theorem of complex multiplication.

Theorem 2.27. (First Main Theorem of Complex Multiplication)
Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Then $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$.

For proofs, see [Cox13, Theorem 11.1.] and [Lan87, Chapter 10, §1, Theorem 1]. □

Recall the definition of the ray class field for a modulus $\mathfrak{m}$. It is the unique abelian extension $K_{\mathfrak{m}}/K$ corresponding to the congruence subgroup $P_{K,1}(\mathfrak{m})$. We already saw that for the modulus $\mathfrak{m} = 1$ or equivalently $\mathfrak{m} = \mathcal{O}_K$, the ray class field for $\mathfrak{m}$ is the Hilbert class field of K. Recall the inclusions

$$P_{K,1}(f\mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f\mathcal{O}_K).$$

By setting $f = 1$, we have the equality $P_{K,1}(\mathcal{O}_K) = P_{K,\mathbb{Z}}(1)$ and we see that the ring class field of the maximal order $\mathcal{O}_K$ is the Hilbert class field.

Corollary 2.28. *For an imaginary quadratic field K, the Hilbert class field of K is given by $K(j(\mathcal{O}_K))$.* □

We know from class field theory that any abelian extension L/K of an imaginary quadratic field K is contained in the ray class field for some modulus $\mathfrak{m}$. It turns out that $\mathfrak{m}$ does

not need to be complicated.

Lemma 2.29. *Let K be an imaginary quadratic field and let L/K be an abelian extension. Then L is contained in the ray class field for some modulus of the form $m\mathcal{O}_K$, where m is a positive integer.*

For a proof, see [Cox13, p. 219]. □

Hence, to describe all abelian extensions L/K, it is enough to find generators for the ray class fields for the moduli $m\mathcal{O}_K$ for all positive integers m and the second main theorem of complex multiplication gives a solution for this problem.

First we need to define the *Weber function* $h(z, L)$ for a lattice L. It is given by

$$h(z,L) = \begin{cases} \dfrac{g_2(L)^2}{\Delta(L)}\wp(z,L)^2 & \text{if } g_3(L) = 0 \\ \dfrac{g_3(L)}{\Delta(L)}\wp(z,L)^3 & \text{if } g_2(L) = 0 \\ \dfrac{g_2(L)g_3(L)}{\Delta(L)}\wp(z,L) & \text{otherwise,} \end{cases}$$

where $\Delta(L) = g_2(L)^3 - g_3(L)^2$. Recall also the number

$$w_K = \frac{d_K + \sqrt{d_K}}{2},$$

where d_K is the discriminant of the field K.

Theorem 2.30. (Second Main Theorem of Complex Multiplication)
Let K be an imaginary quadratic field with discriminant d_K and let $\mathcal{O}$ be the order of conductor m. Then

$$K(j(\mathcal{O}_K), h(1/m, \mathcal{O}_K)) = K(j(\mathcal{O}), h(w_K, \mathcal{O}))$$

and this field is the ray class field for the modulus $m\mathcal{O}_K$.

For proofs, see [Lan87, Chapter 10, §1, Theorem 2] and [Shi71, Chapter 5] or the references in [Cox13, Theorem 11.39.]. □

3 Modular Functions and Shimura Reciprocity

In this section we will state Shimura's reciprocity law. To do so, we need two important components. One of them is the universal norm residue map

$$(\quad, K) : \mathbf{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

which we have already seen in the first section. The other is a collection of maps

$$\sigma_z : \mathbf{I}_K \longrightarrow \mathrm{Aut}(\mathbf{F}),\ z \in K \cap \mathfrak{h}$$

relating idèles to automorphisms of modular function fields. We will define modular function fields in 3.1. and give a precise description of their automorphism groups, before stating Shimura's reciprocity law in 3.2..

Several of the mentioned concepts will be explained in greater detail throughout the next section.

3.1 Modular Function Fields and their automorphisms

Definition 3.1. Let N be a positive integer. The *congruence subgroup* of level N, denoted by Γ_N, is the group of all $A \in \mathrm{SL}_2(\mathbb{Z})$, satisfying

$$A \equiv I \mod N.$$

It is easy to check that Γ_N is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Let $f : \mathfrak{h} \to \mathbb{C}$ be a meromorphic function and let $q = q(\tau) = e^{2\pi i \tau}$. For every $\tau \in \mathfrak{h}$ we have $0 < |q(\tau)| < 1$ and there is a Laurent expansion

$$f(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n,$$

called the *q-expansion* of $f(\tau)$.

Definition 3.2. A *modular function* of level N is a function $f : \mathfrak{h} \to \mathbb{C}$ with the following properties.

(i) f is meromorphic on $\mathfrak{h}$.

(ii) f is invariant under Γ_N, i.e. $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma_N$.

(iii) For every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the power series expansion of $f(\gamma\tau)$ in the parameter $q^{1/N}$ has only finitely many terms with negative exponents. We also say that f is *meromorphic at the cusps.*

We denote by $\mathbf{F}_{N,\mathbb{C}}$ the set of modular functions of level N. It is not hard to check that $\mathbf{F}_{N,\mathbb{C}}$ is a field with respect to addition and multiplication. We call the union

$$\mathbf{F}_{\mathbb{C}} = \bigcup_{N=1}^{\infty} \mathbf{F}_{N,\mathbb{C}}$$

the *modular function field* over $\mathbb{C}$.

Let $f \in \mathbf{F}_{N,\mathbb{C}}$ and let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Then $f(\gamma\tau)$ is meromorphic on $\mathfrak{h}$. Since Γ_N is normal in $\mathrm{SL}_2(\mathbb{Z})$, for every $\alpha \in \Gamma_N$ there is $\alpha' \in \Gamma_N$ such that $\gamma\alpha = \alpha'\gamma$. Then we have

$$f(\gamma\alpha\tau) = f(\alpha'\gamma\tau) = f(\gamma\tau),$$

implying that $f(\gamma\tau)$ is Γ_N-invariant and by definition $f(\gamma\tau)$ is meromorphic at the cusps. Since $-I$ acts trivially, we can think of $\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma_N$ as a group of automorphisms acting on $\mathbf{F}_{N,\mathbb{C}}$ with fixed field $\mathbf{F}_{1,\mathbb{C}}$ and we obtain the isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma_N \cong \mathrm{Gal}(\mathbf{F}_{N,\mathbb{C}}/\mathbf{F}_{1,\mathbb{C}}).$$

Note that reduction modulo N yields an injection

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_N \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

which is in fact an isomorphism.

We know from Theorem 2.24. that the j-function is holomorphic and $\mathrm{SL}_2(\mathbb{Z})$-invariant. Furthermore we have the following result, proving that $j(\tau)$ is a modular function of level 1.

Theorem 3.3. *The q-expansion of the j-function is given by*

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n,$$

where every c_n is an integer.

For a proof, see [Cox13, Theorem 11.8.]. □

It turns out that the j-function generates the modular functions of level 1.

Theorem 3.4. *We have* $\boldsymbol{F}_{1,\mathbb{C}} = \mathbb{C}(j)$.

For a proof, see [Lan87, Chapter 6 §2, Theorem 1]. □

To find generators for $\mathbf{F}_{N,\mathbb{C}}$, we need the *first Weber function*

$$f_0 : \mathbb{C} \times \mathfrak{h} \longrightarrow \mathbb{C}$$

$$(w, \tau) \mapsto -2^7 3^5 \frac{g_2(L_\tau) g_3(L_\tau)}{\Delta(L_\tau)} \wp(w, L_\tau),$$

where $L_\tau = [1, \tau]$. Now let N be a positive integer and let $r, s \in \mathbb{Z}$, not both divisible by N. Then we set

$$f_{r,s,N}(\tau) = f_0\left(\frac{r\tau + s}{N}, \tau\right).$$

The functions $f_{r,s,N}$ are called the *Fricke Functions*.

Note that if r and s are both divisible by N, then the $\wp$-function is not defined. Moreover, due to the periodicity of the $\wp$-function, we have $f_{r,s,N} = f_{r',s',N}$ for all $r, r', s, s' \in \mathbb{Z}$ satisfying

$$r \equiv r' \mod N$$

$$s \equiv s' \mod N.$$

Let

$$a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in \mathbb{Q}^2 - \mathbb{Z}^2.$$

Then we can write

$$f_a(\tau) = f_0(a_1\tau + a_2, \tau)$$

and we obtain every Fricke function in this way. Note that $f_a(\tau)$ depends only on the residue class of $a \mod \mathbb{Z}^2$, so we can assume that $a \in \mathbb{Q}^2/\mathbb{Z}^2$ and $a \neq 0$.

Lemma 3.5. *Let N be a positive integer. The Fricke functions $f_{r,s,N}$ are modular functions of level N.*

Proof: Let f_a be a Fricke function, where we view

$$a = \begin{pmatrix} a_1, a_2 \end{pmatrix} \in \mathbb{Q}^2$$

as a row vector. We will prove that the relation

$$f_{a\alpha}(\tau) = f_a(\alpha\tau)$$

holds for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathfrak{h}$.

Recall the notation $L_\tau = [1, \tau]$. Then

$$j(L_\tau) = j(\tau) = j(\alpha\tau) = j(L_{\alpha\tau}),$$

since the j-function is $\mathrm{SL}_2(\mathbb{Z})$ invariant, which implies that L_τ and $L_{\alpha\tau}$ are homothetic. If

$$\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix},$$

then the homothety is given by

$$L_\tau = (\alpha_3\tau + \alpha_4)L_{\alpha\tau}.$$

Recall that for a lattice L and $\lambda \in \mathbb{C}$, we have

$$g_2(L) = \lambda^4 g_2(\lambda L),\ g_3(L) = \lambda^6 g_3(\lambda L) \text{ and } \wp(z, L) = \lambda^2 \wp(\lambda z, \lambda L).$$

By setting $\lambda = \alpha_3\tau + \alpha_4$ and appplying these equalities to the definition of $f_a(\alpha\tau)$, we obtain our desired result.

If $\alpha \in \Gamma_N$ and f_a corresponds to the function $f_{r,s,N}$, then it is easy to see that $f_a = f_{a\alpha}$ and by the relation we just proved, $f_{r,s,N}$ is Γ_N invariant.

It is proven in [Lan87, Chapter 4, Proposition 5 and p. 64] that the Fricke functions are holomorphic and meromorphic at the cusps. Furthermore, it is also shown that the coefficients of the q-expansion of $f_{r,s,N}$ are contained in the field $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity. □

We can now describe the field extension $\mathbf{F}_{N,\mathbb{C}}/\mathbf{F}_{1,\mathbb{C}}$.

Theorem 3.6. *Let N be a positive integer. Then we have*

$$\boldsymbol{F}_{N,\mathbb{C}} = \boldsymbol{F}_{1,\mathbb{C}}(f_{r,s,N})_{r,s},$$

for all $r, s \in \mathbb{Z}/N\mathbb{Z}$, not both zero. The Galois group is given by

$$\mathrm{Gal}(\mathbf{F}_{N,\mathbb{C}}/\mathbf{F}_{1,\mathbb{C}}) \cong \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma_N \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1,$$

where the matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ corresponds to the automorphism

$$f \mapsto f^\gamma,\ \textit{where } f^\gamma(\tau) = f(\gamma\tau)$$

for $f \in \mathbf{F}_{N,\mathbb{C}}$.

Proof: We already know that

$$\mathrm{Gal}(\mathbf{F}_{N,\mathbb{C}}/\mathbf{F}_{1,\mathbb{C}}) \cong \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma_N.$$

We also have shown in Lemma 3.5. that $\mathbf{F}_{1,\mathbb{C}}(f_{r,s,N})_{r,s}$ is contained in $\mathbf{F}_{N,\mathbb{C}}$ and that $\mathrm{SL}_2(\mathbb{Z})$ permutes the Fricke functions $f_{r,s,N}$ for fixed N.

Hence $\mathrm{SL}_2(\mathbb{Z})/\Gamma_N$ acts as a finite group of automorphisms on $\mathbf{F}_{1,\mathbb{C}}(f_{r,s,N})_{r,s}$. Let now $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, acting trivially on $\mathbf{F}_{1,\mathbb{C}}(f_{r,s,N})_{r,s}$. We will use the fact, proven in [Cox13, Lemma 10.4.], that for an arbitrary lattice L, we have

$$\wp(z, L) = \wp(w, L) \text{ if and only if } z \equiv \pm w \mod L$$

and the relation

$$f_{a\alpha}(\tau) = f_a(\alpha\tau)$$

to obtain

$$f_{1,0,N}^{\gamma} = f_{\pm 1,0,N},$$
$$f_{0,1,N}^{\gamma} = f_{0,\pm 1,N}$$

and consequently

$$\gamma \equiv \pm I \mod N,$$

since $\det(\gamma) = 1$. Since $-I$ acts trivially, we obtain an embedding

$$\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma_N \hookrightarrow \mathrm{Gal}(\mathbf{F}_{1,\mathbb{C}}(f_{r,s,N})_{r,s}/\mathbf{F}_{1,\mathbb{C}})$$

with fixed field $\mathbf{F}_{1,\mathbb{C}}$ and by Galois theory, this embedding becomes an isomorphism. □

Definition 3.7. Let N be a positive integer. The *modular function field of level N* is the field

$$\mathbf{F}_N = \mathbb{Q}(j, f_{r.s.N})_{r,s},$$

for all $r, s \in \mathbb{Z}/N\mathbb{Z}$, not both zero. Similar to above, the union

$$\mathbf{F} = \bigcup_{N=1}^{\infty} \mathbf{F}_N$$

is called *the modular function field.*

We are again interested in the Galois group of $\mathbf{F}_N$ over $\mathbf{F}_1 = \mathbb{Q}(j)$. Note that we can write any element $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & \det(\alpha) \end{pmatrix} \gamma, \tag{3.1.1}$$

where $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is uniquely determined. Recall also that the coefficients of the q-expansions of the Fricke functions $f_{r,s,N}$ are contained in $\mathbb{Q}(\zeta_N)$.

Theorem 3.8. *Let N be a positive integer and let ζ_N be a primitive N-th root of unity. Then*

$$\mathrm{Gal}(\mathbf{F}_N/\mathbf{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1.$$

For $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the induced automorphism acts by

$$\zeta_N \mapsto \zeta_N^{\det(\alpha)}$$

on the coefficients of the q-expansion of $f \in \mathbf{F}_N$ and by the action of γ, given by Theorem 3.6., where $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is the matrix from (3.1.1).

Proof: Let $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ be the automorphism mapping ζ_N to ζ_N^d. We can extend σ_d to the map

$$\sigma_d : \mathbb{Q}(\zeta_N)((q^{1/N})) \longrightarrow \mathbb{Q}(\zeta_N)((q^{1/N}))$$

$$\sum_{k=-\infty}^{\infty} a_k q^{1/N} \mapsto \sum_{k=-\infty}^{\infty} \sigma_d(a_k) q^{1/N}$$

between the fields of formal power series in the variable $q^{1/N}$. It is proven in [Lan87, Chapter 4 §2] that the only exponents of ζ_N in the q-expansion of the Fricke function $f_{r,s,N}(\tau)$ are $\pm s$ and $2s$. This implies that σ_d maps $f_{r,s,N}$ to $f_{r,ds,N}$. Hence σ_d can be represented by the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}.$$

In particular, σ_d fixes the j-function, since by Theorem 3.3., its q-expansion is contained in $\mathbb{Q}((q^{1/N}))$ and so we can view σ_d as an element of $\mathrm{Gal}(\mathbf{F}_N/\mathbf{F}_1)$.

We know that $\mathrm{SL}_2(\mathbb{Z})$ permutes the Fricke functions and by repeating the arguments in the proof of Theorem 3.6., it is easy to see that $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ is contained in the Galois group, and so we obtain an embedding

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1 \hookrightarrow \mathrm{Gal}(\mathbf{F}_N/\mathbf{F}_1).$$

We know that the fixed field of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ is contained in $\mathbf{F}_{1,\mathbb{C}} = \mathbb{C}(j)$. Similarly, the collection of all σ_d's fixes $\mathbb{Q}((q^{1/N}))$. This implies that the fixed field of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ is

$$\mathbb{Q}((q^{1/N})) \cap \mathbb{C}(j) = \mathbb{Q}(j) = \mathbf{F}_1,$$

which yields the desired isomorphism.

It is also clear that the action of an element $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathbf{F}_N$ is exactly as predicted, since σ_d corresponds to the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}.$$

□

We need one more Galois group for the formulation of Shimura's reciprocity law, the automorphism group of the modular function field

$$\mathrm{Aut}(\mathbf{F}) = \mathrm{Gal}(\mathbf{F}/\mathbb{Q}).$$

Recall the ring of p-adic integers $\mathbb{Z}_p$ and the field of p-adic numbers $\mathbb{Q}_p$.

Definition 3.9. The *finite adelic group of* GL_2, denoted by $\mathrm{GL}_2(\mathbb{A})$, is given as the restricted product

$$\mathrm{GL}_2(\mathbb{A}) = \prod_{p \text{ prime}}^{*} \mathrm{GL}_2(\mathbb{Q}_p),$$

where all but finitely many components of an element are contained in $\mathrm{GL}_2(\mathbb{Z}_p)$.

