Arithmetic of Quaternion Orders and Its Applications

February 2012

Waseda University
Graduate School of Fundamental Science and Engineering
Major in Pure and Applied Mathematics
Research on Number Theory

Fang-Ting TU
Acknowledgement

First of all, I would like to dedicate the sincere appreciation to my advisors, Professor Ki-ichiro Hashimoto and Professor Yifan Yang. Much fundamental knowledge and the results of the dissertation herein are discussed with them. In the past few years, being a graduate student of National Chiao Tung University, I have worked under the guidance of Professor Yang. Without his constant encouragement, patient instruction, and enthusiastic supports, it is impossible for me today to be in this position. Many thanks are due to Professor Hashimoto for providing me the opportunity to be a research student at Waseda University under his supervision. He gives me several enlightening advices during the periods while I stay here. Without his kindly help, and instructive suggestions, it is impossible to complete this thesis. They lead me into such a wonderful, fascinating world of mathematics. Not only mathematics but also many personal virtues such as ”be patient”, ”be passionate”, and ”be positive”, that I learn by their guiding. I am honored and forever grateful for being welcomed to be their student.

In addition, I also appreciate Professor Keiichi Komatsu and Professor Manabu Ozaki during the thesis defenses.

For my student life, I felt an immense gratitude to Professor Winnie Li, Professor Jin Yu, as well as the government of Republic of China (Taiwan). Because of their organizations and supports, I have the chances to attend conferences, workshops, and study aboard. Also, I would like to thank my friends, especially best friends, and those in Japan. Thank you for doing me favors generously when I got into troubles. Thank you guys for making my student life colorful and smooth. Too many persons whom I want to express my gratitude, so please forgive me if I do not list all of you.

Finally, I am particularly indebted to my family which is the most important and indispensable cornerstone for my life. Without saying any big words, thank you for always behind me.

Warmest thanks to my beloved family, respected advisors, and lovely friends. Because of you, I arrive at the current stage. There is still a long and challenging journey in front of me. Though I still have to learn many things, I will do my best, with your support and what you taught me, to keep going.
## Contents

1 Introduction 1

2 Background 6
   2.1 Basic Properties of Quaternion Algebras 6
   2.2 Orders and Ideals 10
   2.3 Quaternion Algebras over Local Fields 13
   2.4 Maximal Orders in $\mathbf{M}(2, K)$ over a Non-Archimedean Local Field 15
   2.5 Quaternion Algebras over Number Fields 19
   2.6 Orders in a Quaternion Algebra over a Number Field 20
   2.7 Groups of Quaternion Transformations 24
   2.8 Shimura Curves 26
   2.9 Automorphic Forms on Shimura Curves 27
   2.10 Construction of Modular Forms 29

3 Orders of $\mathbf{M}(2, K)$ over a Non-Archimedean Local Field 32
   3.1 Introduction 32
   3.2 Explicit Way to Obtain an Intersection Order 36
   3.3 Proof of Lemma 3.2.4 37
   3.4 Classification of Orders Arising from Intersection 41

4 Lattice Packing from Quaternion Algebras 44
   4.1 Lattice Packing from Number Fields 45
   4.2 Lattices from Quaternion Algebras 46

5 Defining Equation of Modular Curves $X_0(2^{2n})$ 52
   5.1 Introduction 52
   5.2 Modular Curve $X_0(2^n)$ 53
5.3 Defining Equations and the Fermat Curves . . . . . . . . . . . . . . . 56
5.4 Proof of Theorem 5.3.1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 60
Chapter 1

Introduction

It goes without saying that some of the most important roles in the developments of number theory during the last century were played by modular forms and modular curves, which are associated with certain congruence subgroups of $\text{SL}(2, \mathbb{Z})$. A reason of this fact is because of the connection with the moduli space of elliptic curves with some level structure, and that the elliptic curves, being algebraic curves of the smallest positive genus, are related with many nontrivial Diophantine Problems in number theory. The proof of Fermat’s last theorem by A.Wiles, obtained as an application of the Taniyama-Shimura conjecture for elliptic curves over $\mathbb{Q}$, was a typical and the most epoch making achievement in this context. Also we recall a striking result of G.V.Belyi that every algebraic curve defined over an algebraic number field is obtained as a quotient of the upper half plane by a modular group which is a subgroup of $\text{SL}(2, \mathbb{Z})$ of finite index.

These facts show the significance of modular groups and modular forms associated with them. It is, therefore, strongly desirable to have enough knowledge of the classification of modular groups, as well as their structures and arithmetic properties of the associated modular forms. Since this problem does not seem to be easily handled, one may instead ask to study the similar problem for orders of the matrix algebra $\text{M}(2, \mathbb{Q})$. Indeed, the two problems are closely related to each other. To a modular group $\Gamma$ one can assign an order $\mathcal{O}_\Gamma$, and conversely, one obtains from an order $\mathcal{O}$ a group $\Gamma$ consisting of the elements of $\mathcal{O}$ with determinant 1.

The same problem can be asked for quaternion algebras over $\mathbb{Q}$, by which we do not lose significance at all. This is not just because $\text{M}(2, \mathbb{Q})$ is a special quaternion algebra, but it is known by Eichler and Shimura that the
Thus, in this dissertation, we are concerned with the classification problem and arithmetic properties of certain quaternion orders.

Recall that a quaternion algebra $B$ over a base field $K$ is a 4-dimensional central simple $K$-algebra. If $K$ is a field of fractions of a Dedekind domain $R$, an order of $B$ is a finitely generated $R$-module containing a $K$-basis for $B$, and at the same time, it is also a ring with unity. In other words, an order of a quaternion algebra over $K$ is a complete $R$-lattice of $B$, and a ring with unity. Furthermore, for the case of a global field $K$, the completion of $B$ at the place $v$ defined by $B_v := B \otimes_K K_v$ is a quaternion algebra over the field $K_v$. In particular, for all but finitely many places, the localization $B_v$ is isomorphic to the algebra of 2 by 2 matrices $M(2, K_v)$. Also, the localization of the order $\mathcal{O}$, $\mathcal{O}_v := \mathcal{O} \otimes_R R_v$, is again an order in $B_v$, and $\mathcal{O}_v$ is maximal for almost all places. According to the local-global correspondence, the arithmetic of global orders is closely related to the arithmetic of local orders, especially the orders in $M(2, K_v)$. Therefore,

\[
\text{to classify all the orders of } M(2, K) \text{ over a non-Archimedean local field,}
\]

is an important basic problem for the study of arithmetic theory of quaternion orders.