Let $x \in \mathbb{Q}^*$. Then x is a unit in $\mathbb{Z}_p$ for all but finitely many primes p and so the tuple $(xI, ..., xI)$ is contained in $\mathrm{GL}_2(\mathbb{A})$. Thus, we obtain an embedding $\mathbb{Q}^* \hookrightarrow \mathrm{GL}_2(\mathbb{A})$. Our goal is to show that $\mathrm{Aut}(\mathbf{F}) \cong \mathrm{GL}_2(\mathbb{A})/\mathbb{Q}^*$.

We denote by U the projective limit

$$\varprojlim_N \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p)$$

and by $\mathrm{GL}_2(\mathbb{Q})^+$ the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ of all matrices with positive determinant. The first important property of $\mathrm{GL}_2(\mathbb{A})$ is that every element has a decomposition into elements of these two groups.

Proposition 3.10. *We have*

$$\mathrm{GL}_2(\mathbb{A}) = \mathrm{GL}_2(\mathbb{Q})^+ U.$$

Proof: Let K be a field. We will use the fact that $\mathrm{SL}_2(K)$ is generated by the matrices

$$X(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ and } Y(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \ a \in K.$$

Let $x = (x_{p_1}, x_{p_2}, ...) \in \mathrm{GL}_2(\mathbb{A})$ and take x_p such that $x_p \notin \mathrm{GL}_2(\mathbb{Z}_p)$ with $\det(x_p) = p^r \varepsilon$, where $r \in \mathbb{Z}$ and ε a unit in $\mathbb{Z}_p$. Let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & p^{-r} \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}.$$

Then $Ax_pB \in \mathrm{SL}_2(\mathbb{Q}_p)$ and so we can write

$$Ax_pB = Z(a_1)...Z(a_k),$$

where $Z(a_i)$ is either $X(a_i)$ or $Y(a_i)$ for $a_i \in \mathbb{Q}_p$. By approximating the p-adic expansions of every a_i, we obtain a matrix

$$C = Z(\tilde{a_1})...Z(\tilde{a_k}) \in \mathrm{SL}_2(\mathbb{Q}),$$

such that $\tilde{I} = C^{-1}Ax_pB$ is arbitrarily close to the unit matrix in $\mathrm{SL}_2(\mathbb{Q}_p)$, which means that for a sufficiently strong approximation, we have $\tilde{I} \in \mathrm{SL}_2(\mathbb{Z}_p)$. We now have the decomposition

$$x = (x_{p_1}, x_{p_2}, ..., x_p, ...) = A^{-1}C(C^{-1}Ax_{p_1}, C^{-1}Ax_{p_2}, ..., \tilde{I}B^{-1}, ...).$$

Since the only primes appearing in the denominators of the entries of $C^{-1}A$ are powers of p, and $\det(C^{-1}A) = p^{-r}$, we have $C^{-1}A \in \mathrm{GL}_2(\mathbb{Z}_q)$ for every prime $q \neq p$. We further have $B \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $A^{-1}C \in \mathrm{GL}_2(\mathbb{Q})^+$.

By repeating this for all of the finitely many components $x_{p_i} \notin \mathrm{GL}_2(\mathbb{Z}_{p_i})$, we obtain our desired decomposition. □

Using this decomposition, we can assign every element $\alpha u \in \mathrm{GL}_2(\mathbb{A})$, where $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and $u \in U$, to an automorphism of $\mathbf{F}$. For any positive integer N, there is a canonical homomorphism

$$U \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$
$$u \mapsto \tilde{u},$$

which we will explicitly describe in section 4. If the Fricke function f_a corresponds to $f_{r,s,N}$, we will denote $f_{a\tilde{u}}$ by f_{au}.

Proposition 3.11. *Let f_a be the Fricke functions. For every $u \in U$ there is $\sigma_u \in \mathrm{Gal}(\mathbf{F}/\mathbf{F}_1)$, such that*

$$f_a^{\sigma_u} = f_{au}$$

for all nonzero $a \in \mathbb{Q}^2/\mathbb{Z}^2$ and the map

$$u \mapsto \sigma_u$$

induces an injective homomorphism

$$U/\pm I \longrightarrow \mathrm{Gal}(\mathbf{F}/\mathbf{F}_1).$$

Proof: We have already seen that permuting the Fricke functions yields an automorphism of the modular function field and that $-I$ is contained in the kernel. If $u \in U$ acts trivially, it is easy to see that the induced matrix $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ equals $\pm I$ for every N and so $u = \pm I$ in U. □

In particular, the action of $u \in U$ on $\mathbf{F}_N$ is given by the action of $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ described in Theorem 3.8..

For $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, we define the automorphism σ_α simply by

$$f^{\sigma_\alpha}(\tau) = f(\alpha\tau) \tag{3.1.2}$$

for any $f \in \mathbf{F}$. We obtain an injective homomorphism

$$\mathrm{GL}_2(\mathbb{Q})^+/\mathbb{Q}^* \longrightarrow \mathrm{Aut}(\mathbf{F}),$$

since the kernel of the map $\alpha \mapsto \sigma_\alpha$ is the subgroup of scalar matrices.

Note that the decompositon of elements of $\mathrm{GL}_2(\mathbb{A})$ is not unique, since

$$U \cap \mathrm{GL}_2(\mathbb{Q})^+ = \mathrm{SL}_2(\mathbb{Z}).$$

However, this does not cause any problems for the corresponding automorphisms.

Lemma 3.12. *The maps $u \mapsto \sigma_u$ and $\alpha \mapsto \sigma_\alpha$ from Proposition 3.11. and (3.1.2) coincide on $\mathrm{SL}_2(\mathbb{Z})$.*

Proof: This immediately follows from the definitions of σ_α and σ_u, the relation

$$f_{a\alpha}(\tau) = f_a(\alpha\tau),\ \alpha \in \mathrm{SL}_2(\mathbb{Z})$$

for the Fricke functions, proven in Lemma 3.5., and the fact that the Fricke functions generate $\mathbf{F}$ together with the j-function, which is $\mathrm{SL}_2(\mathbb{Z})$-invariant. □

Theorem 3.13. *Let $\alpha, \alpha', \beta \in \mathrm{GL}_2(\mathbb{Q})^+$ and let $u, u', v \in U$ such that $\alpha u = \alpha' u' = v\beta$. Then $\sigma_\alpha\sigma_u = \sigma_{\alpha'}\sigma_{u'} = \sigma_v\sigma_\beta$.*

Proof: Let $\alpha u = \alpha' u'$. Then we have

$$uu'^{-1} = \alpha^{-1}\alpha' \in \mathrm{SL}_2(\mathbb{Z}).$$

By setting $\delta = uu'^{-1}$, we obtain by multiplicativity

$$\sigma_{\alpha'}\sigma_{u'} = \sigma_{\alpha\delta}\sigma_{\delta^{-1}u} = \sigma_\alpha\sigma_\delta\sigma_{\delta^{-1}}\sigma_u = \sigma_\alpha\sigma_u.$$

For the second equality, see [Lan87, Chapter 7 §2, Theorem 4] and [Shi71, Proposition 6.22.]. □

Hence, we obtain a well-defined map

$$\mathrm{GL}_2(\mathbb{A}) \longrightarrow \mathrm{Aut}(\mathbf{F})$$

$$\alpha u \mapsto \sigma_\alpha\sigma_u,$$

which does not depend on the chosen decomposition αu. We can now describe the group $\mathrm{Aut}(\mathbf{F})$.

Theorem 3.14. (Shimura Exact Sequence)
The sequence

$$0 \to \mathbb{Q}^* \to \mathrm{GL}_2(\mathbb{A}) \to \mathrm{Aut}(\mathbf{F}) \to 0$$

is exact. In particular, every automorphism of $\boldsymbol{F}$ can be written as $\sigma_\alpha \sigma_u$ for $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and $u \in U$.

For proofs, see [Lan87, Chapter 7 §3, Theorem 6] and [Shi71, Theorem 6.23.]. □

3.2 Shimura's Reciprocity Law

Let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic field for a negative integer n. For a prime number p, we denote by K_p the tensor product

$$K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K.$$

We will see later that

$$K_p \cong \prod_{\mathfrak{p}|p\mathbb{Z}} K_{\mathfrak{p}}$$

so that we can identify the idèle group $\mathbf{I}_K$ with the restricted product of all K_p.

Let now $z \in K \cap \mathfrak{h}$. We need the well-defined map

$$q_z : K^* \longrightarrow \mathrm{GL}_2(\mathbb{Q})^+,$$

given by the relation

$$q_z(\xi) \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} \xi z \\ \xi \end{pmatrix},$$

for $\xi \in K^*$.

We can extend q_z to

$$q_{z,p} : K_p^* \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p)$$

by continuity and then extend it further to a mapping of idèles

$$q_z : \mathbf{I}_K \longrightarrow \mathrm{GL}_2(\mathbb{A}).$$

Recall the automorphism of $\mathbf{F}$ given by $\sigma = \sigma_\alpha \sigma_u$ for $\alpha u \in \mathrm{GL}_2(\mathbb{A})$. For every $z \in K \cap \mathfrak{h}$ we obtain a map

$$\sigma_z : \mathbf{I}_K \longrightarrow \mathrm{Aut}(\mathbf{F})$$

given by $\sigma_z(s) = \sigma(q_z(s))$ for an idèle s.

We are now ready to state Shimura's reciprocity law.

Theorem 3.15. (Shimura's Reciprocity Law)
Let $s \in \mathbf{I}_K, z \in K \cap \mathfrak{h}$ and let $(\quad, K)$ denote the universal norm residue map. Then for every $f \in \mathbf{F}$, defined at z, we have $f(z) \in K^{\mathrm{ab}}$ and

$$(s^{-1}, K)f(z) = f^{\sigma_z(s)}(z).$$

Sketch of Proof: The fact that $f(z) \in K^{\mathrm{ab}}$ for every $f \in \mathbf{F}$ is a direct consequence of the second theorem of complex multiplication.

Let $q_z(s) = u\alpha$, where $u \in U$ and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. Then we have

$$j^{\sigma_z(s)}(\tau) = (j^{\sigma_u})^{\sigma_\alpha}(\tau) = j^{\sigma_\alpha}(\tau) = j(\alpha\tau),$$

since the j-function is U-invariant. By the idelic version of complex multiplication, one can show that we have

$$(s^{-1}, K)j(\tau) = j(\alpha\tau)$$

and so

$$(s^{-1}, K)j(\tau) = j^{\sigma_z(s)}(\tau).$$

The same can be shown for the Fricke functions by an argument involving elliptic curves.

To show that this holds for any $f \in \mathbf{F}$, consider the ring $K[j]$. The Kronecker-Weber theorem tells us that K is contained in a cyclotomic field, and so $K[j] \subseteq \mathbf{F}$, since every root of unity can be viewed as a constant modular function. Let R be the integral closure of $K[j]$ in $\mathbf{F}$ and let $\mathfrak{m}$ and $\mathfrak{M}$ be the kernels of the homomorphism

$$f \mapsto f(z), \ f \in \mathbf{F},$$

in $K[j]$ and R respectively. By showing that j^{σ_α} is integral over $K[j]$, one can deduce that $\sigma_z(s)$ and σ_α induce automorphisms of R. Since we have

$$j(\alpha z) = (s^{-1}, K)j(z),$$

it is trivial to check that

$$\sigma_\alpha(\mathfrak{m}) \subseteq \mathfrak{M}$$

and so $\sigma_\alpha^{-1}(\mathfrak{M})$ and $\mathfrak{M}$ are both maximal ideals, containing $\mathfrak{m}$. This implies the existence of an element $\phi \in \mathrm{Gal}(\mathbf{F}/K(j))$, such that

$$\phi(\mathfrak{M}) = \sigma_\alpha^{-1}(\mathfrak{M})$$

or equivalently

$$\sigma_\alpha\phi(\mathfrak{M}) = \mathfrak{M}.$$

There is a surjective homomorphism from the decomposition group $D_{\mathfrak{M}} \subseteq \mathrm{Gal}(\mathbf{F}/K(j))$ onto the Galois group of the extension of residue fields $R/\mathfrak{M}/K[j]/\mathfrak{m}$, where $K[j]/\mathfrak{m} = K(j(z))$, so we can take $\lambda \in D_{\mathfrak{M}}$, such that

$$\overline{\lambda\sigma_\alpha\phi} = (s^{-1}, K)$$

for the corresponding maps on the residue fields. By taking $\rho = \lambda\sigma_\alpha\phi$, we see that $\rho \in \mathrm{Aut}(\mathbf{F})$ maps $\mathfrak{M}$ onto itself, which means that $\overline{\rho}$ is indeed defined. ρ coincides with $\sigma_z(s)$ on the field $K(j)$ and consequently also on $\mathbf{F}_1 = \mathbb{Q}(j)$. Hence $\rho^{-1}\sigma_z(s) \in \mathrm{Gal}(\mathbf{F}/\mathbf{F}_1)$ and

$$f_a^{\rho^{-1}\sigma_z(s)}(z) = f_a(z)$$

for the Fricke functions f_a. By [Lan87, Chapter 9 §3, Theorems 2' and 3'], this implies that

$$f^\rho(z) = f^{\sigma_z(s)}(z)$$

for all $f \in \mathbf{F}$. Since we further have

$$\overline{\rho} = (s^{-1}, K)$$

on $R/\mathfrak{M}$, i.e.

$$f^\rho(z) = (s^{-1}, K)f(z)$$

for all $f \in R$, the desired result follows by passing to the quotient field.

For complete proofs, see [Lan87, Chapter 11 §1, Theorem 1] and [Shi71, Theorem 6.31.]. □

Remark 3.16. Note that it is not enough to prove the Reciprocity Law for the j-function and the Fricke functions f_a, which generate the field $\mathbf{F}$. Let $f \in \mathbf{F}$ and $z \in K \cap \mathfrak{h}$. If we write

$$f = \frac{g_1(j, f_a)}{g_2(j, f_a)}$$

for polynomials g_1 and g_2, it may happen that $g_2(j, f_a)(z) = 0$, but f is still defined at z.

4 Shimura Reciprocity and Prime Idèles

Let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic number field and let $\mathfrak{n}_\mathfrak{p} = (1, ..., \varpi_\mathfrak{p}, ..., 1)$ with $\varpi_\mathfrak{p}$ at position $\mathfrak{p}$, be an idèle, where $\varpi_\mathfrak{p}$ is a prime element in $K_\mathfrak{p}$. We say that $\mathfrak{n}_\mathfrak{p}$ is a *prime idèle*. Recall the universal norm residue map

$$(\quad, K) : \mathbf{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

which we can view as a surjective homomorphism

$$(\quad, K) : \mathbf{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Given $z \in K \cap \mathfrak{h}$, our goal in this section is to describe the action of $(\mathfrak{n}_\mathfrak{p}^{-1}, K)$ on $f(z)$ for an arbitrary $f \in \mathbf{F}$, such that $f(z) \in K^{\mathrm{ab}}$ is defined. By Shimura's reciprocity law, this amounts to computing the automorphism $\sigma_z(\mathfrak{n}_\mathfrak{p}) \in \mathrm{Aut}(\mathbf{F})$, since we have

$$(\mathfrak{n}_\mathfrak{p}^{-1}, K) f(z) = f^{\sigma_z(\mathfrak{n}_\mathfrak{p})}(z).$$

To see why $(\mathfrak{n}_\mathfrak{p}^{-1}, K)$ is an interesting object to study, recall that the universal norm residue map is induced by the global norm residue symbols

$$(\quad, L/K) : \mathbf{I}_K \to \mathrm{Gal}(L/K),$$

for abelian extensions L/K. For an idèle s with components $s_\mathfrak{p}$, the automorphism $(s, L/K)$ is defined as

$$(s, L/K) = \prod_{\mathfrak{p} \text{ prime}} (s_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}),$$

where the maps on the right-hand side are the local norm residue symbols

$$(\quad, L_\mathfrak{P}/K_\mathfrak{p}) : K_\mathfrak{p}^* \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})^{\mathrm{ab}}$$

for a prime $\mathfrak{P}$ dividing $\mathfrak{p}$. By Proposition 1.8., we know that the particular choice of $\mathfrak{P}$ has no effect on $(s, L/K)$ and that $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ is isomorphic to the decomposition group $D_\mathfrak{P}$, which means it can be viewed as a subgroup of $\mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(L/K)$ is abelian, we have

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})^{\mathrm{ab}}.$$

Let us assume that $\mathfrak{p}$ is unramified in L and let $\overline{K}_\mathfrak{p}$ and $\overline{L}_\mathfrak{P}$ denote the residue fields of $K_\mathfrak{p}$ and $L_\mathfrak{P}$ respectively. Then $L_\mathfrak{P}/K_\mathfrak{p}$ is an unramified extension of degree $[\overline{L}_\mathfrak{P} : \overline{K}_\mathfrak{p}]$ and there is a canonical isomorphism

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong \mathrm{Gal}(\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p})$$

induced by

$$\overline{\sigma}(x + \hat{\mathfrak{P}}) = \sigma(x) + \hat{\mathfrak{P}}, \quad x \in \mathcal{O}_{L_\mathfrak{P}},$$

where $\hat{\mathfrak{P}}$ is the prime ideal in $L_\mathfrak{P}$. The *Frobenius automorphism* is the map $\overline{\phi} \in \mathrm{Gal}(\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p})$, with the property

$$\overline{\phi}(x) = x^q,$$

where $q = |K_\mathfrak{p}|$. Via the isomorphisms

$$\mathrm{Gal}(\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p}) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong D_\mathfrak{P},$$

we obtain elements $\phi \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ and $\phi_\mathfrak{P} \in \mathrm{Gal}(L/K)$, also called *Frobenius automorphisms*. The map $\phi_\mathfrak{P}$ does not depend on the choice of $\mathfrak{P}$ and coincides with the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right),$$

which is defined by the relation in Proposition 1.11..

The automorphisms $\overline{\phi}$ and ϕ generate their respective Galois groups and we have the following result.

Lemma 4.1. *Let $a \in K_\mathfrak{p}^*$ and let $v_\mathfrak{p}$ be the valuation in $K_\mathfrak{p}$ for a prime $\mathfrak{p}$, unramified in L. Then*

$$(a, L_\mathfrak{P}/K_\mathfrak{p}) = \phi^{v_\mathfrak{p}(a)}.$$

For a proof, see [Neu13, Chapter II, Theorem 4.8]. □

Assume that L/K is a finite abelian extension of number fields. It is a known fact that only finitely many primes $\mathfrak{p}$ ramify in L and we see that $(s, L/K)$ is well-defined, since all but finitely many components $s_\mathfrak{p}$ of the idèle s are units in $\mathcal{O}_{K_\mathfrak{p}}$ with $(s_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}) = 1$. By taking projective limits, $(s, L/K)$ is then well-defined for any abelian extension L/K.

Let $\mathfrak{n}_\mathfrak{p} = (1, ..., \varpi_\mathfrak{p}, ..., 1)$ be a prime idèle. Lemma 4.1. tells us that

$$(\mathfrak{n}_\mathfrak{p}, L/K) = \left(\frac{L/K}{\mathfrak{p}}\right)$$

for every abelian extension L/K, in which $\mathfrak{p}$ does not ramify. Taking the projective limit with respect to these extensions, we obtain the maximal Artin symbol

$$\left(\frac{K^{\mathfrak{p},\mathrm{ab}}/K}{\mathfrak{p}}\right),$$

where $K^{\mathfrak{p},\mathrm{ab}}$ is the maximal abelian extension of K, in which $\mathfrak{p}$ does not ramify.

This means in particular, that $(\mathfrak{n}_\mathfrak{p}^{-1}, K) \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is an automorphism, of which the restriction onto $K^{\mathfrak{p},\mathrm{ab}}$ is

$$\left(\frac{K^{\mathfrak{p},\mathrm{ab}}/K}{\mathfrak{p}}\right)^{-1}$$

and this result does not depend on the choice of the prime element $\varpi_\mathfrak{p}$, determining $\mathfrak{n}_\mathfrak{p}$.

By Shimura's reciprocity law, we then obtain the relation

$$\left(\frac{K^{\mathfrak{p},\mathrm{ab}}/K}{\mathfrak{p}}\right)^{-1} f(\tau) = f^{\sigma_z(\mathfrak{n}_\mathfrak{p})}(\tau)$$

for $f \in \mathbf{F}$ and $\tau \in K \cap \mathfrak{h}$ such that $f(\tau) \in K^{\mathfrak{p},\mathrm{ab}}$.

In particular, let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ with prime decomposition

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{r_i}$$

and let

$$\sigma = \prod_{i=1}^{k} \sigma_z(\mathfrak{n}_{\mathfrak{p}_i}^{r_i}).$$

Then by repeatedly applying the reciprocity law, we obtain

$$\left(\frac{L/K}{\mathfrak{a}}\right)^{-1} f(\tau) = f^\sigma(\tau)$$

for any abelian extension L/K, in which every $\mathfrak{p}_i$ is unramified and for $\tau \in K \cap \mathfrak{h}$ such that $f(\tau) \in L$. We will see this again in 4.6..

4.1 The Automorphism σ_z

We now need a better understanding of the automorphism

$$\sigma_z : \mathbf{I}_K \longrightarrow \mathrm{Aut}(\mathbf{F})$$

and an explicit description of its action on modular functions.

The simplest component of σ_z is the map

$$q_z : K^* \longrightarrow \mathrm{GL}_2(\mathbb{Q})^+,$$

given by

$$q_z(\xi)\begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} \xi z \\ \xi \end{pmatrix}.$$

A straightforward computation yields the following

Lemma 4.2. *Let $\xi = a + b\sqrt{n} \in K^*$ and $z = x + y\sqrt{n} \in K \cap \mathfrak{h}$. Then*

$$q_z(\xi) = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{b(ny^2 - x^2)}{y} \\ \dfrac{b}{y} & a - \dfrac{bx}{y} \end{pmatrix}$$

with determinant $N_{K/\mathbb{Q}}(\xi) = a^2 - nb^2$. □

Note that the matrix is defined, since $y \neq 0$ and a quick computation shows that $q_z(\xi)z = z$, where $q_z(\xi)$ acts on z via Möbius transformation.

To understand the continuous extension

$$q_{z,p} : K_p^* \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p)$$

and the resulting map

$$q_z : \mathbf{I}_K \longrightarrow \mathrm{GL}_2(\mathbb{A}),$$

we need to relate the tensor product

$$K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$$

to the completion $K_{\mathfrak{p}}$, where the prime ideal $\mathfrak{p}$ divides $p\mathbb{Z}$.

Note that we have an embedding

$$K \hookrightarrow \mathbb{Q}_p \otimes_{\mathbb{Q}} K$$

given by

$$\alpha \mapsto 1 \otimes \alpha.$$

If we write $\alpha = x + y\sqrt{n}$ with $x, y \in \mathbb{Q}$, we have

$$x + y\sqrt{n} \mapsto 1 \otimes (x + y\sqrt{n}) = x(1 \otimes 1) + y(1 \otimes \sqrt{n}),$$

or alternatively

$$x + y\sqrt{n} \mapsto x + y\sqrt{\mathbf{n}},$$

where $\sqrt{\mathbf{n}}$ denotes the element

$$1 \otimes \sqrt{n} \in \mathbb{Q}_p \otimes_{\mathbb{Q}} K,$$

which is the image of $\sqrt{n} \in K$ under the embedding. The ring $\mathbb{Q}_p[\sqrt{\mathbf{n}}]$ is then defined as the subring of $\mathbb{Q}_p \otimes_{\mathbb{Q}} K$, generated by $\sqrt{\mathbf{n}}$.

Let $f(X) = X^2 - n$ be the minimal polynomial of $\sqrt{n}$. Then we have

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} K \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[X]/(f) \cong \mathbb{Q}_p[X]/(f)$$

and the elements $1 \otimes 1$ and $1 \otimes \sqrt{n} = \sqrt{\mathbf{n}}$ correspond to the elements $1 + (f)$ and $X + (f)$ respectively. In particular, every element of $\mathbb{Q}_p \otimes_{\mathbb{Q}} K$ can be uniquely written as

$$a(1 \otimes 1) + b(1 \otimes \sqrt{n}),$$

or simply as

$$a + b\sqrt{\mathbf{n}}$$

with $a, b \in \mathbb{Q}_p$ and we obtain an isomorphism of $\mathbb{Q}_p$-algebras

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} K \cong \mathbb{Q}_p[\sqrt{\mathbf{n}}].$$

We now need to consider two cases.

(1) If $f(X)$ splits into linear factors over $\mathbb{Q}_p$, say

$$X^2 - n = (X - \sqrt{n}_p)(X + \sqrt{n}_p),$$

then we obtain the homomorphisms

$$\mu_1, \mu_2 : \mathbb{Q}_p \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{Q}_p,$$

mapping an element $a + b\sqrt{\mathbf{n}}$ to

$$a + b\sqrt{n}_p$$

and

$$a - b\sqrt{n}_p$$

respectively. Since the topology on $\mathbb{Q}_p \otimes_{\mathbb{Q}} K$ is equivalent to the product topology on $\mathbb{Q}_p^2$, it is clear that μ_1 and μ_2 are continuous.

Thus we obtain the continuous isomorphism of $\mathbb{Q}_p$-algebras

$$\mu_1 \oplus \mu_2 : \mathbb{Q}_p \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{Q}_p \oplus \mathbb{Q}_p.$$

The injectivity is easy to show and since we have a linear map between two $\mathbb{Q}_p$-vector spaces of the same dimension, the surjectivity follows as well.

We can now describe the completions $K_{\mathfrak{p}}$ for the primes $\mathfrak{p}$ dividing $p\mathbb{Z}$.

Proposition 4.3. *Let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic number field and let p be a prime number. Then*

(i) *p splits completely in K, i.e. $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, if and only if $f(X) = X^2 - n$ splits into linear factors over $\mathbb{Q}_p$.*

(ii) *If p splits completely in K, there are isomorphisms $K_{\mathfrak{p}} \cong \mathbb{Q}_p \cong K_{\overline{\mathfrak{p}}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the prime ideals, dividing $p\mathbb{Z}$. In particular, the map*

$$\mu_1 \oplus \mu_2 : \mathbb{Q}_p \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{Q}_p \oplus \mathbb{Q}_p$$

induces isomorphisms

$$K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K \cong \mathbb{Q}_p \oplus \mathbb{Q}_p \cong K_{\mathfrak{p}} \oplus K_{\overline{\mathfrak{p}}}.$$

Proof: (i) Let p be odd. By Theorem 1.6., we know that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ if and only if the discriminant d_K is a square modulo p. This is equivalent to n being a square modulo p, since the possible values of d_K are n and $4n$ and p is odd. So we have to show that n is a square modulo p if and only if n is a square in $\mathbb{Q}_p$.

If $f(X)$ splits into distinct linear factors modulo p, then by Hensel's lemma, $f(X)$ splits into linear factors over $\mathbb{Q}_p$. Conversely, if n is a square in $\mathbb{Q}_p$, we see that $\sqrt{n}_p \in \mathbb{Z}_p$, since $2v_p(\sqrt{n}_p) = v_p(n)$ and $v_p(n) \geq 0$. If we take p-adic expansions and reduce the equation ${\sqrt{n}_p}^2 = n$ modulo p, we are done.

Again by Theorem 1.6., we know that the prime 2 splits completely in K, if and only if $d_K \equiv 1 \mod 8$. By the definition of the discriminant, this is equivalent to $n \equiv 1 \mod 8$.

Let $n = 8a + 1$ with $a \in \mathbb{Z}$ and consider the polynomial

$$g(X) = X^2 + X - 2a \in \mathbb{Z}_2[X].$$

We have

$$g(X) \equiv X^2 + X \equiv X(X+1) \mod 2$$

and so, by Hensel's lemma, $g(X)$ has two roots in $\mathbb{Z}_2$. Let α be one of these roots. Then

$$\alpha^2 + \alpha = 2a,$$

which implies

$$1 + 4\alpha + 4\alpha^2 = 8a + 1,$$

or equivalently

$$(1 + 2\alpha)^2 = n,$$

proving that n is a square in $\mathbb{Q}_2$.

Conversely, if n is a square in $\mathbb{Q}_2$, then $0 \leq v_2(n) \leq 1$, since n is squarefree and consequently $v_2(\sqrt{n}_2) = 0$. Taking 2-adic expansions, a straightforward computation shows that $n \equiv 1 \mod 8$ and we are done.

(ii) Let v_p and $v_{\mathbb{Q}_p}$ denote the p-adic valuations in $\mathbb{Q}$ and $\mathbb{Q}_p$ respectively. We have a canonical embedding

$$K \hookrightarrow \mathbb{Q}_p \otimes_{\mathbb{Q}} K$$

and hence, by restricting the maps μ_i from above to K, continuous homomorphisms

$$\mu_i|_K : K \longrightarrow \mathbb{Q}_p, \ i = 1, 2.$$

Let $a, b \in \mathbb{Q}$ nonzero and $\alpha = a + b\sqrt{n} \in K$. Then $\mu_i(\alpha) = 0$ if and only if

$$\sqrt{n}_p = \pm\frac{a}{b},$$

which is impossible, since $\sqrt{n}_p$ is not rational and we see that the $\mu_i|_K$ are injective.

The canonical embedding of $\mathbb{Q}$ in $\mathbb{Q}_p$ factors through

$$\mathbb{Q} \hookrightarrow K \xrightarrow{\mu_i} \mathbb{Q}_p.$$

By continuity, we see that the restriction $v_{\mathbb{Q}_p}|_K = v_i$ with respect to the embedding μ_i defines a discrete valuation in K, extending the valuation v_p. Since $\mathbb{Q}_p$ is complete with respect to $v_{\mathbb{Q}_p}$, it is the completion of K with respect to v_i, i.e. $K_{v_i} = \mathbb{Q}_p$.

To identify the valuation v_i, we need to determine the prime ideals

$$\mathfrak{p}_i = \{x \in K : v_i(x) \geq 1\},$$

corresponding to v_i. Since $v_{\mathbb{Q}_p}(p) = 1$, we have $v_i(p) = 1$ as well. This means that $\mathfrak{p}_i$ contains $p\mathcal{O}_K$ but $\mathfrak{p}_i^2$ does not.

Let $\sqrt{n}_p \equiv n_0 \mod p$ with $n_0 \in \mathbb{Z}$. Since n is a unit in $\mathbb{Z}_p$, so is $\sqrt{n}_p$ and we have $n_0 \neq 0$. Then

$$v_{\mathbb{Q}_p}(n_0 - \sqrt{n}_p) = v_{\mathbb{Q}_p}(-n_0 + \sqrt{n}_p) \geq 1,$$

which implies

$$v_1(-n_0 + \sqrt{n}) = v_2(n_0 + \sqrt{n}) \geq 1,$$

so that $\mathfrak{p}_1$ contains the ideal $(p, \sqrt{n} - n_0)$ and $\mathfrak{p}_2$ contains $(p, \sqrt{n} + n_0)$.

Assume $n \not\equiv 1 \mod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$ and as we have seen in the proof of (i), p is odd. Then

$$X^2 - n \equiv (X - n_0)(X + n_0) \mod p$$

and by Proposition 1.4., we have

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},$$

where $\mathfrak{p} = (p, \sqrt{n} - n_0)$ and $\overline{\mathfrak{p}} = (p, \sqrt{n} + n_0)$, which shows that

$$\mathfrak{p}_1 = \mathfrak{p} = \overline{\mathfrak{p}}_2$$

and

$$K_{\mathfrak{p}} = K_{v_1} \cong \mathbb{Q}_p \cong K_{v_2} = K_{\overline{\mathfrak{p}}}.$$

If $n \equiv 1 \mod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where

$$\alpha = \frac{1 + \sqrt{n}}{2}$$

with minimal polynomial

$$g(X) = X^2 - X - \frac{n-1}{4}.$$

A straightforward computation shows that

$$g_1(\alpha) = \frac{\sqrt{n} - n_0}{2} \text{ and } g_2(\alpha) = \frac{\sqrt{n} + n_0}{2},$$

where g_1 and g_2 are the linear factors of g modulo p, i.e. $g \equiv g_1 g_2 \mod p$. If p is odd, then 2 is a unit in $\mathbb{Z}_p$, so the denominator does not change the valuations.

If $p = 2$, then $n \equiv 1 \mod 8$ and it is easy to check that $\sqrt{n}_2 \equiv 1 \mod 4$ and so the valuation of

$$\frac{\sqrt{n} - 1}{2}$$

is still positive. By applying these arguments to $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we see again that

$$\mathfrak{p} \subseteq \mathfrak{p}_1 \text{ and } \overline{\mathfrak{p}} \subseteq \mathfrak{p}_2$$

and consequently

$$\mathfrak{p}_1 = \mathfrak{p} = \overline{\mathfrak{p}_2}.$$

□

(2) If $f(X)$ is irreducible over $\mathbb{Q}_p$, we have a field extension $\mathbb{Q}_p(\sqrt{n})/\mathbb{Q}_p$ of degree 2 inside the algebraic closure $\overline{\mathbb{Q}_p}$ and we obtain the continuous isomorphism

$$\mu : \mathbb{Q}_p \otimes_{\mathbb{Q}} K \cong \mathbb{Q}_p(\sqrt{\mathbf{n}}) \longrightarrow \mathbb{Q}_p(\sqrt{n}),$$

mapping $\sqrt{\mathbf{n}}$ to $\sqrt{n}$, where we have the product topology on $\mathbb{Q}_p^2$ on both sides and the obvious embedding

$$K = \mathbb{Q}(\sqrt{n}) \hookrightarrow \mathbb{Q}_p(\sqrt{n}).$$

Proposition 4.4. *Let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic number field and let p be a prime number. Assume that $f(X) = X^2 - n$ is irreducible over $\mathbb{Q}_p$. Then there is only one prime ideal $\mathfrak{p}$ dividing $p\mathbb{Z}$ and there are isomorphisms*

$$K_{\mathfrak{p}} \cong \mathbb{Q}_p(\sqrt{n}) \cong K_p,$$

induced by

$$\mu : \mathbb{Q}_p \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{Q}_p(\sqrt{n}).$$

Proof: We know by Proposition 4.3. that p does not split completely in K and so there is a unique prime ideal $\mathfrak{p}$ dividing $p\mathbb{Z}$. Again, we have an embedding

$$\mathbb{Q} \hookrightarrow K \xrightarrow{\mu} \mathbb{Q}_p(\sqrt{n})$$

and by continuity, we obtain a discrete valuation $v = v_{\mathbb{Q}_p(\sqrt{n})}|_K$ in K, extending v_p with index 1 or 2. Either way, we see that $v(p) > 0$ and so the prime ideal $\mathfrak{p}_v$, associated with the valuation v contains the ideal $p\mathcal{O}_K$. But we already know that $\mathfrak{p}$ is the unique prime ideal containing $p\mathcal{O}_K$ and so

$$\mathfrak{p}_v = \mathfrak{p}$$

and

$$K_{\mathfrak{p}} = K_v \cong \mathbb{Q}_p(\sqrt{n}),$$

since $\mathbb{Q}_p(\sqrt{n})$ is a complete field by Proposition 1.7.. □

From Propositions 4.3. and 4.4., we obtain the immediate

Corollary 4.5. *There are isomorphisms*

$$K_p \cong \prod_{\mathfrak{p}|p\mathbb{Z}} K_{\mathfrak{p}}$$

and

$$\prod_{p \text{ prime}} K_p \cong \prod_{\mathfrak{p} \text{ prime ideal}} K_{\mathfrak{p}}.$$

In particular, we can identify the idèle group $\mathbf{I}_K$ with the restricted product of the K_p's. □

Alternatively, one could show the general result, that for a Galois extension of number fields L/K and a prime $\mathfrak{p}$ of K there is an isomorphism

$$K_{\mathfrak{p}} \otimes_K L \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}.$$

For proofs, see [Ser79, Chapter II, §3, Theorem 1 (iii)] and [CasFro67, Theorem, p. 57].