We now let $K$ be a non-Archimedean local field. It is well-known that each maximal order in $M(2, K)$ is isomorphic to the maximal order $M(2, R)$, where $R$ is the valuation ring of $K$. Besides, the so-called split order, which contains $R \oplus R$ as a subring, has been studied from 1950 by numerous mathematicians, such as Ehichler[20, 21, 22, 23, 24, 25], Hijikata[37, 38, 39], Pizer[49, 50], Shimura[57, 58] and so on (reported at some references [18, 32, 33, 34, 48, 51]). In 1974, Hijikata[37] gave a complete characterization of split orders. He showed that the split orders can be determined uniquely as the intersection of at most two maximal orders. Since then most studies and applications of quaternion orders are relying on the split orders.

Here, take the connection between split orders and modular forms for an example. Let $B$ be a definite quaternion algebra over $\mathbb{Q}$ with discriminant $q$ and $\mathcal{O}$ be an Eichler order, which is the intersection of two maximal orders. Then the theta series attached to each ideal of the order $\mathcal{O}$ will be a modular form of weight 2 on $\Gamma_0(qN)$ for a proper integer $N$. In literature, such theta series have been studied extensively. In particular, the work of

\[
\text{arithmetic of quaternion algebras is a subject which contains as deep and interesting properties as that of modular curves and modular forms.}
\]
Eichler, Hijikata, Pizer, and Shemanske [23, 38] showed that the action of Hecke operators on the theta series can be explicitly described in terms of the so-called Brandt matrices, which are intrinsic to the Eichler order \( \mathcal{O} \). These results enabled them to solve a basis problem for the space of modular forms on \( \Gamma_0(qN) \). Hijikata, Satio [39], Hasegawa and Hashimoto [32, 34] also contributed the relation between the class numbers, type numbers and the dimension of weight 2 cusps forms via the theory of these theta series. Moreover, linear relations among these theta series have deep arithmetic meaning in terms of \( L \)-functions of cusp forms (see references [15, 31, 33, 51]).

In the case of the intersection of two maximal orders, there is a rich theory connecting Eichler orders and modular forms. Actually, there are still many orders that are neither maximal orders nor Eichler orders. Without doubt, we are excepting that there are many interesting results and applications of quaternion orders as the applications of the Eichler orders.

In order to deal with the classification problem of local orders in \( \text{M}(2, K) \), there still exist non-split orders that have not been characterized completely yet, so it is natural to ask the questions

- Can we classify all orders that are the intersections of finitely many maximal orders?
- Is there any order that is not the intersection of maximal orders?

In this thesis, we will give the answer for the first problem and two examples to show the existence of non-intersection orders (chapter 3).

**Theorem 1.0.1.** Given finite number of maximal orders \( \mathcal{O}_1, \ldots, \mathcal{O}_r \) in \( \text{M}(2, K) \), there exist at most 3 maximal orders \( \mathcal{O}_{j_1}, \mathcal{O}_{j_2}, \text{ and } \mathcal{O}_{j_3} \) among them so that

\[
\bigcap_{i=1}^r \mathcal{O}_i = \mathcal{O}_{j_1} \cap \mathcal{O}_{j_2} \cap \mathcal{O}_{j_3}.
\]

The main result is somehow surprising, because that naively one would expect that as the number of maximal orders increases or as the local field varies the number of maximal orders needed to determine the intersection should also vary. However, the theorem shows that 3 is always enough. In fact, we can explicitly find these 3 maximal orders. According to this result, we then give a complete classification for the intersection orders.
Theorem 1.0.2. (Classification of Intersection Orders of $M(2, K)$)

If an order in $M(2, K)$ is the intersection of finitely many maximal orders, then it is isomorphic to exactly one of the following orders

$$\begin{cases} \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) : a, b, c, d \in R, \\ \left( \begin{array}{cc} a \pi^n c & b \\ \pi c & d \end{array} \right) : a, b, c, d \in R, \end{cases}$$

$$(n > 0, \mathcal{O}_{j_2} = \mathcal{O}_{j_3})$$

where $\pi$ is a fixed uniformizer of $K$.

Regard as applications of the arithmetic of quaternion orders described in the thesis, one is to construct lattices having best known densities in Euclidean spaces, which is related to the lattice packing problem; the other is to obtain defining equations of modular curves $X_0(2^{2n})$.

For lattice packing problem (chapter 4), we construct lattices in $4n$-dimensional Euclidean space, which have higher possible densities. The main idea is to construct a positive definite symmetric bilinear form via the norm form of an ideal of a definite quaternion algebra together with a totally positive element. To be more precise, the bilinear form defined by $\text{Tr}(x \bar{y})$ on a definite quaternion algebra $B$ is positive and symmetric, where $\text{Tr}$ is the reduced trace on $B$. For a chosen definite $K$-quaternion algebra $B$ and ideal $I$, by a suitable scaled trace construction with a totally positive integral element $\alpha$ in $K$, the map $\text{Tr}_K^K(\alpha \text{Tr}(x \bar{y}))$ gives a positive definite symmetric $\mathbb{Z}$-bilinear form on the ideal $I$. In this case, we denote $(I, \alpha)$ the ideal lattice. Viewing $(I, \alpha)$ as an Euclidean lattice, one has a determinant formula

$$\det I = d_K^K N_Q^K (d_B^K \alpha^4 N(I)^4),$$

where $d_K$ is the discriminant of the field $K$, $d_B$ is the discriminant of the quaternion algebra $B$, and $N(I)$ is the reduced norm of the ideal $I$ of $B$. Using this information, we successfully constructed ideal lattices which have best known densities in dimension 4, 8, 12, 16, 24, and 32. In particular, these lattices are isomorphic to the well-known root lattices $D_4$, $E_8$, Coxeter-Todd lattice $K_{12}$, the laminated $\Lambda_{16}$, and the Leech lattice $\Lambda_{24}$, respectively.