We can now describe the map

$$q_{z,p} : K_p^* \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p),$$

where $K_p^* = (\mathbb{Q}_p \otimes_{\mathbb{Q}} K)^*$ and $\mathrm{GL}_2(\mathbb{Q}_p)$ are necessarily endowed with the product topology on $\mathbb{Q}_p^2$ and $\mathbb{Q}_p^4$ respectively. This follows from the fact that any topology on a finite dimensional vector space over $\mathbb{Q}_p$ is equivalent to the product topology. For a proof, see [Gou97, Theorem 5.2.1].

Let

$$\xi = a + b\sqrt{\mathbf{n}} \in (\mathbb{Q}_p \otimes_{\mathbb{Q}} K)^*$$

with $a, b \in \mathbb{Q}_p$. We can approximate a and b with rational sequences $a_k, b_k \in \mathbb{Q}$ respectively to obtain $a_k + b_k\sqrt{\mathbf{n}}$, which corresponds to the element

$$\xi_k = a_k + b_k\sqrt{n} \in K$$

via the canonical embedding and we obtain

$$q_{z,p}(\xi) = \lim_{k\to\infty} q_z(\xi_k) = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{b(ny^2 - x^2)}{y} \\ \dfrac{b}{y} & a - \dfrac{bx}{y} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p).$$

We will see this in more detail later on in sections 4.2-4.4.

It is then clear that the map

$$q_z : \mathbf{I}_K \longrightarrow \mathrm{GL}_2(\mathbb{A})$$

is the componentwise extension of the $q_{z,p}$'s. However, we still need to check that q_z is well-defined.

Proposition 4.6. *The map*

$$q_z : \mathbf{I}_K \longrightarrow \mathrm{GL}_2(\mathbb{A})$$

is well-defined, i.e. $q_z(s) \in \mathrm{GL}_2(\mathbb{A})$ *for every idèle* s.

Proof: Let

$$s = (s_{\mathfrak{p}_1}, s_{\mathfrak{p}_2}, \dots) \in \mathbf{I}_K.$$

We need to show that all but finitely many components of $q_z(s)$ are contained in $\mathrm{GL}_2(\mathbb{Z}_p)$. We can ignore the finitely many $s_{\mathfrak{p}}$, where $s_{\mathfrak{p}}$ is not a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$.

Furthermore, by Theorem 1.6., we see that a prime number p ramifies in K if and only if it divides the discriminant d_K. Since there are only finitely many such p, we can ignore them as well.

Assume that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ for an odd prime p and that $s_{\mathfrak{p}}$ and $s_{\overline{\mathfrak{p}}}$ are units in $\mathcal{O}_{K_{\mathfrak{p}}}$ and $\mathcal{O}_{K_{\overline{\mathfrak{p}}}}$ respectively. Since

$$K_{\mathfrak{p}} \cong \mathbb{Q}_p \cong K_{\overline{\mathfrak{p}}},$$

the pair $(s_{\mathfrak{p}}, s_{\overline{\mathfrak{p}}})$ corresponds to an element

$$(\alpha, \beta) \in \mathbb{Q}_p \oplus \mathbb{Q}_p,$$

where α and β are units in $\mathbb{Z}_p$. By taking the inverse of (α, β) under $\mu_1 \oplus \mu_2$, we obtain the element

$$\xi = \frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2\sqrt{n}_p}\sqrt{\mathbf{n}} \in \mathbb{Q}_p \otimes_{\mathbb{Q}} K.$$

By setting

$$a = \frac{\alpha+\beta}{2} \text{ and } b = \frac{\alpha-\beta}{2\sqrt{n}_p},$$

we obtain again the matrix

$$q_{z,p}(\xi) = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{b(ny^2 - x^2)}{y} \\ \dfrac{b}{y} & a - \dfrac{bx}{y} \end{pmatrix}$$

with unit determinant $a^2 - nb^2 = \alpha\beta$. Now, x and y are both units in $\mathbb{Z}_p$ for all but finitely many p, so it is enough to show that $a, b \in \mathbb{Z}_p$, but this is clear since $\sqrt{n}_p$ is a unit in $\mathbb{Z}_p$.

If $p\mathcal{O}_K = \mathfrak{p}$ for an odd prime p and $s_{\mathfrak{p}}$ is a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$, then $s_{\mathfrak{p}}$ corresponds under μ to an element

$$\xi = a + b\sqrt{n} \in \mathbb{Q}_p(\sqrt{n}) \cong \mathbb{Q}_p(\sqrt{\mathbf{n}})$$

of valuation 0. By Proposition 1.9., we have the formula

$$v_{\mathbb{Q}_p(\sqrt{n})}(\xi) = \frac{v_p(N_{\mathbb{Q}_p(\sqrt{n})/\mathbb{Q}_p})(\xi)}{f},$$

where f is the inertia index of the extension $\mathbb{Q}_p(\sqrt{n})/\mathbb{Q}_p$ and we see that ξ is a unit in $\mathbb{Q}_p(\sqrt{n})$ if and only if $\det(q_{z,p}(\xi)) = a^2 - nb^2$ is a unit in $\mathbb{Z}_p$.

By Theorem 1.6., we know that $p \nmid n$, so that n is a unit in $\mathbb{Z}_p$ and that n is not a square modulo p. By the properties of discrete valuations, we have

$$0 = v_p(a^2 - nb^2) \geq \min(v_p(a^2), v_p(-nb^2)) = 2\min(v_p(a), v_p(b))$$

and it is easy to check that we have equality if $v_p(a) \neq v_p(b)$.

Assume that $v_p(a) = v_p(b) = m < 0$ and let a_m, b_m and n_0 be the first nonzero coefficients of the p-adic expansions of a, b and n respectively. Then we have

$$a_m^2 \equiv n_0 b_m^2 \mod p,$$

which is impossible since n is not a square modulo p. This proves that $a, b \in \mathbb{Z}_p$ and consequently $q_{z,p}(\xi) \in \mathrm{GL}_2(\mathbb{Z}_p)$. □

The next step is to understand the map

$$\sigma : \mathrm{GL}_2(\mathbb{A}) \longrightarrow \mathrm{Aut}(\mathbf{F}).$$

We know from Proposition 3.10. that we can write any element $x \in \mathrm{GL}_2(\mathbb{A})$ as $x = \alpha u$, with

$$\alpha \in \mathrm{GL}_2(\mathbb{Q})^+ \text{ and } u \in U = \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p).$$

Then

$$\sigma(x) = \sigma(\alpha u) = \sigma_\alpha \sigma_u$$

and the action on a modular function $f \in \mathrm{Aut}(\mathbf{F})$ is given by

$$f^{\sigma(x)} = f^{\sigma_\alpha \sigma_u} = (f^{\sigma_\alpha})^{\sigma_u}.$$

Here, σ_α acts on f by

$$f^{\sigma_\alpha}(\tau) = f(\alpha\tau),$$

for $\tau \in \mathfrak{h}$, such that $f(\alpha\tau)$ is defined.

Let now $f \in \mathbf{F}_N$. To understand the action of σ_u on f, we need to extract a matrix $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ from u in a canonical way, since by Theorem 3.8., we have an isomorphism

$$\mathrm{Gal}(\mathbf{F}_N/\mathbf{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1.$$

Let $N = p_1^{r_1} ... p_l^{r_l}$. First of all, we have the obvious isomorphism

$$U = \prod_{q \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_q) \cong \mathrm{GL}_2\Big(\prod_{q \text{ prime}} \mathbb{Z}_q\Big).$$

Recall that we can identify $\mathbb{Z}_q$ with a subring of

$$\prod_{r \in \mathbb{N}} \mathbb{Z}/q^r\mathbb{Z},$$

yielding the maps

$$\prod_{q \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_q) \longrightarrow \mathrm{GL}_2\Big(\prod_{q,r} \mathbb{Z}/q^r\mathbb{Z}\Big) \longrightarrow \mathrm{GL}_2\Big(\mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_l^{r_l}\mathbb{Z}\Big),$$

where the last map is the projection onto the components $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$. By the chinese remainder theorem, we get a well-defined element $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If u has components u_p, then we can characterise $\tilde{u}$ by

$$\tilde{u} \equiv u_{p_i} \mod p_i^{r_i} \text{ for all } i = 1, ..., l. \tag{4.1.1}$$

Let

$$\sum_{k=-\infty}^{\infty} a_k q^{k/N}$$

be the q-expansion of $f(\tau)$ with $q = e^{2\pi i\tau}$ and $a_k \in \mathbb{Q}(\zeta_N)$ for a primitive N-th root of unity ζ_N. Let us write $a_k = g_k(\zeta_N)$ for polynomials $g_k \in \mathbb{Q}[X]$. From Theorem 3.8., we know that $\tilde{u}$ acts on the coefficients a_k by

$$g_k(\zeta_N) \mapsto g_k(\zeta_N^{\det(\tilde{u})}).$$

To extract the determinant, we can decompose $\tilde{u}$ as

$$\tilde{u} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{d} \end{pmatrix} \tilde{\gamma}$$

with $\overline{d} = \det(\tilde{u})$ and $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since we have an isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_N \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

we can lift the matrix $\tilde{\gamma}$ to $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\gamma \equiv \tilde{\gamma} \mod N \tag{4.1.2}$$

and the action of γ on $f(\tau)$ is then given by $f(\gamma\tau)$. To summarize these results, we have the following

Proposition 4.7. *Let $f \in \boldsymbol{F}_N$ with q-expansion*

$$\sum_{k=-\infty}^{\infty} g_k(\zeta_N)(e^{2\pi i\tau})^{k/N}$$

and let $u, \tilde{u}$ and γ be as in (4.1.1) and (4.1.2). Then the action of σ_u on f is given by

$$f^{\sigma_u}(\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_N^{\det(\tilde{u})})(e^{2\pi i\gamma\tau})^{k/N}.$$

□

Let $f \in \mathbf{F}_N$. To finally assemble the action $(f^{\sigma_\alpha})^{\sigma_u}$, we still need to determine the level of $f^{\sigma_\alpha}(\tau) = f(\alpha\tau)$. Since multiplying α with a scalar matrix does not change its

action on $\mathfrak{h}$, we can take any multiple of α with integer entries. If $\tilde{\alpha}$ is such a matrix, then we have

$$f^{\sigma_\alpha}(\tau) = f(\alpha\tau) = f(\tilde{\alpha}\tau) = f^{\tilde{\alpha}}(\tau).$$

Lemma 4.8. *Let $\tilde{\alpha}$ be a matrix with integer entries and positive determinant d and let $f \in \mathbf{F}_N$. Then $f^{\tilde{\alpha}} \in \mathbf{F}_{dN}$.*

Proof: Let $\gamma \in \Gamma_{dN}$. Then we can write $\gamma = I + dN\delta$, where δ has integer entries. The matrix

$$\tilde{\alpha}\gamma\tilde{\alpha}^{-1} = I + dN\tilde{\alpha}\delta\tilde{\alpha}^{-1}$$

has unit determinant and since $d\tilde{\alpha}^{-1}$ has integer entries, we see that $\tilde{\alpha}\gamma\tilde{\alpha}^{-1} \in \Gamma_N$. So for every $\gamma \in \Gamma_{dN}$ there is $\tilde{\gamma} \in \Gamma_N$, such that $\tilde{\alpha}\gamma = \tilde{\gamma}\tilde{\alpha}$ and we obtain

$$f^{\tilde{\alpha}}(\gamma\tau) = f(\tilde{\alpha}\gamma\tau) = f(\tilde{\gamma}\tilde{\alpha}\tau) = f(\tilde{\alpha}\tau) = f^{\tilde{\alpha}}(\tau),$$

showing that $f^{\tilde{\alpha}}$ is invariant under Γ_{dN}.

Let now $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z})$. We need to show that $f^{\tilde{\alpha}\tilde{\gamma}}(\tau) = f(\tilde{\alpha}\tilde{\gamma}\tau)$ has a q-expansion in $q^{1/dN}$ with only finitely many terms with negative exponents. It is easy to check that a matrix with integer entries and determinant d can be written in the form

$$\gamma \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

with $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $a, b, c \in \mathbb{Z}$, satisfying $ac = d$. Since $\tilde{\alpha}\tilde{\gamma}$ is such a matrix, we can write $\tilde{\alpha}\tilde{\gamma} = \gamma\alpha'$, where

$$\alpha' = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

and we have $f(\tilde{\alpha}\tilde{\gamma}\tau) = f(\gamma\alpha'\tau)$. Let

$$\sum_{k=-\infty}^{\infty} a_k q^{k/N}$$

be the q-expansion of $f(\gamma\tau)$, having only finitely many terms with negative exponents. Now

$$\alpha'\tau = \frac{a\tau + b}{c} = \frac{a^2\tau + ab}{d}$$

and

$$a_k(e^{2\pi i\alpha'\tau})^{k/N} = a_k(e^{2\pi i/dN})^{abk}(e^{2\pi i\tau})^{a^2k/dN} = a'_k q^{a^2k/dN}.$$

Since a^2 and d are positive, we have only finitely many terms with negative exponents and since $f^{\tilde{\alpha}}$ is clearly meromorphic on $\mathfrak{h}$, we are done. □

We can now summarize as follows.

Corollary 4.9. *Let $f \in \mathbf{F}_N$ and $x = \alpha u \in \mathrm{GL}_2(\mathbb{A})$. Let $\tilde{\alpha}$ be a scalar multiple of α with integer entries and determinant d and let $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/dN\mathbb{Z})$ be the matrix induced by u, as in (4.1.1) with $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as in Proposition 4.7.. If*

$$\sum_{k=-\infty}^{\infty} g_k(\zeta_N) q^{k/N}$$

is the q-expansion of $f(\tau)$ with $g_k \in \mathbb{Q}[X]$ and

$$f^{\sigma_\alpha}(\tau) = f(\alpha\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_N)(e^{2\pi i\alpha\tau})^{k/N} = \sum_{k=-\infty}^{\infty} \tilde{g_k}(\zeta_{dN}) q^{k/dN}$$

is the q-expansion of f^{σ_α}, then we have

$$(f^{\sigma_\alpha})^{\sigma_u}(\tau) = \sum_{k=-\infty}^{\infty} \tilde{g_k}(\zeta_{dN}{}^{\det(\tilde{u})})(e^{2\pi i\gamma\tau})^{k/dN}.$$

□

We now have the necessary tools to explicitly describe $\sigma_z(\mathfrak{n}_\mathfrak{p})$, where $\mathfrak{n}_\mathfrak{p} = (1, ..., \varpi_\mathfrak{p}, ..., 1)$. Let $K = \mathbb{Q}(\sqrt{n})$ be an imaginary quadratic number field, let p be a prime number and let $z = x + y\sqrt{n} \in K \cap \mathfrak{h}$. There are three cases to consider.

4.2 The Case $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$

If p splits completely in K, the polynomial $X^2 - n$ splits into linear factors over $\mathbb{Q}_p$ by Proposition 4.3. and we have isomorphisms

$$K_p = \mathbb{Q}_p \otimes_\mathbb{Q} K \cong \mathbb{Q}_p \oplus \mathbb{Q}_p \cong K_\mathfrak{p} \oplus K_{\bar{\mathfrak{p}}}.$$

The element

$$(\varpi_\mathfrak{p}, 1) \in K_\mathfrak{p} \oplus K_{\bar{\mathfrak{p}}}$$

can then be identified with an element of the form

$$(p\varepsilon, 1) \in \mathbb{Q}_p \oplus \mathbb{Q}_p,$$

where ε is a unit in $\mathbb{Z}_p$.