For the equations of $X_0(2^{2n})$ (chapter 5), we remark that the modular curve $X_0(N)$, the quotient space of the extended upper half plane by the
Eichler order

$$\Gamma_0(N) = \left\{ \gamma \in \text{SL}(2, \mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

of $M(2, \mathbb{Q})$, is a compact Riemann surface. Note that there is a natural covering map from $X_0(2^{2n+2})$ to $X_0(2^{2n})$. Once the defining equation of $X_0(2^{2n})$ is known, one may deduce an equation of $X_0(2^{2n+2})$ from the covering map. The key point of our method is to obtain relations between the generators of the function fields of the modular curves $X_0(2^{2n})$. Therefore, we can easily figure out the defining equations of $X_0(2^{2n})$ by observation of the equation for the curve $X_0(64)$.

In the following context, we will first, without proof, say a few words about properties of quaternion algebras, orders of quaternion algebras, and Shimura curves in chapter 2. Afterward we will describe our work for orders in $M(2, K)$, ideal lattices from quaternion algebras, and equations of $X_0(2^{2n})$ in details.
Chapter 2

Background

In this chapter, we will first recall some basic definitions and properties of quaternion algebras. Then we will briefly review Shimura curves, modular curves, and modular forms. Most of the materials are referred to [1, 19, 43, 58, 66]. The fields what we mainly concerned with are the number fields or the completion fields ($\mathcal{P}$-adic fields) related to number fields. Henceforth, in the sequent discussions, we assume that $K$ is a field whose characteristic is not 2.

2.1 Basic Properties of Quaternion Algebras

A well-known quaternion algebra is the Hamilton’s quaternions

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij, \quad \text{with} \quad i^2 = j^2 = -1, \ ij = -ji.$$  

It is the unique division algebra of dimension 4 over the real numbers, up to isomorphism. For an element $h = a + bi + cj + dij$ in $\mathbb{H}$, its conjugate element is $\bar{h} = a - bi - cj - dij$, the trace of $h$ is $\text{Tr}(h) = 2a$ and the norm of $h$ is $h\bar{h} = a^2 + b^2 + c^2 + d^2$. In particular, the quaternion algebra $\mathbb{H}$ can be viewed as a quadratic space with the quadratic form $Q(x) = x\bar{x}$.

In general, a quaternion algebra can be seen as a generalization of the Hamilton’s quaternions $\mathbb{H}$ to any base field. In this section, we will state the definition and properties of a quaternion algebra over an arbitrary field, and then simply classify $K$-quaternion algebras for certain fields.
2.1.1 Quaternion algebras

A quaternion algebra $B$ over a field $K$ is a central simple algebra of dimension 4 over $K$, or equivalently, there exist $i, j \in B$ and $a, b \in K^*$ so that

$$B = K + Ki + Kj + Kij, \quad i^2 = a, \quad j^2 = b, \quad ij = -ji.$$ 

For $\text{char } K = 2$, we also have a similar result

$$B = K + Ki + Kj + Kij, \quad i^2 + i = a, \quad j^2 = b, \quad ij = j(1 + i).$$

In such case, we denote the quaternion algebra $B$ by $(a, b)_K$, which has canonical $K$-basis $\{1, i, j, ij\}$. Familiar examples are Hamilton’s quaternions $\mathbb{H} = \left(\frac{-1}{R}\right)$ and the 2 by 2 matrix algebra $M(2, K) \cong \left(\frac{1,1}{K}\right)$.

**Remark 2.1.1.** The isomorphism from $\left(\frac{1,1}{K}\right)$ to $M(2, K)$ can be given by the map

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

According to the following theorem, we have the fact that if a $K$-quaternion algebra is not a division algebra, then it is isomorphic to $M(2, K)$.

**Theorem 2.1.2. (Wedderburn Theorem)** Any central simple algebra over a field $K$ is isomorphic to $M(n, D)$, for some positive integer $n$, where $D$ is a $K$-central division algebra.

Writing the quaternion algebra $B$ in the form $(a, b)_K$, we observe that if $a$ has a square root $\alpha$ in $K$ then $B$ has a zero divisor $h = \alpha - i$ so that $B$ is isomorphic to the 2 by 2 matrix algebra. Hence we obtain the following Corollary 2.1.3. If a field $K$ has no quadratic extension, then any $K$-quaternion algebra is isomorphic to $M(2, K)$. In particular, this is the case for an algebraically closed field.

**Corollary 2.1.3.** Each quaternion algebra over an algebraically closed field $K$ is isomorphic to $M(2, K)$.

2.1.2 Quaternion algebras as quadratic spaces

Notice that a quaternion algebra is a central simple algebra of dimension 4, so every element $h$ in a quaternion algebra satisfies a monic polynomial
equation over $K$ of degree at most 2. Therefore, any quaternion algebra $B$ is provided with the unique anti-involution $^{-} : B \to B$ satisfying $h + h \in K$ for all $h \in B$. Here an anti-involution of $B$ is a $K$-linear map from $B$ to itself satisfying

$$ax + by = a\bar{x} + b\bar{y}, \quad \bar{x} = x, \quad \bar{xy} = \bar{y}\bar{x}, \quad \text{for all } a, b \in K, \ x, y \in B.$$ 

The maps **reduced trace**, and **reduced norm** on $B$ are defined by

$$\text{Tr}(h) = h + \bar{h}, \quad \text{and} \quad N(h) = h\bar{h},$$

respectively. Then these maps lead to a nondegenerate symmetric $K$-bilinear form on $B$, which is given by $\text{Tr}(x\bar{y})$. In other words, the quaternion algebra $B$ is a quadratic space with the quadratic form given by the reduced norm of $B$.

**Remark 2.1.4.** We note that $\text{Tr}(h) = 2h$ and $N(h) = h^2$, while $h$ lies in the center $K$. In fact, for an element $h = a_0 + a_1i + a_2j + a_3ij \in \left( \frac{a, b}{K} \right)$, its conjugate is $\bar{h} = a_0 - a_1i - a_2j - a_3ij$. Note also that, if $B = M(2, K)$ then the reduced trace and reduced norm of an element $h$ are the trace and the determinant of the matrix $h$, respectively.

Recall that a quadratic space with a quadratic form $Q$ is said to be **isotropic** if there is a non-zero element $x$ so that $Q(x) = 0$.

**Theorem 2.1.5.** For a quaternion algebra $B = \left( \frac{a, b}{K} \right)$ over $K$, the following are equivalent.

1. $B$ is isomorphic to $M(2, K)$.
2. $B$ is not a division algebra.
3. $B$ is isotropic as a quadratic space with the reduced norm.
4. The quadratic form $ax^2 + by^2$ represents 1.
5. The value $a$ is an element of $N^F_K(F)$, where $F = K(\sqrt{b})$ and $N^F_K$ is the usual norm map from $F$ to $K$.

Denote $B_0$ the **pure quaternion space**, $B_0 = \{x \in B : \text{Tr}(x) = 0\}$. One can see that

$$B_0 = \{h \in B : h \notin K, h^2 \in K\} \cup \{0\}$$
and

\[ B = K \oplus B_0 \]

as a vector space. Furthermore, once the pure quaternion space is given, the isomorphism class of the quaternion algebra \( B \) is determined.

**Theorem 2.1.6.** Let \( B \) and \( B' \) be two quaternion algebras over \( K \). Then \( B \) is isomorphic to \( B' \) if and only if \( B_0 \) and \( B'_0 \) are isometric. Equivalently, the quaternion algebras \( \left( \frac{a,b}{K} \right) \), \( \left( \frac{c,d}{K} \right) \) are isomorphic if and only if the quadratic forms

\[ ax^2 + by^2 - abz^2 \quad \text{and} \quad cx^2 + dy^2 - cdz^2 \]

are equivalent over \( K \).

### 2.1.3 Automorphism theorem

**Theorem 2.1.7.** (Skolem-Noether Theorem) Let \( L, L' \) be two commutative \( K \)-algebras over \( K \) contained in a quaternion algebra \( B \) over \( K \). Then all \( K \)-isomorphism from \( L \) to \( L' \) can be extended to an inner automorphism of \( B \). In particular, the \( K \)-automorphisms of \( B \) are all inner automorphisms.

**Remark 2.1.8.** The inner automorphism of \( B \) is an automorphism given by \( k \mapsto hkh^{-1} \), for some invertible element \( h \) of \( B \). Therefore, Theorem 2.1.7 implies that the automorphism group of the quaternion algebra \( B \) as \( K \)-algebra, \( \text{Aut}_K(B) \), is isomorphic to the factor group \( B^*/K^* \).

Now, if \( F \) is a quadratic algebra over \( K \) contained in a \( K \)-quaternion algebra \( B \), and \( \sigma : F \to F \) is a non-trivial \( K \)-automorphism, then there exists an invertible element \( u \in B \) not in \( F \) so that \( umu^{-1} = \sigma(m) \), for all \( m \in F \). The fact \( u \in B_0 \) implies that \( u^2 = \theta \in K^\times \).

**Corollary 2.1.9.** For all separable quadratic algebras \( F \) over \( K \) contained in \( B \), there exist elements \( u \in B \) and \( \theta \in K^\times \) such that

\[ B = F + Fu, \quad u^2 = \theta \quad \text{and} \quad um = \sigma(m)u, \]

where \( \sigma \) denotes the non-trivial \( K \)-automorphism of \( F \).

In this way, we realize the \( K \)-quaternion algebra \( B \) as \( B = \{ F, \theta \} \). Moreover, the quaternion algebra \( \left( \frac{a,b}{K} \right) \) can be written as \( \{ K(i), b \} \).
Corollary 2.1.10. Let $B = \{F, \theta\}$ with $\theta = a^2$ be a quaternion algebra $B$ over $K$. Then $B$ is isomorphic to $\text{M}(2, K)$ if and only if one of the following occurs.

1. $F$ is not a division algebra.
2. $F$ is a field and $\theta \in N_K^F(F)$.

Corollary 2.1.11. (Frobenius Theorem) Let $D$ be a division ring containing $\mathbb{R}$ in its center of finite dimension over $\mathbb{R}$. Then $D$ is isomorphic to $\mathbb{H}$, the Hamiltonian quaternion.

Corollary 2.1.12. (Wedderburn Theorem). If $K$ is a finite field, then any quaternion algebra over $K$ is isomorphic to $\text{M}(2, K)$.

2.2 Orders and Ideals

As the fractional ideals in a number field, there is a similar theory for ideals in a quaternion algebra. In this section, we let $R$ be a Dedekind domain and $K$ be its field of fractions.

2.2.1 Definitions

Definition 2.2.1. An $R$–lattice of a $K$-vector space $V$ is a finitely generated $R$-module contained in $V$. A complete $R$–lattice $\Lambda$ of $V$ is a $R$–lattice $\Lambda$ of $V$ such that $K \otimes_R \Lambda \simeq V$.

Example 2.2.1. Suppose that $R = \mathbb{Z}$, $K = \mathbb{Q}$, and let $B$ be the quaternion algebra $(-1, -1, \mathbb{Q})$.

1. Let $V = \mathbb{Q}(i) \cong \mathbb{Q}(\sqrt{m})$ and $\Lambda$ be the ring of integers of it. Then $\Lambda$ is a complete lattice.
2. Let $\Lambda_1 = R + Ri$ and $\Lambda_2 = R + Ri + Rj + Rij$. Then they are both $R$-lattices of $B$; while $\Lambda_2$ is complete, $\Lambda_1$ is not complete as a $R$-lattice of $B$.

Definition 2.2.2. An ideal of a quaternion algebra $B$ is a complete $R$-lattice in $B$. If an ideal of $B$ is also a ring with unity, it is called an order. Moreover, for a given order $\mathcal{O}$, we say that $I$ is a left ideal of $\mathcal{O}$ if $\mathcal{O}I \subset I$; $I$ is a right ideal of $\mathcal{O}$ if $I\mathcal{O} \subset I$. 

10
It is easy to see that the intersection of two ideals is again an ideal.

**Definition 2.2.3.** A maximal order of \( B \) is an order that is not properly contained in another order of \( B \). An intersection of two maximal orders of \( B \) is called an Eichler order.