This element maps to

$$\xi = \frac{p\varepsilon + 1}{2} + \frac{p\varepsilon - 1}{2\sqrt{n}_p}\sqrt{\mathbf{n}} = \frac{p\varepsilon + 1}{2}(1 \otimes 1) + \frac{p\varepsilon - 1}{2\sqrt{n}_p}(1 \otimes \sqrt{n}) \in \mathbb{Q}_p \otimes_\mathbb{Q} K$$

via the inverse of the isomorphism $\mu_1 \oplus \mu_2$ given by

$$a_1 + a_2\sqrt{\mathbf{n}} \mapsto (a_1 + a_2\sqrt{n}_p, a_1 - a_2\sqrt{n}_p),$$

where $\sqrt{n}_p$ is a root of $X^2 - n$ in $\mathbb{Q}_p$.

We can now approximate $\varepsilon, \sqrt{n}_p \in \mathbb{Z}_p$ by sequences $\varepsilon_k, \beta_k \in \mathbb{Z}$ respectively, such that for all $k \in \mathbb{N}$, we have

$$\varepsilon_k \equiv \varepsilon \mod p^k$$
$$\beta_k \equiv \sqrt{n}_p \mod p^k.$$

This can be easily achieved by taking the p-adic expansions of ε and $\sqrt{n}_p$. If p is odd and $n \equiv 1 \mod p$, we can even take the p-adic binomial expansion of $\sqrt{n}_p$, given by

$$(1+\eta p)^{1/2} = \sum_{l=0}^{\infty} \binom{1/2}{l} \eta^l p^l,$$

where

$$\binom{1/2}{l} = \frac{1/2(1/2-1)...(1/2-l+1)}{l!}.$$

If we set $\eta = \frac{n-1}{p}$, then $\eta, \binom{1/2}{l} \in \mathbb{Z}_p$, the series converges (for a proof, see [Gou97, Lemma 4.5.11 and Corollary 4.5.12]) and we can approximate by setting

$$\beta_k = \sum_{l=0}^{k} \binom{1/2}{l} \eta^l p^l.$$

We then obtain the sequence

$$\xi_k = \frac{p\varepsilon_k + 1}{2} + \frac{p\varepsilon_k - 1}{2\beta_k}\sqrt{n} \in K \subseteq \mathbb{Q}_p \otimes_{\mathbb{Q}} K.$$

From Lemma 4.2. we obtain

$$q_z(\xi_k) = \begin{pmatrix} \frac{p\varepsilon_k+1}{2} + \frac{(p\varepsilon_k-1)x}{2y\beta_k} & \frac{(p\varepsilon_k-1)(ny^2-x^2)}{2y\beta_k} \\ \frac{p\varepsilon_k-1}{2y\beta_k} & \frac{p\varepsilon_k+1}{2} - \frac{(p\varepsilon_k-1)x}{2y\beta_k} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+.$$

and by taking limits, we get the following

Lemma 4.10. *We have*

$$q_{z,p}(\xi) = \lim_{k\to\infty} q_z(\xi_k) = \begin{pmatrix} \frac{p\varepsilon+1}{2} + \frac{(p\varepsilon-1)x}{2y\sqrt{n}_p} & \frac{(p\varepsilon-1)(ny^2-x^2)}{2y\sqrt{n}_p} \\ \frac{p\varepsilon-1}{2y\sqrt{n}_p} & \frac{p\varepsilon+1}{2} - \frac{(p\varepsilon-1)x}{2y\sqrt{n}_p} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

with

$$\det(q_{z,p}(\xi)) = p\varepsilon.$$

□

We normalize the determinant by multiplying the matrix with $A = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{p} \end{pmatrix}$ on the left and with $B = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\varepsilon} \end{pmatrix}$ on the right. Note that $A \in \mathrm{GL}_2(\mathbb{Z}_q)$ for all prime numbers $p \neq q$ and $B \in \mathrm{GL}_2(\mathbb{Z}_p)$. In the setting of idèles, we have

$$q_z(\mathfrak{n}_\mathfrak{p}) = (I, ..., q_{z,p}(\xi), ..., I) = A^{-1}(I, ..., Aq_{z,p}(\xi)B, ..., I)(A, ..., B^{-1}, .., A) \in \mathrm{GL}_2(\mathbb{A}),$$

with $q_{z,p}(\xi)$ at position p, where

$$(I, ..., Aq_{z,p}(\xi)B, ..., I) \in \ \mathrm{SL}_2(\mathbb{A})$$

and

$$(A, ..., B^{-1}, .., A) \in U = \prod_{q \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_q).$$

Let

$$X(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ and } Y(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

We have the following decomposition

$$Aq_{z,p}(\xi)B = \begin{pmatrix} \frac{p\varepsilon+1}{2} + \frac{(p\varepsilon-1)x}{2y\sqrt{n}_p} & \frac{(p\varepsilon-1)(ny^2-x^2)}{2y\varepsilon\sqrt{n}_p} \\ \frac{p\varepsilon-1}{2yp\sqrt{n}_p} & \frac{p\varepsilon+1}{2p\varepsilon} - \frac{(p\varepsilon-1)x}{2yp\varepsilon\sqrt{n}_p} \end{pmatrix} =$$

$$= X\big(px\big)X\big(py\sqrt{n}_p\big)Y\bigg(\frac{p\varepsilon-1}{2py\sqrt{n}_p}\bigg)X\bigg(-\frac{y\sqrt{n}_p}{\varepsilon}\bigg)X\bigg(-\frac{x}{\varepsilon}\bigg) =$$

$$= X\big(pz_p\big)Y\bigg(\frac{p\varepsilon-1}{2py\sqrt{n}_p}\bigg)X\big(-\frac{z_p}{\varepsilon}\big),$$

where $z_p = x + y\sqrt{n}_p = \mu_1(z)$.

By taking p-adic expansions we may rewrite this as

$$X\bigg(\sum_{i=-k}^{\infty} a_i p^i\bigg)Y\bigg(\sum_{i=-k}^{\infty} b_i p^i\bigg)X\bigg(\sum_{i=-k}^{\infty} c_i p^i\bigg),$$

for $a_i, b_i, c_i \in \mathbb{Z}$ and a sufficiently large positive integer k and we can approximate with

$$C = X\bigg(\sum_{i=-k}^{m} a_i p^i\bigg)Y\bigg(\sum_{i=-k}^{m} b_i p^i\bigg)X\bigg(\sum_{i=-k}^{m} c_i p^i\bigg) \in \mathrm{SL}_2(\mathbb{Q}),$$

for a sufficiently large positive integer m, say $m \geq 4k-1$, so that we have

$$\tilde{I} = C^{-1}Aq_{z,p}B \in \mathrm{SL}_2(\mathbb{Z}_p).$$

This yields our final decomposition

$$q_z(\mathfrak{n}_\mathfrak{p}) = (I, ..., q_{z,p}(\xi), ..., I) = \alpha u = A^{-1}C(C^{-1}A, C^{-1}A, ..., \tilde{I}B^{-1}, ..., C^{-1}A, C^{-1}A),$$

where $\alpha = A^{-1}C \in \ \mathrm{GL}_2(\mathbb{Q})^+$ and

$$u = (C^{-1}A, C^{-1}A, ..., \tilde{I}B^{-1}, ..., C^{-1}A, C^{-1}A) \in U,$$

since p is the only prime appearing in the denominators of the entries of C.

Let $f \in \mathbf{F}_{p^\ell N}$, where p does not divide $N = p_1^{r_1}...p_l^{r_l}$. Since $p^{3k}\alpha$ has integer entries, we have

$$f^{\sigma_\alpha} \in \mathbf{F}_{p^r N} \text{ with } r = 6k + \ell + 1. \tag{4.2.1}$$

We obtain the induced matrix

$$\tilde{u} = \left(\tilde{I}B^{-1}, C^{-1}A..., C^{-1}A\right) \in \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times ... \times \mathrm{GL}_2(\mathbb{Z}/p_l^{r_l}\mathbb{Z})$$

or equivalently

$$\tilde{u} = \left(\tilde{I}B^{-1}, C^{-1}A\right) \in \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}). \tag{4.2.2}$$

We will see in the discussion following Example 4.12., that we can choose an approximating matrix C, such that

$$\tilde{I} \equiv I \mod p^r \tag{4.2.3}$$

and so we may assume that

$$\tilde{u} = \left(B^{-1}, C^{-1}A\right) \in \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

with determinant

$$(\overline{\varepsilon}, \overline{p}^{-1}) \in (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*,$$

yielding the decomposition

$$\tilde{u} = \left(\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{\varepsilon} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{p}^{-1} \end{pmatrix}\right)(I, \tilde{\gamma})$$

for a matrix $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. We can lift $\tilde{\gamma}$ to $\gamma \in \Gamma_{p^r}$, satisfying

$$\gamma \equiv \tilde{\gamma} \mod N. \tag{4.2.4}$$

Then the action of $\tilde{u}$ is given by the usual action of γ and by $\zeta_{p^r} \mapsto \zeta_{p^r}^{\overline{\varepsilon}}$ and $\zeta_N \mapsto \zeta_N^{\overline{p}^{-1}}$ in $\mathbb{Q}(\zeta_{p^r N})$.

Theorem 4.11. *Let K be an imaginary quadratic number field, $z \in K \cap \mathfrak{h}$, $\mathfrak{n}_\mathfrak{p} = (1, ..., p\varepsilon, ..., 1)$ a prime idèle with $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and let f and $\tilde{u}$ be as in (4.2.1) and (4.2.2). If*

$$\sum_{k=-\infty}^{\infty} g_k(\zeta_{p^r}, \zeta_N)(e^{2\pi i\tau})^{k/p^rN}, \ g_k \in \mathbb{Q}[X, Y]$$

is the q-expansion of f^{σ_α}, then

$$(\mathfrak{n}_\mathfrak{p}^{-1}, K)f(z) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{p^r}^{\overline{\varepsilon}}, \zeta_N^{\overline{p}^{-1}})(e^{2\pi i\gamma z})^{k/p^rN},$$

for any matrix $\gamma \in \Gamma_{p^r}$, satisfying (4.2.4) and for any approximation, sufficiently strong to guarantee

$$\tilde{I} \equiv I \mod p^r$$

as in (4.2.3). □

Example 4.12. Let $p = 3, n = -2, \varepsilon = 1$ and $z = \sqrt{-2}$.

Then $B = I$ and

$$Aq_{z,3}(\xi) = \begin{pmatrix} 2 & \sqrt{-2}_3 \\ \dfrac{1}{3\sqrt{-2}_3} & \dfrac{2}{3} \end{pmatrix} = X\big(3\sqrt{-2}_3\big)Y\left(\frac{1}{3\sqrt{-2}_3}\right)X\big(-\sqrt{-2}_3\big).$$

We have the following 3-adic expansions

$$3\sqrt{-2}_3 = 0 + 1 \cdot 3 + 1 \cdot 9 + ...,$$
$$\frac{1}{3\sqrt{-2}_3} = 1 \cdot \frac{1}{3} + 2 + 1 \cdot 3 + ...,$$
$$-\sqrt{-2}_3 = 2 + 1 \cdot 3 + 0 \cdot 9 + ...$$

and we will approximate these values up to the 1-st power, i.e. $m = 1$. We get

$$C = \begin{pmatrix} 17 & 88 \\ \frac{16}{3} & \frac{83}{3} \end{pmatrix} \text{ and } \alpha = \begin{pmatrix} 17 & 88 \\ 16 & 83 \end{pmatrix}$$

with $\det(\alpha) = 3$. Let us take $f \in \mathbf{F}_1$, so that $f^{\sigma_\alpha} \in \mathbf{F}_3$ and a straightforward computation shows that

$$\tilde{I} \equiv \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \mod 3.$$

Since $\det(\tilde{I}) \equiv 1 \mod 3$, we need to lift to a matrix $\tilde{u} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tilde{u} \equiv \tilde{I} \mod 3$. An obvious choice is

$$\tilde{u} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Let $\tau \in \mathfrak{h}$. The action of $\sigma_\alpha \sigma_u$ can now be described as

$$(f^{\sigma_\alpha})^{\sigma_u}(\tau) = f(\alpha \tilde{u} \tau),$$

where

$$\alpha \tilde{u} \tau = \frac{88\tau + 71}{83\tau + 67}.$$

However, since f is $\mathrm{SL}_2(\mathbb{Z})$-invariant, this can be reduced to

$$\gamma \alpha \tilde{u} \tau = \frac{\tau - 1}{3}$$

via the matrix

$$\gamma = \begin{pmatrix} 50 & -53 \\ -83 & 88 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In particular, the action on $z = \sqrt{-2}$ is given by

$$\gamma \alpha \tilde{u} \sqrt{-2} = \frac{\sqrt{-2} - 1}{3}$$

and by Shimura's reciprocity law, we obtain

$$(\mathfrak{n}_\mathfrak{p}^{-1}, K) f(\sqrt{-2}) = f\left(\frac{\sqrt{-2} - 1}{3}\right),$$

where $\mathfrak{n}_\mathfrak{p}$ is the prime idèle $(1, ..., 3, ..., 1)$, with 3 at position $\mathfrak{p}$ and $\mathfrak{p}$ can be chosen as either $(3, \sqrt{-2} + 1)$ or $(3, \sqrt{-2} - 1)$.

In terms of lattices, we have the homothety

$$(\sqrt{-2} + 1)\left[1, \frac{\sqrt{-2} - 1}{3}\right] = [\sqrt{-2} + 1, -1] = [1, \sqrt{-2}]$$

and so

$$j(\sqrt{-2}) = j\left(\frac{\sqrt{-2} - 1}{3}\right)$$

for the j-function. Since j generates the field $\mathbf{F}_1$, we see that

$$f(\sqrt{-2}) = f\left(\frac{\sqrt{-2} - 1}{3}\right)$$

and so we have

$$(\mathfrak{n}_{\mathfrak{p}}^{-1}, K)f(\sqrt{-2}) = f(\sqrt{-2})$$

for every $f \in \mathbf{F}_1$.

This is not surprising, since we have $j(\sqrt{-2}) = 8000$ (for a proof, see [Cox13, pp. 194-195]) and so any Galois automorphism of the extension K^{ab}/K will act as the identity on $f(\sqrt{-2})$.

Remark 4.13. The case $f \in \mathbf{F}_1$ does not seem to be very interesting, however, the methods used in the example can be easily generalized to any $f \in \mathbf{F}_N$, as we will see in 4.3..

In Example 4.12. we had $\tilde{I} \not\equiv \pm I \mod 3$ because our approximation was too weak. If we have the matrix

$$Aq_{z,p}(\xi) = X\Big(\sum_{i=-k}^{\infty} a_i p^i\Big)Y\Big(\sum_{i=-k}^{\infty} b_i p^i\Big)X\Big(\sum_{i=-k}^{\infty} c_i p^i\Big), \tag{4.2.5}$$

assuming $\varepsilon = 1$, and approximate with

$$C = X\Big(\sum_{i=-k}^{m} a_i p^i\Big)Y\Big(\sum_{i=-k}^{m} b_i p^i\Big)X\Big(\sum_{i=-k}^{m} c_i p^i\Big), \tag{4.2.6}$$

then by explicitly computing

$$\tilde{I} = C^{-1}Aq_{z,p}(\xi),$$

we see by the properties of discrete valuations that taking any $m \geq 4k-1$ guarantees that $\tilde{I} \in \mathrm{SL}_2(\mathbb{Z}_p)$, as already mentioned above. Moreover, taking any $m \geq 4k+\ell-1$ yields

$$\tilde{I} \equiv I \mod p^{\ell}.$$

A similar argument for the matrix $\alpha = A^{-1}C$ shows that $\tilde{\alpha} = p^{3k}\alpha$ has integer entries with $\det(\tilde{\alpha}) = 6k+1$. For $f \in \mathbf{F}_{p^r}$, we then have $f^{\sigma_\alpha} \in \mathbf{F}_{p^{6k+r+1}}$ and by approximating with $m \geq 10k+r$, we only have to compute the matrix α, since $u \in U$ acts as the identity.

Note also that it is computationally efficient to take $m = 10k+r$, since the automorphism σ_z does not depend on the decomposition αu. To summarize, we have the following

Lemma 4.14. *Let $f \in \mathbf{F}_{p^r}$ and let A and $q_{z,p}(\xi)$ be as in (4.2.5). If $\mathfrak{n}_{\mathfrak{p}} = (1, ..., p, ..., 1)$, then*

$$(\mathfrak{n}_{\mathfrak{p}}^{-1}, K)f(z) = f(\alpha z),$$

where α is obtained by taking $m \geq 10k+r$ in (4.2.6). □

Of course, this bound may be relaxed if one of the elements to be approximated has valuation greater than $-k$. In Example 4.12. we had

$$v_3(3\sqrt{-2}_3) = 1,\ v_3((3\sqrt{-2}_3)^{-1}) = -1 \text{ and } v_3(-\sqrt{-2}_3) = 0$$

and so $k = 1$. Let $f \in \mathbf{F}_{3^r}$. A straightforward computation shows that taking any $m \geq 2 + r = 2k + r$ is sufficient to guarantee that u acts as the identity.

4.3 The Case $p\mathcal{O}_K = \mathfrak{p}$

4.3.1 The general Case

If p is inert in K, the polynomial $X^2 - n$ is irreducible over $\mathbb{Q}_p$ and we have isomorphisms

$$K_p \cong \mathbb{Q}_p(\sqrt{n}) \cong K_{\mathfrak{p}}$$

by Propositions 4.3. and 4.4..