Now if an ideal \( I \) is given, we can define two orders associated to \( I \), the **left order of \( I \)**,

\[
O_L(I) = \{ h \in B : hI \subseteq I \},
\]

and the **right order of \( I \)**,

\[
O_R(I) = \{ h \in B : Ih \subseteq I \}.
\]

**Definition 2.2.4.** An ideal \( I \) is said to be **two-sided** if \( O_L(I) = O_R(I) \), said to be **integral** if \( I \) is contained in one of \( O_L(I) \) and \( O_R(I) \). If \( O_L(I) \) and \( O_R(I) \) are both maximal orders, then \( I \) is called a **normal ideal**.

**Definition 2.2.5.** An element \( x \) of a quaternion algebra \( B \) is called to be **integral over \( R \)** if \( R[x] \) is a \( R \)-lattice of \( B \).

For instance, the element \( i \) in the quaternion algebra \( \mathbb{H}(-1,-1) \) is an integral element but \( i/2 \) is not. Actually, we have a useful criterion to determine whether an element is integral or not.

**Lemma 2.2.2.** An element of a quaternion algebra \( B \) is integral if and only if its reduced trace and norm are in the ring \( R \).

Related to the property of the integral elements, we have an equivalent definition of an order of a quaternion algebra.

**Proposition 2.2.3.** \( \mathcal{O} \) is an order of \( B \) if and only if \( \mathcal{O} \) is a ring of integral elements in \( B \) which contains \( R \) and a \( K \)-basis for \( B \).

From the equivalent definition of an order, it is easy to see that an integral ideal is an ideal whose elements are all integral elements. Combining with Zorn’s Lemma, one can prove the existence of a maximal order.

**Proposition 2.2.4.** Every order is contained in a maximal order.
There are also the analogue of the norm of an ideal, and the discriminant of an order as those in the algebraic number theory.

The **inverse of an ideal** $I$ is defined to be

$$I^{-1} = \{ h \in B : IhI \subset I \},$$

and the **product** of 2 ideals $I$ and $J$ is given by

$$IJ = \left\{ \sum_{i=1}^{n} h_i k_i \mid n \geq 0, h_i \in I, k_i \in J \right\}$$

which are also ideals. The **norm of** $I$, denoted by $N(I)$, is the $R$-fractional ideal generated by $\{ N(x) : x \in I \}$. The **dual** $I^*$ of $I$ is

$$I^* = \{ h \in B : \text{Tr}(hI) \subset R \}.$$

**Proposition 2.2.5.**

1. $II^{-1} \subseteq O_\ell(I)$ and $I^{-1}I \subseteq O_r(I)$.
2. The set $I^*$ is an ideal satisfying $O_\ell(I) \subset O_r(I^*)$ and $O_r(I) \subset O_\ell(I^*)$.

If $I$ is a left ideal of $\mathcal{O}$, then the **discriminant of** $I$ is defined by $D_I = N(I^{-1})N(I)$. Hence, the **discriminant of an order** $\mathcal{O}$ is $D_{\mathcal{O}} = N(O^{*-1})$.

**Proposition 2.2.6.** We have the following properties:

1. If $I$ is a left ideal of an order $\mathcal{O}$, the square of the discriminant of $I$, $D_I^2$, is equal to the $R$-fractional ideal generated by

$$\{ \det(\text{Tr}(x_i x_j)) : 1 \leq i, j \leq 4, x_i, x_j \in I \}.$$

In particular, if $I$ has free $R$-basis $\{ e_1, e_2, e_3, e_4 \}$, then $D_I^2$ is the principal $R$-fractional ideal $\det(\text{Tr}(e_i e_j))R$.

2. Let $\mathcal{O}$ be a maximal order and $I$ be a left ideal of $\mathcal{O}$. Then

$$D_I = N(I)^2 D_{\mathcal{O}}.$$

3. If an order $\mathcal{O}'$ is contained in another order $\mathcal{O}$, then $D_{\mathcal{O}}$ divides $D_{\mathcal{O}'}$. Therefore, $D_{\mathcal{O}} = D_{\mathcal{O}'}$ if and only if $\mathcal{O} = \mathcal{O}'$.

**Example 2.2.7.**

1. The discriminant of the order $M(2, R)$ is $R$. 

12
(2) Consider the two orders
\[ \mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \]
and
\[ \mathcal{O}' = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1 + i + j + ij}{2} \]
in the quaternion algebra \( \left( \frac{-1,-1}{\mathbb{Q}} \right) \). It obvious that \( \mathcal{O} \subset \mathcal{O}' \) and
\[ D_{\mathcal{O}'}^2 = 4\mathbb{Z} \supset 16\mathbb{Z} = D_{\mathcal{O}}^2. \]

2.2.2 Orders in \( \text{M}(2, K) \)
In the case of the quaternion algebra \( B = \text{M}(2, K) \). One can identify \( B \) with the endomorphism ring of some 2-dimensional vector space over \( K \). Let \( V \) be a vector space over \( K \) with basis \( \{e_1, e_2\} \). Then with respect to this basis, \( \text{M}(2, K) \) can be viewed as the algebra of endomorphisms of \( V \), say \( \text{End}(V) \).

Given a complete \( R \)-lattice \( \Lambda \) in the space \( V \), one can verify that
\[ \text{End}(\Lambda) = \{ \alpha \in \text{End}(V) : \alpha \Lambda \subset \Lambda \} \]
is a maximal order in \( \text{End}(V) \). Conversely, we can show that any maximal order is obtained by \( \text{End}(\Lambda) \) for some complete \( R \)-lattice \( \Lambda \). Given an order \( \mathcal{O} \) in \( \text{End}(V) \), we can associate a complete \( R \)-lattice of \( V \),
\[ \Lambda = \{ \alpha \in \text{Re}_1 + \text{Re}_2 : \mathcal{O} \alpha \subset \text{Re}_1 + \text{Re}_2 \}, \]
to the order \( \mathcal{O} \). Then \( \mathcal{O} \) is contained in the order \( \text{End}(\Lambda) \). In this way, we can see that the maximal orders of \( \text{End}(V) \) are \( \text{End}(\Lambda) \), where \( \Lambda \) runs over all complete lattices of \( V \).

**Proposition 2.2.8.** If \( R \) is a principal ideal domain, then each maximal order in \( \text{M}(2, K) \) is conjugate to the maximal order \( \text{M}(2, R) \).

2.3 Quaternion Algebras over Local Fields
For a local field \( K \), there are at most 2 isomorphism classes of quaternion algebras over \( K \), up to isomorphism. In the case of the Archimedean local field \( \mathbb{C} \), there is only one class, namely \( \text{M}(2, \mathbb{C}) \), by Corollary 2.1.3. When \( K = \mathbb{R} \),
as a result of Corollary 2.1.11, a quaternion algebra over $\mathbb{R}$ is isomorphic to $\text{M}(2, \mathbb{R})$ or the quaternions of Hamilton $\mathbb{H}$. If $K$ is non-Archimedean, then a quaternion algebra over $K$ is isomorphic to exactly one of $\text{M}(2, K)$ or the unique division quaternion algebra over $K$.

### 2.3.1 Quaternion algebras over non-Archimedean local fields

For a non-Archimedean local field $K$, we let $R$ be its ring of integers and $\pi$ be a fixed uniformizer with respect to the normalized additive valuation $\nu$ of $K$ such that $\nu(\pi) = 1$.

**Theorem 2.3.1.** There is a unique class of division quaternion algebra over $K$ and it is isomorphic to $\left(\pi e\right)_K$, where $e$ is a non-square element of $K$ such that $K(\sqrt{e})$ is the unique unramified quadratic extension field of $K$.

We define the **Hasse invariant** of the quaternion algebra $B$ by

$$\varepsilon(B) = \begin{cases} 1, & \text{if } B \cong \text{M}(2, K), \\ -1, & \text{otherwise.} \end{cases}$$

In the case of $K = \mathbb{Q}_p$, the Hasse invariant of $B = \left(\frac{a,b}{\mathbb{Q}_p}\right)$ coincides with the **Hilbert symbol** $(a,b)_p$. Recall that if the characteristic of the local field $K$ is different from 2, the Hilbert symbol $(a,b)$ for $a, b \in K^*$ is defined by

$$(a,b) = \begin{cases} 1, & \text{if } ax^2 + by^2 - z^2 = 0 \text{ has a non-trivial solution in } K^3, \\ -1, & \text{otherwise.} \end{cases}$$

**Remark 2.3.2.** This observation can be followed by Theorem 2.1.5. According to Theorem 2.3.1, for $p > 2$, we have a simple description for the Hilbert symbol $(a,b)_p$ with $p \nmid a$,

$$(a,b)_p = \left( \frac{a}{p} \right) \nu_p(b)$$

where $\nu_p(\cdot)$ is the additive valuation on $\mathbb{Q}_p$ so that $\nu_p(p^n) = n$, and $\left( \frac{\cdot}{p} \right)$ is the Legendre symbol.
2.3.2 Division quaternion algebras over non-Archimedean local fields

As we mention in Theorem 2.3.1, the quaternion algebra \((\pi, e_K)\) is the unique division quaternion algebra over \(K\), up to isomorphism. Therefore, for a division quaternion algebra \(B\), we may always assume that \(B = (\pi, e_K)\) and we can extend the normalized discrete valuation on \(K\) to \(B\). More precisely, the map \(\omega\) given by

\[
\omega(h) = \frac{1}{2} \nu(N(h)), \quad h \neq 0,
\]

defines a discrete valuation on \(B\). Then one may see that there is a unique maximal order in \(B\), which is the associated valuation ring

\[
\mathcal{O} = \{h \in B : w(h) \geq 0\} = \{h \in B : N(h) \in R\}
\]

with respect to the valuation \(w\). Moreover, the set

\[
P = \{h \in B : w(h) > 0\}
\]

is a two-sided prime ideal of \(\mathcal{O}\).

**Theorem 2.3.3.** Let \(B = (\pi, e_K)\), \(F = K(\sqrt{e})\), and \(\mathcal{O}\) be the unique maximal order in \(B\). As above, denote \(P\) the 2-sided prime ideal of \(\mathcal{O}\),

\[
P = \{h \in B : w(h) > 0\}.
\]

Then we have

1. \(P = \mathcal{O}j\) is a prime ideal of \(\mathcal{O}\) and \(P^2 = \mathcal{O}\pi\).
2. \(\mathcal{O} = R_F + R_Fj\), where \(R_F\) is the ring of integers of \(F\).
3. The discriminant of \(\mathcal{O}\) is the norm of the ideal \(P\), \(D_\mathcal{O} = \pi R\).

2.4 Maximal Orders in \(M(2, K)\) over a Non-Archimedean Local Field

As in the last section, we let \(K\) denote a non-Archimedean local field, and \(R\) be its valuation ring with respect to the valuation \(v\). If the quaternion algebra over \(K\) is not a division algebra, then it is isomorphic to \(M(2, K)\). In this section, we will focus on the maximal orders in \(M(2, K)\).
2.4.1 Classification of maximal orders

As we observed in section 2.2.2, each maximal order of $M(2, K)$ is isomorphic to the maximal order $M(2, R)$. More precisely, we have the following properties.

**Theorem 2.4.1.**  
(1) A maximal order of $M(2, K)$ is conjugate to $M(2, R)$ by an element of $GL(2, K)$.

(2) The set of all maximal orders is in one-to-one correspondence with $K^*GL(2, R) \setminus GL(2, K)$.

The standard coset representatives of $K^*GL(2, R) \setminus GL(2, K)$ are

$$
\begin{pmatrix}
\pi^a & c \\
0 & \pi^b
\end{pmatrix},
$$

where $a$ and $b$ are nonnegative integers and $c$ are from $R/(\pi)^b$, subject to the condition that $v(c) = 0$ if $a, b > 0$. Therefore, we can identify all maximal orders of $M(2, K)$ as

$$
\begin{pmatrix}
\pi^a & c \\
0 & \pi^b
\end{pmatrix}^{-1} M(2, R) \begin{pmatrix}
\pi^a & c \\
0 & \pi^b
\end{pmatrix}, \quad a, b \geq 0, c \mod \pi^b,
$$

and $c \notin \pi R$ if $a, b > 0$.