Let $\varpi_{\mathfrak{p}} = \xi = a + b\sqrt{n} \in \mathbb{Q}_p(\sqrt{n})$ and denote by v_p and $v_{\mathfrak{p}}$ the discrete valuations in $\mathbb{Q}_p$ and $\mathbb{Q}_p(\sqrt{n})$ respectively. We know from Proposition 1.9. that

$$v_{\mathfrak{p}}(\xi) = \frac{v_p(N_{\mathbb{Q}_p(\sqrt{n})/\mathbb{Q}_p}(\xi))}{f},$$

where f is the inertia index of the extension $\mathbb{Q}_p(\sqrt{n})/\mathbb{Q}_p$. This yields

$$v_{\mathfrak{p}}(\xi) = \frac{v_p(a^2 - nb^2)}{2}$$

and so ξ is a prime element if and only if

$$v_p(a^2 - nb^2) = 2$$

or in other words, if $\frac{a^2-nb^2}{p^2}$ is a unit in $\mathbb{Z}_p$. Similar to the first case, we can approximate a and b with sequences $a_k, b_k \in \mathbb{Q}$ respectively to obtain

$$\xi_k = a_k + b_k\sqrt{n} \in K \subseteq \mathbb{Q}_p(\sqrt{n})$$

and the matrix

$$q_z(\xi_k) = \begin{pmatrix} a_k + \dfrac{b_k x}{y} & \dfrac{b_k(ny^2 - x^2)}{y} \\ \dfrac{b_k}{y} & a_k - \dfrac{b_k x}{y} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+.$$

Lemma 4.15. *We have*

$$q_{z,p}(\xi) = \lim_{k\to\infty} q_z(\xi_k) = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{b(ny^2 - x^2)}{y} \\ \dfrac{b}{y} & a - \dfrac{bx}{y} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

with $\det(q_{z,p}(\xi)) = a^2 - nb^2$. □

We obtain

$$q_z(\mathfrak{n}_\mathfrak{p}) = (I, ..., q_{z,p}(\xi), ..., I) = A^{-1}(I, ..., Aq_{z,p}(\xi)B, ..., I)(A, ..., B^{-1}, .., A),$$

where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{1}{p^2} \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{p^2}{a^2 - nb^2} \end{pmatrix}.$$

We have $A \in \mathrm{GL}_2(\mathbb{Z}_q)$ for every prime $q \neq p$ and $B \in \mathrm{GL}_2(\mathbb{Z}_p)$. Assuming $b \neq 0$, we have the following decomposition

$$Aq_{z,p}(\xi)B = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{bp^2(ny^2 - x^2)}{y(a^2 - nb^2)} \\ \dfrac{b}{p^2 y} & \dfrac{ay - bx}{y(a^2 - nb^2)} \end{pmatrix} =$$

$$= X(p^2 x)X\left(\frac{p^2 ya}{b}\right)X\left(-\frac{p^2 y}{b}\right)Y\left(\frac{b}{p^2 y}\right)X\left(-\frac{p^2 y}{b}\right)X\left(\frac{p^2 ya}{b(a^2 - nb^2)}\right)X\left(-\frac{p^2 x}{a^2 - nb^2}\right) =$$

$$= X\left(\frac{p^2(xb + ya - y)}{b}\right)Y\left(\frac{b}{p^2 y}\right)X\left(\frac{p^2(ya - y(a^2 - nb^2) - xb)}{b(a^2 - nb^2)}\right).$$

Similar to the first case, we can approximate with the matrix C by using p-adic expansions to obtain $\tilde{I} = C^{-1}Aq_{z,p}(\xi)B$ and the final decomposition

$$q_z(\mathfrak{n}_\mathfrak{p}) = \alpha u = A^{-1}C(C^{-1}A, ..., \tilde{I}B^{-1}, ..., C^{-1}A).$$

The action of $(\mathfrak{n}_\mathfrak{p}^{-1}, K)$ on $f(z)$ can then be described as in Theorem 4.11..

4.3.2 The special Case $\varpi_{\mathfrak{p}} = p$

If $b = 0$, we have the much simpler matrix

$$Aq_{z,p}(\xi)B = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}.$$

If we now take $\varpi_{\mathfrak{p}} = p$, then we have $B = I$,

$$Aq_{z,p}(\xi) = \begin{pmatrix} p & 0 \\ 0 & \frac{1}{p} \end{pmatrix}$$

and we can approximate by simply taking $C = Aq_{z,p}(\xi)$. We further have $\alpha = pI$ and

$$u = \left(p^{-1}I, ..., I, ..., p^{-1}I\right)$$

and so σ_α is the identity. Note that this decomposition is independent of the choice of z.

Similar to above, if $f \in \mathbf{F}_{p^r N}$, where p does not divide N, we obtain the induced matrix

$$\tilde{u} = \left(I, \overline{p}^{-1}I\right) \in \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/p^r N\mathbb{Z})$$

with determinant $(\overline{1}, \overline{p}^{-2}) \in (\mathbb{Z}/p^r\mathbb{Z})^* \times (\mathbb{Z}/N\mathbb{Z})^*$ and we have the decomposition

$$\tilde{u} = \left(I, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{p}^{-2} \end{pmatrix}\right)\left(I, \begin{pmatrix} \overline{p}^{-1} & \overline{0} \\ \overline{0} & \overline{p} \end{pmatrix}\right).$$

We can now lift the matrix

$$\left(I, \begin{pmatrix} \overline{p}^{-1} & \overline{0} \\ \overline{0} & \overline{p} \end{pmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/p^r N\mathbb{Z})$$

to a matrix

$$\gamma \in \Gamma_{p^r} \text{ satisfying } \gamma \equiv \begin{pmatrix} \overline{p}^{-1} & \overline{0} \\ \overline{0} & \overline{p} \end{pmatrix} \mod N.$$

This matrix will act in the usual way and the determinant $(\overline{1}, \overline{p}^{-2})$ will act on the coefficients of the q-expansion by $\zeta_N \mapsto \zeta_N^{\overline{p}^{-2}}$ and by leaving ζ_{p^r} fixed. Hence we can summarize as follows.

Theorem 4.16. *Let K be an imaginary quadratic field, $p\mathcal{O}_K = \mathfrak{p}$ and $\mathfrak{n}_{\mathfrak{p}} = (1, ..., p, ..., 1)$. If $f \in \mathbf{F}_{p^r N}$ with q-expansion*

$$\sum_{k=-\infty}^{\infty} g_k(\zeta_{p^r}, \zeta_N)(e^{2\pi i\tau})^{k/p^r N}, \; g_k \in \mathbb{Q}[X, Y],$$

where p and N are relatively prime, then

$$(\mathfrak{n}_{\mathfrak{p}}^{-1}, K)f(\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{p^r}, \zeta_N^{\overline{p}^{-2}})(e^{2\pi i\gamma\tau})^{k/p^rN}$$

for any $\tau \in K \cap \mathfrak{h}$, where $f(\tau)$ is defined and any matrix $\gamma \in \Gamma_{p^r}$, satisfying the congruence

$$\gamma \equiv \begin{pmatrix} \overline{p}^{-1} & \overline{0} \\ \overline{0} & \overline{p} \end{pmatrix} \mod N.$$

In particular, if $f \in \mathbf{F}_{p^r}$, we have

$$(\mathfrak{n}_{\mathfrak{p}}^{-1}, K)f(\tau) = f(\tau).$$

□

Example 4.17. Let $p = 5$ and $f \in \mathbf{F}_{17640}$. We have $17640 = 2^3 3^2 57^2$ and

$$\frac{1}{5} = 1 + 0 \cdot 2 + 1 \cdot 4 + \ldots \text{ in } \mathbb{Z}_2,$$

$$\frac{1}{5} = 2 + 0 \cdot 3 + \ldots \text{ in } \mathbb{Z}_3,$$

$$\frac{1}{5} = 3 + 1 \cdot 7 + \ldots \text{ in } \mathbb{Z}_7$$

and we obtain the element

$$(\overline{5}, \overline{2}, \overline{1}, \overline{10}) \in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z}$$

and thus the matrix

$$\tilde{u} = \begin{pmatrix} \overline{12701} & \overline{0} \\ \overline{0} & \overline{12701} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/17640\mathbb{Z})$$

with determinant $\overline{-2399}$ and so we have

$$\tilde{u} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{-2399} \end{pmatrix} \begin{pmatrix} \overline{12701} & \overline{0} \\ \overline{0} & \overline{7061} \end{pmatrix}.$$

We can lift the matrix

$$\begin{pmatrix} \overline{12701} & \overline{0} \\ \overline{0} & \overline{7061} \end{pmatrix}$$

to

$$\gamma = \begin{pmatrix} 12701 & 17640 \\ -521 \cdot 17640 & -724 \cdot 17640 + 7061 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Let

$$\sum_{k=-\infty}^{\infty} g_k(\zeta_{17640})(e^{2\pi i\tau})^{k/17640}$$

be the q-expansion of $f(\tau)$ and let $\mathfrak{n}_\mathfrak{p} = (1, ..., 5, ..., 1)$. Then we have

$$(\mathfrak{n}_\mathfrak{p}^{-1}, K)f(\tau) = \sum_{k=-\infty}^{\infty} g_k({\zeta_{17640}}^{-2399})(e^{2\pi i\gamma\tau})^{k/17640}$$

for every $\tau \in K \cap \mathfrak{h}$, where $f(\tau)$ is defined.

4.4 The Case $p\mathcal{O}_K = \mathfrak{p}^2$

If p is ramified in K, we have an isomorphism

$$K_\mathfrak{p} \cong \mathbb{Q}_p(\sqrt{n}),$$

again by Proposition 4.4.. The main difference between the ramified and the inert case is the valuation in $\mathbb{Q}_p(\sqrt{n})$.

For $\varpi_\mathfrak{p} = \xi = a + b\sqrt{n} \in \mathbb{Q}_p(\sqrt{n})$ we have

$$v_\mathfrak{p}(\xi) = v_p(a^2 - nb^2),$$

since now the inertia index equals 1 and so ξ is a prime element if and only if

$$v_p(a^2 - nb^2) = 1,$$

or in other words if $\frac{a^2-nb^2}{p}$ is a unit in $\mathbb{Z}_p$. Repeating the approximation and decomposition steps shown in case 2, we obtain by Lemma 4.15.

$$q_{z,p}(\xi) = \begin{pmatrix} a + \dfrac{bx}{y} & \dfrac{b(ny^2 - x^2)}{y} \\ \dfrac{b}{y} & a - \dfrac{bx}{y} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

and the decomposition

$$Aq_{z,p}(\xi)B = X\left(\frac{p(xb + ya - y)}{b}\right)Y\left(\frac{b}{py}\right)X\left(\frac{p(ya - y(a^2 - nb^2) - xb)}{b(a^2 - nb^2)}\right),$$

where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{1}{p} \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{p}{a^2 - nb^2} \end{pmatrix}$$

are normalizing the determinant. By approximating with the matrix C we obtain again the decomposition

$$q_z(\mathfrak{n}_\mathfrak{p}) = \alpha u = A^{-1}C(C^{-1}A, ..., \tilde{I}B^{-1}, ..., C^{-1}A),$$

where $\tilde{I} = C^{-1}Aq_{z.p}(\xi)B$ and we have the analogue of Theorem 4.11. for the action of $(\mathfrak{n}_\mathfrak{p}^{-1}, K)$ on $f(z)$.

Note that $b \neq 0$, since $v_p(a^2) = 1$ is impossible for $a \in \mathbb{Q}_p$. This means we cannot choose $\varpi_\mathfrak{p} = p$ and so the general result from Theorem 4.16. does not hold. We can simplify by choosing $\varpi_\mathfrak{p} = \sqrt{n}$ to obtain

$$Aq_{z,p}(\xi)B = X\Big(p(x-y)\Big)Y\left(\frac{1}{py}\right)X\left(\frac{p(x-ny)}{n}\right).$$

Note however, that there is an exceptional case where the prime elements are characterised differently. If $p = 2$ and $n \equiv 3 \mod 4$, then 2 is ramified in K, but n is odd and hence a unit in $\mathbb{Z}_2$. This means in particular that $\sqrt{n}$ is not a prime element in $\mathbb{Q}_2(\sqrt{n})$ and we can choose $\varpi_\mathfrak{p} = 1 + \sqrt{n}$ to obtain

$$Aq_{z,2}(\xi)B = X\big(2x\big)Y\left(\frac{1}{2y}\right)X\left(\frac{2(ny-x)}{1-n}\right).$$

Example 4.18. Let $p = 7, n = -35, \varpi_\mathfrak{p} = \sqrt{-35}$ and $z = \frac{1+\sqrt{-35}}{2}$. Then

$$q_{z,7}(\xi) = \begin{pmatrix} 1 & -18 \\ 2 & -1 \end{pmatrix}$$

and we have the decomposition

$$Aq_{z,7}(\xi)B = Y\left(\frac{2}{7}\right)X\Big(-\frac{18}{5}\Big).$$

Since

$$-\frac{18}{5} = 2 + 2 \cdot 7 + ... \text{ in } \mathbb{Z}_7,$$

we have

$$C = \begin{pmatrix} 1 & 16 \\ \frac{2}{7} & \frac{39}{7} \end{pmatrix}$$

by approximating up to the 1-st power. Then

$$\alpha = A^{-1}C = \begin{pmatrix} 1 & 16 \\ 2 & 39 \end{pmatrix},$$

$$\tilde{I}B^{-1} = C^{-1}Aq_{z,7}(\xi) = \begin{pmatrix} 1 & -98 \\ 0 & 5 \end{pmatrix}$$

and

$$u = \left(\begin{pmatrix} \frac{39}{7} & -\frac{16}{7} \\ -\frac{2}{7} & \frac{1}{7} \end{pmatrix}, ..., \begin{pmatrix} 1 & -98 \\ 0 & 5 \end{pmatrix}, ..., \begin{pmatrix} \frac{39}{7} & -\frac{16}{7} \\ -\frac{2}{7} & \frac{1}{7} \end{pmatrix}\right).$$

Let now $f \in \mathbf{F}_{36}$. Then $f^{\sigma_\alpha} \in \mathbf{F}_{252}$, since $\det(\alpha) = 7$. We have $252 = 2^2 3^2 7$,

$$\begin{pmatrix} \frac{39}{7} & -\frac{16}{7} \\ -\frac{2}{7} & \frac{1}{7} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \mod 4,$$

$$\begin{pmatrix} \frac{39}{7} & -\frac{16}{7} \\ -\frac{2}{7} & \frac{1}{7} \end{pmatrix} \equiv \begin{pmatrix} 3 & -1 \\ 1 & 4 \end{pmatrix} \mod 9$$

and

$$\begin{pmatrix} 1 & -98 \\ 0 & 5 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \mod 7.$$

These congruences correspond to the matrix

$$\tilde{u} = \begin{pmatrix} \overline{57} & \overline{-28} \\ \overline{-98} & \overline{103} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/252\mathbb{Z}),$$

which can be decomposed as

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{103} \end{pmatrix} \begin{pmatrix} \overline{57} & \overline{-28} \\ \overline{70} & \overline{1} \end{pmatrix}$$

and the matrix

$$\begin{pmatrix} \overline{57} & \overline{-28} \\ \overline{70} & \overline{1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/252\mathbb{Z})$$

can be lifted to

$$\gamma = \begin{pmatrix} -1959 & -28 \\ 70 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

To be able to compute $f^{\sigma_\alpha}(\tau)$ explicitly, we first need to transform $f(\tau)$.

We have $\alpha = \delta\alpha'$, where

$$\delta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \alpha' = \begin{pmatrix} 1 & 16 \\ 0 & 7 \end{pmatrix}$$

and we will give the action of $(\mathfrak{n}_\mathfrak{p}^{-1}, K)$ on $f\left(\frac{1+\sqrt{-35}}{2}\right)$ in terms of the q-expansion of

$$f^\delta(\tau) = f(\delta\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{36})(e^{2\pi i\tau})^{k/36}$$

for $\tau \in \mathfrak{h}$, polynomials $g_k \in \mathbb{Q}[X]$ and $\mathfrak{n}_\mathfrak{p} = (1, ..., \sqrt{-35}, ...1)$ with $\mathfrak{p} = (7, (7+\sqrt{-35})/2)$. We have

$$f^{\sigma_\alpha}(\tau) = f(\alpha\tau) = f(\delta\alpha'\tau) = f^\delta(\alpha'\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{36})(e^{2\pi i})^{4k/63}(e^{2\pi i\tau})^{k/252}$$

and consequently

$$(f^{\sigma_\alpha})^{\sigma_u}(\tau) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{36}{}^{103})(e^{2\pi i})^{34k/63}(e^{2\pi i\gamma\tau})^{k/252}.$$

In particular, we obtain

$$(\mathfrak{n}_\mathfrak{p}^{-1}, K)f\left(\frac{1+\sqrt{-35}}{2}\right) = \sum_{k=-\infty}^{\infty} g_k(\zeta_{36}{}^{103})(e^{2\pi i})^{sk}(e^{2\pi i\sqrt{-35}})^{-tk},$$

where

$$s = \frac{1363171}{2^3 \cdot 3^2 \cdot 44171} \text{ and } t = \frac{1}{2^3 \cdot 3^2 \cdot 44171}.$$

Of course, we first had to transform our modular function with the matrix δ, to obtain a satisfying formula. One way to relate $f(\tau)$ to $f^\delta(\tau)$ is given by the identity

$$f_a(\delta\tau) = f_{a\delta}(\tau),\ a \in \mathbb{Q}^2$$

for the Fricke functions $f_a = f_{r,s,36}$. Then δ induces an automorphism of $\mathbf{F}_{36}$, given by $f_{r,s,36} \mapsto f_{r+2s,s,36}$ and $j \mapsto j$ on the generators of $\mathbf{F}_{36}$.