Also, Hijikata gave a classification of the Eichlers order of $M(2, K)$.

**Proposition 2.4.2.** If $\mathcal{O}$ is an order in $M(2, K)$, then the followings are equivalent.

1. $\mathcal{O}$ is an Eichler order.
2. There exists a unique pair of maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ such that $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$.
3. There exists a non-negative integer $n$ such that $\mathcal{O}$ is conjugate to $(\pi^n R \oplus R)$.
4. The order $\mathcal{O}$ contains $R \oplus R$ as a subring.

If an Eichler order is conjugate to the order $(\pi^n R \oplus R)$, we say that this Eichler order is of level $\pi^n R$. 

16
2.4.2 Graph of maximal orders

For more information described in this section, please see [56].

**Definition 2.4.1.** Let $O_1, O_2$ be two maximal orders in $M(2, K)$ and let $O$ be the Eichler order obtained as $O = O_1 \cap O_2$. Then if the index of $O$ in $O_1$ is $q^n$, then so is the index of $O$ in $O_2$. In this case, we call $n$ to be the **distance** between $O_1$ and $O_2$, denoted by 

$$d(O_1, O_2) = n.$$ 

Here $q$ is the cardinality of the residue field $R/\pi R$. In other words, the distance $d(O_1, O_2)$ equals to $n$ if the Eichler order $O_1 \cap O_2$ is of level $\pi^n R$.

We now define a graph $X$ of maximal orders as follows. The vertices of $X$ are the maximal orders and two vertices are connected by a simple edge if the two corresponding maximal orders has distance 1.

**Example 2.4.3.** Let $O_0 = M(2, R)$,

$$O_1 = (\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix})^{-1} O_0 (\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}) = (\begin{smallmatrix} R & \pi^{-1} R \\ \pi R & R \end{smallmatrix}),$$

and

$$O_2 = (\begin{smallmatrix} 1 & 0 \\ 0 & \pi \end{smallmatrix})^{-1} O_0 (\begin{smallmatrix} 1 & 0 \\ 0 & \pi \end{smallmatrix}) = (\begin{smallmatrix} R & \pi R \\ \pi^{-1} R & R \end{smallmatrix}).$$

We have $O_0 \cap O_1 = (\begin{smallmatrix} R & R \\ \pi R & R \end{smallmatrix})$, 

$$O_0 \cap O_2 = (\begin{smallmatrix} R & \pi R \\ \pi^{-1} R & R \end{smallmatrix}), \quad \text{and} \quad O_1 \cap O_2 = (\begin{smallmatrix} R & \pi R \\ \pi^{-1} R & R \end{smallmatrix}) \cong (\begin{smallmatrix} R & R \\ \pi R & R \end{smallmatrix}).$$

Thus, $d(O_0, O_1) = d(O_0, O_2) = 1$ and $d(O_1, O_2) = 2$. The subgraph of these maximal orders is

$$O_2 \quad \bullet \quad O_1 \quad \bullet \quad O_0$$

Note that the number of paths of length $n$ with a fixed starting vertex $O_0$ and without backtracking is equal to $q^n + q^{n-1}$, since this is the number of maximal orders of distance $n$ from $O_0$. These paths are in one-to-one correspondence with words $c_n c_{n-1} \ldots c_1$ of length $n$ formed by the $q + 1$ letters

$$\gamma_0 = (\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}), \quad \gamma_c = (\begin{smallmatrix} 1 & c \\ 0 & \pi \end{smallmatrix}), \quad c \in R/\langle \pi \rangle,$$

subject to the condition $c_{j+1} c_j$ is not in $M(2, \pi R)$. The path corresponding to such a word is the one connecting the maximal orders $O_0$, $c_1^{-1} O_0 c_1$, $\ldots$, $(c_j c_{j-1} \ldots c_1)^{-1} O_0 (c_j c_{j-1} \ldots c_1)$, for $j = 1, \ldots, n$. 

17
Example 2.4.4. Let $O_1 = M(2, \mathbb{Z}_2)$ and

$$O_2 = (\begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix})^{-1} O_1 (\begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix}) = [((\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}) (\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}) (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}))^{-1} O_1 (\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}) (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})].$$

The distance between $O_1$ and $O_2$ is 3. The subgraph of these corresponding maximal orders is

Here, the matrix $\alpha$ next to a vertex means that the maximal order is $\alpha^{-1} M(2, \mathbb{Z}_2) \alpha$.

**Proposition 2.4.5.** The graph $X$ is a ($q + 1$)-regular tree, i.e., a connected graph without cycles, and every vertex has precisely $q + 1$ edges connecting to it.

Example 2.4.6. Here is a subtree of maximal orders of $M(2, \mathbb{Q}_2)$.

Since the graph is a tree, for each pair of maximal orders $O_1$ and $O_2$, there is one and only one path from $O_1$ to $O_2$. In other words, the intermediate vertices that are on a path leading from $O_1$ to $O_2$ are uniquely determined by the pair $O_1$ and $O_2$. For instance, if $O_1 = M(2, R)$ and $O_2 = \gamma^{-n} O_1 \gamma^n$ with $\gamma = (\begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix})$, then the intermediate vertices connecting $O_1$ to $O_2$ are $\gamma^{-j} O_1 \gamma^j$, $j = 1, \ldots, n - 1$.

Remark 2.4.7. We remark that the group $\text{PGL}(2, K)$ acts on the coset $K^* \text{GL}(2, R) \backslash \text{GL}(2, K)$, and hence acts by conjugation on the tree of maximal orders in $M(2, K)$. In particular, $\text{PGL}(2, K)$ acts on the set

$$\mathcal{L}^{(n)} = \{(O_1, O_2) \in X \times X : d(O_1, O_2) = n\}$$
transitively.

2.5 Quaternion Algebras over Number Fields

In this section, let us see something about the classification of quaternion algebras over a number field. Let $K$ be a number field, and $R$ be its ring of integers. Let $K_v$ be the local field with respect to the place $v$ of $K$.

2.5.1 Classification

A quaternion algebra $B$ over a number field $K$ is said to be **ramified at** $v$ if its localization $B_v = B \otimes K_v$ with respect to the place $v$ is a division algebra. Otherwise, $B$ is **unramified or split** at $v$.