4.5 Application for Higher Ramification Groups

We will now show, how Shimura's reciprocity law can be used to describe the higher ramification groups of prime ideals in abelian extensions of imaginary quadratic number fields, which are generated by singular values of certain modular functions. For this, we will consider the ray class fields K_N for moduli of the form $N\mathcal{O}_K$, where $N \in \mathbb{N}$ and $K = \mathbb{Q}(\sqrt{n})$ is an imaginary quadratic number field with $n < 0$.

The second theorem of complex multiplication describes these ray class fields and by the properties of the Weber function, one can deduce that there is a suitable $z \in K \cap \mathfrak{h}$, such that the ray class field K_N is generated over K by all defined values $f(z)$, where $f \in \mathbf{F}_N$. This is proven in [Lan87, Chapter 10 §1, Corollary].

From now on, we will assume that $n \not\equiv 1 \mod 4$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$. In this case, again by [Lan87, Chapter 10 §1, Corollary], we can take $z = \sqrt{n}$ and we have

$$K_N = K(j(\sqrt{n}), f_{r,s,N}(\sqrt{n}))_{r,s}.$$

We will now define higher ramification groups and see, how they can be related to Shimura's reciprocity law.

Definition 4.19. Let L/M be a finite extension of $\mathfrak{p}$-adic number fields. For any $s \in [-1, \infty)$, the *s-th ramification group* of the extension L/M is the subgroup of $\mathrm{Gal}(L/M)$, given by

$$G_s = \{\sigma \in \mathrm{Gal}(L/M) : v_L(\sigma(a) - a) \geq s + 1 \text{ for all } a \in \mathcal{O}_M\}.$$

However, for our purposes we need an alternative definition of the groups G_s.

Definition 4.20. Let $t \in [-1, \infty)$. The *t-th ramification group in the upper numbering* G^t is given by $G_s = G^t$, where

$$t = \int_0^s \frac{dx}{(G_0 : G_x)}.$$

If $x < 0$, we set $(G_0 : G_x) = 1$.

Let now M be a $\mathfrak{p}$-adic number field with prime ideal $\mathfrak{p}$.

Definition 4.21. Let k be a positive integer. The *k-th group of higher units* U^k is the subgroup of M^*, given by

$$U^k = 1 + \mathfrak{p}^k.$$

If $k = 0$, we set $U^0 = \mathcal{O}_M^*$.

We can now relate the higher ramification groups in the upper numbering with the higher unit groups via the norm residue symbol as follows.

Proposition 4.22. *Let L/M be a finite abelian extension of $\mathfrak{p}$-adic number fields and let*

$$(\quad, L/M) : M^* \longrightarrow \mathrm{Gal}(L/M)$$

be the norm residue symbol. Then

$$(U^k, L/M) = G^k$$

for any nonnegative integer k.

For a proof, see [Neu99, Chapter V, Theorem 6.2]. □

To make use of this Proposition, we can take a prime $\mathfrak{p}$ in K and a prime $\mathfrak{P}$ in K_N, such that $\mathfrak{P}$ divides $\mathfrak{p}$ and pass to the completions with respect to these primes. Recall that we have an isomorphism $\mathrm{Gal}(K_{N_\mathfrak{P}}/K_\mathfrak{p}) \cong D_\mathfrak{P}$, so that we can view the G^k's as subgroups of $\mathrm{Gal}(K_N/K)$. There is also a definition of higher global ramification groups, which coincides with these subgroups. To apply Shimura's reciprocity law, we still need

to know, how we can relate the higher ramification groups to the global norm residue map. Let

$$\langle\ \rangle : K_{\mathfrak{p}}^* \longrightarrow \mathbf{I}_K$$

be the map, sending $x \in K_{\mathfrak{p}}^*$ to the idèle $(1, .., x, ..., 1)$, with x in position $\mathfrak{p}$.

Proposition 4.23. *The diagram*

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{(\ ,K_{N_{\mathfrak{P}}}/K_{\mathfrak{p}})} & \mathrm{Gal}(K_{N_{\mathfrak{P}}}/K_{\mathfrak{p}}) \\ \langle\ \rangle \downarrow & & \downarrow D_{\mathfrak{P}} \cong \mathrm{Gal}(K_{N_{\mathfrak{P}}}/K_{\mathfrak{p}}) \\ \mathbf{I}_K & \xrightarrow[(\ ,K_N/K)]{} & \mathrm{Gal}(K_N/K) \end{array}$$

commutes.

For a proof, see [Neu99, Chapter VI, Proposition 5.6]. □

To now determine $G^k \subseteq \mathrm{Gal}(K_N/K)$ means to determine the values

$$\sigma(f_{r,s,N}(\sqrt{n})) \text{ and } \sigma(j(\sqrt{n}))$$

for every $\sigma \in G^k$ and $r, s \in \mathbb{Z}/N\mathbb{Z}$, it is sufficient to compute

$$(\langle t^{-1}\rangle, K_N/K) f_{r,s,N}(\sqrt{n}) \text{ and } (\langle t^{-1}\rangle, K_N/K) j(\sqrt{n})$$

for every $t \in U^k$. By Shimura's reciprocity law, this is equivalent to computing the action of the automorphism $\sigma_{\sqrt{n}}(\langle t\rangle)$ on the Fricke functions and the j-invariant.

Remark 4.24. It is also possible to determine the groups G^k without using Shimura's reciprocity law. Let $K_{\mathfrak{m}}$ be the ray class field for the modulus

$$\mathfrak{m} = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

By the global reciprocity law, $\mathrm{Gal}(K_{\mathfrak{m}}/K)$ is isomorphic to $\mathbf{C}_K/\mathbf{C}_K^{\mathfrak{m}}$, where $\mathbf{C}_K = \mathbf{I}_K/K^*$ is the idèle class group and $\mathbf{C}_K^{\mathfrak{m}}$ is the *congruence subgroup mod* $\mathfrak{m}$. The latter is defined as $\mathbf{I}_K^{\mathfrak{m}} \cdot K^*/K^*$, where

$$\mathbf{I}_K^{\mathfrak{m}} = \prod_{\mathfrak{p} \text{ prime}} U_{\mathfrak{p}}^{n_{\mathfrak{p}}}$$

for the higher unit groups $U_{\mathfrak{p}}^{n_{\mathfrak{p}}} \subseteq K_{\mathfrak{p}}$. Recall that the ray class field K_1 for the modulus $\mathcal{O}_K$, which is a subfield of $K_{\mathfrak{m}}$, is simply the Hilbert class field of K. We have $\mathrm{Gal}(K_1/K) \cong \mathbf{C}_K/\mathbf{C}_K^1$ and since every prime $\mathfrak{p}$ of K is unramified in K_1, the higher ramification groups $G_{\mathfrak{p}}^k \subseteq \mathrm{Gal}(K_{\mathfrak{m}}/K)$ are all contained in the subgroup

$$\mathrm{Gal}(K_{\mathfrak{m}}/K_1) \cong \mathbf{C}_K^1/\mathbf{C}_K^{\mathfrak{m}}.$$

We have

$$\mathbf{C}_K^1/\mathbf{C}_K^{\mathfrak{m}} = \mathbf{I}_K^1 \cdot K^*/K^*/\mathbf{I}_K^{\mathfrak{m}} \cdot K^*/K^* \cong \mathbf{I}_K^1 \cdot K^*/\mathbf{I}_K^{\mathfrak{m}} \cdot K^* \cong \mathbf{I}_K^1/\mathbf{I}_K^{\mathfrak{m}} \cdot (\mathbf{I}_K^1 \cap K^*)$$

with

$$\mathbf{I}_K^1 = \prod_{\mathfrak{p} \text{ prime}} U_{\mathfrak{p}},$$

and

$$\mathbf{I}_K^1 \cap K^* = \mathcal{O}_K^* = \{1, -1\}$$

for all imaginary quadratic number fields K, other than $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Hence we obtain

$$\mathbf{C}_K^1/\mathbf{C}_K^{\mathfrak{m}} \cong \prod_{\mathfrak{p}|\mathfrak{m}} U_{\mathfrak{p}}/\pm U_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

If, for example, p is inert in K and we take the modulus $\mathfrak{m} = p^\ell \mathcal{O}_K = \mathfrak{p}^\ell$, we obtain

$$\mathbf{C}_K^1/\mathbf{C}_K^{\mathfrak{m}} \cong U_{\mathfrak{p}}/\pm U_{\mathfrak{p}}^\ell$$

and by Propositions 4.22. and 4.23. we have the isomorphism

$$G_{\mathfrak{p}}^k \cong U_{\mathfrak{p}}^k/U_{\mathfrak{p}}^\ell \cdot (\{\pm 1\} \cap U_{\mathfrak{p}}^k),$$

for the $k-$th higher ramification group $G_{\mathfrak{p}}^k$. Now, $U_{\mathfrak{p}}^k$ does not contain -1 if $k \geq 1$ and so

$$G_{\mathfrak{p}}^k \cong U_{\mathfrak{p}}^k/U_{\mathfrak{p}}^\ell.$$

For a classification of the higher unit groups, see [Has69, Chapter 15].

Although this method allows us to obtain the higher ramification groups in an abstract way, it does not describe their explicit action on the ray class field.

We already mentioned that the G^k's are determined by their action on singular values of the Fricke functions and the j-function and we will now present an alternative interpretation of this action. Consider the lattice $L = [1, \sqrt{n}]$. Recall from section 2 that this lattice can be identified with an elliptic curve E. Then the set of solutions $E(\mathbb{C})$ consists of all points of the form $(\wp(z), \wp'(z))$ and ∞, where $\wp(z) = \wp(z, L)$ and $z \in \mathbb{C}/L$. Points of the form

$$\left(\wp\left(\frac{r\sqrt{n}+s}{N}\right), \quad \wp'\left(\frac{r\sqrt{n}+s}{N}\right)\right) \in E(\mathbb{C})$$

are called *points of $N-$th order*, since $r\sqrt{n}+s$ is contained in L and therefore maps to ∞ under the canonical isomorphism. We denote the set of these points by E_N and we can identify them with the values $f_{r,s,N}(\sqrt{n})$ due to the way the Fricke functions are defined.

We will see in the proof of Proposition 4.25. that the j-function is invariant under the action of the higher ramification groups. Hence the G^k's are essentially subgroups of the

permutation group of all $f_{r,s,N}(\sqrt{n})$, which we then can view as the automorphism group $\mathrm{Aut}(E_N)$. Hence we have an embedding

$$G^k \hookrightarrow \mathrm{Gal}(K_N/K(j(\sqrt{n}))) \cong \mathrm{Aut}(E_N) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$$

and a matrix acts on a point

$$\left(\wp\left(\frac{r\sqrt{n}+s}{N}\right), \quad \wp'\left(\frac{r\sqrt{n}+s}{N}\right)\right) \in E(\mathbb{C})$$

as ordinary matrix multiplication with the row vector

$$\begin{pmatrix} \frac{r}{N} & \frac{s}{N} \end{pmatrix}.$$

Let p be the prime number contained in $\mathfrak{p}$. We will now examine the following special case.

Proposition 4.25. *Let K_{p^ℓ} be the ray class field for the modulus $p^\ell\mathcal{O}_K$ for an odd prime p and $k \geq 1$ and let G^k be the k-th higher ramification group of the extension K_{p^ℓ}/K with respect to the prime ideal $\mathfrak{p}$.*

(i) *If p splits completely in K and $k \geq \ell$, then G^k is trivial. If $k < \ell$, then G^k is isomorphic to the cyclic group of order $p^{\ell-k}$. An element $a \in \mathbb{Z}/p^{\ell-k}\mathbb{Z}$ corresponds to the matrix*

$$\begin{pmatrix} 1+\frac{p^k a}{2} & \frac{p^k a n}{2\sqrt{n_p}} \\ \frac{p^k a}{2\sqrt{n_p}} & 1+\frac{p^k a}{2} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^\ell\mathbb{Z}),$$

which can be identified as an element of $\mathrm{Aut}(E_{p^\ell})$ via ordinary multiplication with the row vectors

$$\begin{pmatrix} \frac{r}{p^\ell} & \frac{s}{p^\ell} \end{pmatrix}.$$

(ii) *If p is inert in K and $k \geq \ell$, then G^k is trivial. If $k < \ell$, then G^k is isomorphic to an abelian group of order $p^{2(\ell-k)}$ with $(\mathbb{Z}/p^{\ell-k}\mathbb{Z})^2$ as its underlying set. More precisely, if $2k \geq \ell$, we have*

$$G^k \cong (\mathbb{Z}/p^{\ell-k}\mathbb{Z}, +)^2.$$

An element (a, b) corresponds to the matrix

$$\begin{pmatrix} 1+p^k a & p^k b n \\ p^k b & 1+p^k a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^\ell\mathbb{Z}),$$

which can be identified as an element of $\mathrm{Aut}(E_{p^\ell})$ as in (i).

(iii) *If p is ramified in K and $k \geq 2\ell$, then G^k is trivial. If $k < 2\ell$, then G^k is isomorphic to an abelian group of order $p^{2\ell-k}$. More precisely, if $k \geq \ell$, we have*

$$G^k \cong (\mathbb{Z}/p^{\ell-k/2}\mathbb{Z}, +)^2$$

if k is even and

$$G^k \cong (\mathbb{Z}/p^{\ell-(k-1)/2}, +) \times (\mathbb{Z}/p^{\ell-(k+1)/2}, +)$$

if k is odd. An element (a, b) corresponds to the matrices

$$\begin{pmatrix} 1 + n^{k/2}a & n^{k/2}bn \\ n^{k/2}b & 1 + n^{k/2}a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^\ell\mathbb{Z})$$

and

$$\begin{pmatrix} 1 + n^{(k-1)/2}bn & n^{(k-1)/2}an \\ n^{(k-1)/2}a & 1 + n^{(k-1)/2}bn \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^\ell\mathbb{Z})$$

respectively. These can be identified as elements of $\mathrm{Aut}(E_{p^\ell})$ as in (i).

Proof: (i) If p splits completely in K, then by Proposition 4.3., we know that $K_\mathfrak{p} \cong \mathbb{Q}_p$ and we can write $t \in U^k$ as $t = 1 + p^k a$ for some $a \in \mathbb{Z}_p$. We can now apply the methods used in 4.2. The fact that t is a unit and not a prime element is not problematic, it makes things even easier. The element

$$(1 + p^k a, 1) \in \mathbb{Q}_p \oplus \mathbb{Q}_p$$

maps to

$$\xi = 1 + \frac{p^k a}{2} + \frac{p^k a}{2\sqrt{n}_p}\sqrt{\mathbf{n}} \in \mathbb{Q}_p \otimes_\mathbb{Q} K$$

and by Lemma 4.10., we obtain the matrix

$$q_{\sqrt{n},p}(\xi) = \begin{pmatrix} 1 + \dfrac{p^k a}{2} & \dfrac{p^k an}{2\sqrt{n}_p} \\ \dfrac{p^k a}{2\sqrt{n}_p} & 1 + \dfrac{p^k a}{2} \end{pmatrix}.$$

Since we assume that p is odd, the denominators are all units in $\mathbb{Z}_p$ and so the matrix is contained in $\mathrm{GL}_2(\mathbb{Z}_p)$. Hence no further decomposing is needed and we obtain

$$u = (I, ..., q_{\sqrt{n},p}(\xi), ..., I) \in U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

Since we are working with modular functions of level p^ℓ, the induced matrix satisfies

$$\tilde{u} \equiv q_{\sqrt{n},p}(\xi) \mod p^\ell.$$

If $k \geq \ell$, we have

$$\tilde{u} \equiv I \mod p^{\ell}$$

for every $a \in \mathbb{Z}_p$, which proves that G^k is the trivial group. Assume that $k < \ell$.

Since the j-function is U-invariant, we only need to determine the action of $\tilde{u}$ on the Fricke functions f_{r,s,p^ℓ}. By Proposition 3.11. it is clear that the Fricke functions are permuted under $\tilde{u}$ and we see that f_{r,s,p^ℓ} is mapped to $f_{\tilde{r},\tilde{s},p^\ell}$, where

$$\tilde{r} = r + \frac{p^k a}{2\sqrt{n}_p}(\sqrt{n}_p r + s) \text{ and } \tilde{s} = s + \frac{p^k a}{2\sqrt{n}_p}(nr + \sqrt{n}_p s)$$

or in other words, $(r,s) \in (\mathbb{Z}/p^\ell\mathbb{Z})^2$ is mapped to $(\tilde{r},\tilde{s}) \in (\mathbb{Z}/p^\ell\mathbb{Z})^2$. This yields the desired action, when we view $\tilde{u}$ as an element of $\mathrm{Aut}(E_{p^\ell})$.

We also have

$$(1,0) \mapsto \left(1 + \frac{p^k a}{2}, \quad \frac{p^k an}{2\sqrt{n}_p}\right)$$

$$(0,1) \mapsto \left(\frac{p^k a}{2\sqrt{n}_p}, \quad 1 + \frac{p^k a}{2}\right)$$

and we see that the action of $\tilde{u}$ depends only on the image of $(0,1)$. Recall from the proof of Theorem 3.6. that

$$\wp(z,L) = \wp(w,L) \text{ if and only if } z \equiv \pm w \mod L$$

for the Weierstrass $\wp$-function. This implies that for $a, b \in \mathbb{Z}_p$, the action of the induced matrices $\tilde{u}_a$ and $\tilde{u}_b$ are equal, if and only if

$$1 + \frac{p^k a}{2} \equiv 1 + \frac{p^k b}{2} \mod p^{\ell} \text{ and } \frac{p^k a}{2\sqrt{n}_p} \equiv \frac{p^k b}{2\sqrt{n}_p} \mod p^{\ell},$$

since

$$1 + \frac{p^k a}{2} \equiv -1 - \frac{p^k b}{2} \mod p^{\ell}$$

is impossible if p is odd and $k \geq 1$. Since p splits completely in K, it does not divide n and so 2 and $\sqrt{n}_p$ are units in $\mathbb{Z}/p^\ell\mathbb{Z}$. Hence we obtain

$$a \equiv b \mod p^{\ell-k}$$

and so we can view G^k as an abelian group with $\mathbb{Z}/p^{\ell-k}\mathbb{Z}$ as its underlying set. Note that the action of $\tilde{u}_a$ is the identity, if and only if $a \equiv 0 \mod p^{\ell-k}$. This means that the kernel of the surjection

$$U^k \longrightarrow G^k$$

consists of all elements of the form

$$1 + p^{k+(\ell-k)}a, \quad a \in \mathbb{Z}_p,$$

i.e. of all elements contained in U^ℓ. Hence we have an isomorphism

$$U^k/U^\ell \cong G^k.$$

Let us define

$$a * b := a + b + p^k ab$$

for $a, b \in \mathbb{Z}/p^{\ell-k}\mathbb{Z}$. The map

$$U^k \longrightarrow (\mathbb{Z}/p^{\ell-k}\mathbb{Z}, *)$$
$$1 + p^k a \mapsto a$$

is then a surjective homomorphism with kernel U^ℓ and we have isomorphisms

$$G^k \cong U^k/U^\ell \cong (\mathbb{Z}/p^{\ell-k}\mathbb{Z}, *).$$

Clearly, the operation $*$ is simply addition if $2k \geq \ell$. If $2k < \ell$, we have $1*1 = 1+(1+p^k)$ and by induction we obtain

$$\underbrace{1 * 1 * ... * 1 * 1}_{p^{\ell-k-1} \text{ times}} = \sum_{i=0}^{p^{\ell-k-1}-1} (1+p^k)^i.$$

Note that $1 + p^k$ generates a cyclic subgroup of order $p^{\ell-2k}$ of the multiplicative group $(\mathbb{Z}/p^{\ell-k}\mathbb{Z})^*$, which consists of all elements of the form $1 + p^k c$ for $c \in \mathbb{Z}/p^{\ell-k}\mathbb{Z}$. This means we have

$$\underbrace{1 * 1 * ... * 1 * 1}_{p^{\ell-k-1} \text{ times}} = p^{k-1} \sum_{i=0}^{p^{\ell-2k}-1} (1+p^k i) = p^{\ell-k-1} + p^{2k-1} \sum_{i=0}^{p^{\ell-2k}-1} i = p^{\ell-k-1} + \frac{(p^{\ell-2k}-1)p^{\ell-1}}{2}$$

and since

$$p^{\ell-1} \equiv 0 \mod p^{\ell-k},$$

we obtain

$$\underbrace{1 * 1 * ... * 1 * 1}_{p^{\ell-k-1} \text{ times}} = p^{\ell-k-1} \neq 0,$$

which means that $1 \in (\mathbb{Z}/p^{\ell-k}\mathbb{Z}, *)$ has order $p^{\ell-k}$ and so $(\mathbb{Z}/p^{\ell-k}\mathbb{Z}, *) \cong G^k$ is cyclic.

(ii) If p is inert in K, we have $K_\mathfrak{p} \cong \mathbb{Q}_p(\sqrt{n})$ by Proposition 4.4. Note that the ring of nonnegatively valued elements of $\mathbb{Q}_p(\sqrt{n})$ is simply $\mathbb{Z}_p[\sqrt{n}]$, due to the formula in Proposition 1.9. and the fact that n is not a square modulo p. This means, we can write any $t \in U^k$ as

$$t = 1 + p^k(a + b\sqrt{n}),$$

where $a, b \in \mathbb{Z}_p$. By Lemma 4.15., we obtain

$$q_{\sqrt{n},p}(t) = \begin{pmatrix} 1+p^k a & p^k bn \\ p^k b & 1+p^k a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$$

and

$$u = (I, ..., q_{\sqrt{n},p}(t), ..., I) \in U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

Again, if $k \geq \ell$, we obtain

$$\tilde{u} \equiv I \mod p^\ell$$

and so G^k is trivial.

Similarly to (i), we need to determine the action of this matrix on the Fricke functions for $k < \ell$. We immediately see that (r, s) gets mapped to

$$\big(r + p^k(ra + sb), \quad s + p^k(rbn + sa)\big)$$

and we have

$$(0, 1) \mapsto (p^k b, 1 + p^k a).$$

If we have elements

$$t_1 = 1 + p^k(a_1 + b_1\sqrt{n}) \in U^k$$

and

$$t_2 = 1 + p^k(a_2 + b_2\sqrt{n}) \in U^k,$$

then t_1 and t_2 map to the same automorphism in G^k if and only if

$$p^k b_1 \equiv p^k b_2 \mod p^\ell \text{ and } 1 + p^k a_1 \equiv 1 + p^k a_2 \mod p^\ell,$$

which is equivalent to

$$b_1 \equiv b_2 \mod p^{\ell-k} \text{ and } a_1 \equiv a_2 \mod p^{\ell-k}.$$

Note that

$$1 + p^k a_1 \equiv -1 - p^k a_2 \mod p^\ell$$

is again impossible. It is also clear that the kernel of the surjection

$$U^k \longrightarrow G^k$$

is again U^ℓ, so there is an isomorphism

$$U^k / U^\ell \cong G^k.$$

We now define a group structure on $\left(\mathbb{Z}/p^{\ell-k}\mathbb{Z}\right)^2$. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}/p^{\ell-k}\mathbb{Z}$. Then let

$$(a_1, b_1) \circ (a_2, b_2) := (a_1 + a_2 + p^k(a_1a_2 + b_1b_2n), b_1 + b_2 + p^k(a_1b_2 + a_2b_1)).$$

The map

$$U^k \longrightarrow ((\mathbb{Z}/p^{\ell-k}\mathbb{Z})^2, \circ)$$

$$1 + p^k(a + b\sqrt{n}) \mapsto (a, b)$$

is then a surjective group homomorphism with kernel U^ℓ, i.e. we have an isomorphism

$$G^k \cong ((\mathbb{Z}/p^{\ell-k}\mathbb{Z})^2, \circ).$$

In particular, if $2k \geq \ell$, the operation $\circ$ is simply componentwise addition.

(iii) If p is ramified in K, p is no longer a prime element in $\mathbb{Q}_p(\sqrt{n}) \cong K_\mathfrak{p}$ and we have to take $\sqrt{n}$ to obtain

$$t = 1 + \sqrt{n}^k(a + b\sqrt{n}).$$

Again, we can assume that $a, b \in \mathbb{Z}_p$. We obtain

$$q_{\sqrt{n},p}(t) = \begin{pmatrix} 1 + n^{k/2}a & n^{k/2}bn \\ n^{k/2}b & 1 + n^{k/2}a \end{pmatrix}$$

if k is even and

$$q_{\sqrt{n},p}(t) = \begin{pmatrix} 1 + n^{(k-1)/2}bn & n^{(k-1)/2}an \\ n^{(k-1)/2}a & 1 + n^{(k-1)/2}bn \end{pmatrix}$$

if k is odd.

The rest works analogously to (i) and (ii), by using the fact that p divides n. □

If $n \equiv 1 \mod 4$, we have a similar version of Proposition 4.25.. The G^k's have the same structure as groups, only their action on E_{p^ℓ} is different. The proof works in the same way, by taking $z = \frac{1+\sqrt{n}}{2}$.

4.6 Application for Ring Class Fields

In the following, we will show how one can apply the results of this section to find the conjugates of certain singular values of modular functions that lie in the ring class field of an order $\mathcal{O}$ in K.

Let $L_\mathcal{O}$ denote the ring class field of $\mathcal{O}$. Recall that by class field theory, we have an isomorphism

$$C(\mathcal{O}) \cong \mathrm{Gal}(L_\mathcal{O}/K),$$

where $C(\mathcal{O})$ is the ideal class group of $\mathcal{O}$ and this isomorphism is induced by the surjective homomorphism

$$\mathfrak{a} \mapsto \left(\frac{L_{\mathcal{O}}/K}{\mathfrak{a}\mathcal{O}_K}\right),$$

where $\mathfrak{a}$ is an ideal in $\mathcal{O}$, prime to the conductor f.
Let $\mathfrak{a}$ now be a proper fractional ideal in $\mathcal{O}$. We know from the first main theorem of complex multiplication that $j(\mathfrak{a})$ generates $L_{\mathcal{O}}$ over K. If $\mathfrak{b}$ is another proper fractional ideal, contained in a different ideal class, then one can show that $j(\mathfrak{a})$ and $j(\mathfrak{b})$ are conjugate over K with the help of the following

Theorem 4.26. *Let $\mathfrak{b}$ be a proper fractional ideal in $\mathcal{O}$ and let $\mathfrak{p}$ be a prime of K. Then*

$$\left(\frac{L_{\mathcal{O}}/K}{\mathfrak{p}}\right) j(\mathfrak{b}) = j(\overline{\mathfrak{p} \cap \mathcal{O}}\mathfrak{b}).$$

For proofs, see [Lan87, Chapter 10 §1 Theorem 1] and [Shi71, p. 122, (5.4.1)]. □

It is now easy to show that there is an isomorphism

$$C(\mathcal{O}) \cong \mathrm{Gal}(L_{\mathcal{O}}/K)$$

$$\mathfrak{a} \mapsto \sigma_{\mathfrak{a}},$$

where $\sigma_{\mathfrak{a}}$ is defined by the relation

$$\sigma_{\mathfrak{a}}(j(\mathfrak{b})) = j(\overline{\mathfrak{a}}\mathfrak{b})$$

for a proper fractional ideal $\mathfrak{b}$ in $\mathcal{O}$ and from this, one can deduce that $j(\mathfrak{a})$ and $j(\mathfrak{b})$ are indeed conjugates.

For arbitrary modular functions $f \in \mathbf{F}$, this is not so easy, since we first need to determine whether the value $f(\tau)$ is contained in $L_{\mathcal{O}}$. For this, we need to introduce *extended ring class fields.*

We denote by $P_{K,\mathbb{Z},N}(fN)$ the subgroup of $I_K(fN)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where

$$\alpha \in \mathcal{O}_K \text{ and } \alpha \equiv a \mod f N\mathcal{O}_K \text{ for some } a \in \mathbb{Z} \text{ with } a \equiv 1 \mod N.$$

This subgroup is a congruence subgroup for the modulus $fN\mathcal{O}_K$ and by class field theory, we obtain an extension $L_{\mathcal{O},N}/L_{\mathcal{O}}$. The field $L_{\mathcal{O},N}$ is called the *extended ring class field of level N.*

We can describe the Galois group in the following way.

Lemma 4.27. *There is an exact sequence*

$$\mathcal{O}^* \longrightarrow (\mathcal{O}/N\mathcal{O})^* \longrightarrow \mathrm{Gal}(L_{\mathcal{O},N}/L_{\mathcal{O}}),$$

where the second map is induced by

$$\alpha \mapsto \alpha\mathcal{O}_K$$

for $\alpha \in \mathcal{O}$, relatively prime to fN.

For proofs, see [Cox13, Lemma 15.13.] and [GeeSte98]. □

Let $\tau \in K \cap \mathfrak{h}$ be a root of the polynomial $aX^2 + bX + c$, where a, b, c are relatively prime integers with $a > 0$. Then $a\tau \in \mathcal{O}_K$ and $\mathcal{O} = [1, a\tau]$ is an order in K. From now on, we will assume that τ and $\mathcal{O}$ are of this form.

An important property of extended ring class fields is given by the following

Theorem 4.28. *Let τ and $\mathcal{O}$ be as above and let $f \in \mathbf{F}_N$, such that $f(\tau)$ is defined. Then $f(\tau) \in L_{\mathcal{O},N}$.*

For proofs, see [Cox13, Theorem 15.16.] and [GeeSte98]. □

The theorem tells us that it is sufficient to compute $\sigma(f(\tau))$ for every $\sigma \in \mathrm{Gal}(L_{\mathcal{O},N}/L_{\mathcal{O}})$ to determine if $f(\tau) \in L_{\mathcal{O}}$. This can be achieved by the following modified version of Shimura's reciprocity law.

Let $u \in (\mathcal{O}/N\mathcal{O})^*$ and let $g_\tau(u) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be given by the relation

$$g_\tau(u)\begin{pmatrix}\tau\\1\end{pmatrix} = u\begin{pmatrix}\tau\\1\end{pmatrix}.$$

The matrix $g_\tau(u)$ is the analogue of the matrix $q_z(\xi)$ in the classical formulation of the reciprocity law. Let $\sigma_u \in \mathrm{Gal}(L_{\mathcal{O},N}/L_{\mathcal{O}})$ denote the automorphism corresponding to u via the exact sequence from Lemma 4.27..

Theorem 4.29. (Shimura Reciprocity for $L_{\mathcal{O},N}$)
Let τ and $\mathcal{O}$ be as above and let $f \in \mathbf{F}_N$ such that $f(\tau)$ is defined. Then

$$\sigma_{u^{-1}}(f(\tau)) = f^{g_\tau(u)}(\tau).$$

For proofs, see [Cox13, Theorem 15.17.] and [GeeSte98]. □

It is obvious that $f(\tau) \in L_{\mathcal{O}}$ if and only if $\sigma_u(f(\tau)) = f(\tau)$ for every $u \in (\mathcal{O}/N\mathcal{O})^*$ and Theorem 4.29. makes it possible to explicitly compute these values.

Remark 4.30. If we now have $f(\tau) \in L_{\mathcal{O}}$, we want to compute its conjugate $\sigma_{\mathfrak{a}}(f(\tau))$ for every ideal class $[\mathfrak{a}] \in C(\mathcal{O})$. Recall that if $\mathfrak{a}$ is an ideal in $\mathcal{O}$, prime to the conductor, then $\sigma_{\mathfrak{a}}$ is given by

$$\left(\frac{L_{\mathcal{O}}/K}{\mathfrak{a}\mathcal{O}_K}\right).$$

It is not hard to check that $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ lie in inverse ideal classes and so we have

$$\sigma_{\overline{\mathfrak{a}}} = \left(\frac{L_{\mathcal{O}}/K}{\mathfrak{a}\mathcal{O}_K}\right)^{-1},$$

i.e. we want to compute

$$\left(\frac{L_{\mathcal{O}}/K}{\mathfrak{a}\mathcal{O}_K}\right)^{-1} f(\tau).$$

As we already mentioned in the beginning of this section, this amounts to repeatedly applying Shimura's reciprocity law for the prime idèles $\mathfrak{n}_{\mathfrak{p}_i}$, for every $\mathfrak{p}_i$ that appears in the factorization of $\mathfrak{a}$ and by the results of this section, one can explicitly compute the conjugates of $f(\tau)$ over K.

Bibliography

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Wiley, Hoboken, second edition, 2013.

[Lan87] Serge Lang. *Elliptic Functions.* Springer-Verlag, New York, second edition, 1987.

[Ser79] Jean-Pierre Serre. *Local Fields.* Springer Science, New York, 1979.

[Neu13] Jürgen Neukirch. *Class Field Theory -The Bonn Lectures- Edited by Alexander Schmidt.* Springer-Verlag Berlin Heidelberg, 2013

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin, 1999.

[CasFro67] J.W.S. Cassels, A. Fröhlich. *Algebraic number theory.* Academic Press, London, 1967.

[Gou97] Fernando O. Gouvêa. *p-adic Numbers, an Introduction.* Springer, Berlin, second edition, 1997.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, Princeton, 1971.

[Ste01] Peter Stevenhagen. *Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity.* Advanced Studies in Pure Mathematics 30, 2001, pp. 161-176.

[GeeSte98] Alice Gee, Peter Stevenhagen. *Generating Class Fields Using Shimura Reciprocity.* Lecture Notes in Cornput. Sci. 1423, Springer-Verlag, Berlin, 1998, pp. 441-453.

[Jan73] G. Janusz. *Algebraic Number Fields.* Academic Press, New York, 1973.

[Has69] Helmut Hasse. *Number Theory.* Akademie-Verlag, Berlin, 1969.