**Theorem 2.5.1. (Hasse-Minkowski Theorem)**
The quaternion algebra $B$ is isomorphic to $M(2, K)$ if and only if $B$ splits over $K_v$ for all places $v$.

Let $\text{Ram}(B)$ denote the set of ramified places of $B$.

**Definition 2.5.1.** The **reduced discriminant** of a quaternion algebra $B$ is the integral ideal of $R$ defined by

$$D_B = \prod_{v \in \text{Ram}(B), v < \infty} v.$$ 

In the case that $R$ is a principal ideal domain, we identify the ideal $D_B$ with its generator, up to units. For example, the reduced discriminant of a quaternion algebra over $\mathbb{Q}$ is given by an integer.

From the following theorem, we conclude that the isomorphism class of a quaternion algebra $B$ is almost uniquely determined by the reduced discriminant.

**Theorem 2.5.2.**

1. The cardinality of $\text{Ram}(B)$ is finite and even.
2. Two quaternion algebras $B$ and $B'$ over $K$ are isomorphic if and only if $\text{Ram}(B) = \text{Ram}(B')$.
3. Given a finite set $S$ of noncomplex places of $K$ such that $|S|$ is even, then there exists a quaternion algebra $B$ over $K$ such that $\text{Ram}(B) = S$. 

19
Therefore, if an even number of noncomplex places of \( K \) is given, then there exists one and only one \( K \)-quaternion algebra that ramifies exactly at these places.

**Example 2.5.3.**

1. A quaternion algebra over a number field \( K \) is isomorphic to \( M(2, K) \) if and only if \( D_B = R \).
2. The discriminant of the quaternion algebra \( \left( \frac{-1, -1}{q} \right) \) is 2, since the values of the Hilbert symbols are

\[
(-1, -1)_p = \begin{cases} 
-1, & \text{if } p = \infty, 2, \\
1, & \text{if } p > 2.
\end{cases}
\]

**Definition 2.5.2.** For a totally real number field \( K \), if a quaternion algebra over \( K \) is ramified at all the real infinite places, we say that the quaternion algebra is **definite**; otherwise, it is **indefinite**.

We remark that a quaternion algebra \( B \) is definite if and only if the quadratic form given by \( \text{Tr}(x\bar{y}) \) on \( B \) is positive definite.

### 2.6 Orders in a Quaternion Algebra over a Number Field

Let \( I \) be an ideal in a quaternion algebra \( B \) over a number field \( K \). Denote \( R_v \) by the ring of integers of the localization \( K_v \). Then the completion of \( I \) at \( v \), \( I_v = I \otimes_{\mathbb{Z}} R_v \), is an ideal in the quaternion algebra \( B_v \) and \( I = B \cap (\prod_v I_v) \). As the Hasse-Minkowski theorem for quaternion algebras, being a maximal order or an Eichler order satisfies the local-global correspondence.

#### 2.6.1 Orders in the global case

Let \( \mathcal{O} \) be an order in \( B \). It is clear that \( \mathcal{O}_v \) is again an order in \( B_v \) and \( (\mathcal{O}_v)_v = \mathcal{O}_v \). Therefore, we have a criterion for global maximal orders from the information of the discriminants.

**Proposition 2.6.1.** Let \( \Lambda \) be a lattice in a quaternion algebra \( B \) over \( K \). For any finite place \( v \) in \( K \), we consider the local lattice \( L_v \) of \( L \) in \( B_v \) with respect to \( v \). Assume that \( L_v = \Lambda_v \) for almost all \( v \). Then there exists a lattice \( \Lambda' \) in \( B \) such that \( \Lambda'_v = L_v \) for all finite places \( v \).
Proposition 2.6.2. An order $\mathcal{O}$ is maximal in the quaternion algebra $B$ if and only if its discriminant is equal to the discriminant of $B$, i.e, $D_{\mathcal{O}} = D_B$.

Example 2.6.3. In the quaternion algebra $B = \left( \frac{-1-1}{\mathbb{Q}} \right)$, the order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ is not a maximal order and we can verify that its discriminant is $4$; the order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+i}{2}$ is a maximal order, whose discriminant is $2$.

Lemma 2.6.4. Let $I$ be an ideal in $B$ so that its right order $\mathcal{O} = \mathcal{O}_r(I)$ is a maximal order. Then there exists an element $h_v \in B_v^*$ so that $I_v = h_v I_v$.

Corollary 2.6.5. For an ideal $I$ in $B$,

1. the right order of $I$, $\mathcal{O}_r(I)$, is maximal if and only if the left order of $I$, $\mathcal{O}_l(I)$, is maximal.
2. if $I$ is normal then $I^{-1}I = \mathcal{O}_r(I)$ and $II^{-1} = \mathcal{O}_l(I)$.

Definition 2.6.1. The level of a global Eichler order is the unique integral ideal $N_{\mathcal{O}}$ in $R$ so that $(N_{\mathcal{O}})_v$ is the level of each $\mathcal{O}_v$ at each unramified finite place of $K$. That is, $N_{\mathcal{O}} = \prod_v N_{\mathcal{O}_v}$. If $R$ is a PID, we identify the ideal $N_{\mathcal{O}}$ with its generator, up to units.

It is easy to obtain the relation between the discriminant of an Eichler order and the reduced discriminant of the quaternion algebra $B$ which it belongs to.

Proposition 2.6.6. If $\mathcal{O}$ is an Eichler order of level $N$, then the discriminant of $\mathcal{O}$ is $D_{\mathcal{O}} = D_{B}N$.

Unlike the case of maximal orders, we have no explicit characterization of Eichler orders in terms of the discriminant, in general. For maximal orders, we have a criterion to check an order is maximal or not (see Proposition 2.6.2). One can not, however, conclude that a given order is an Eichler order from its discriminant except its discriminant is a product of distinct prime ideals. In the following subsection, as an example, we will give the characterization of Eichler orders in quaternion algebras over $\mathbb{Q}$.
2.6.2 Eichler orders in \( \mathbb{Q} \)-quaternion algebras

Let \( B \) be a quaternion algebra over \( \mathbb{Q} \) of discriminant \( D \). According to the proposition 2.6.1, for each positive integer \( N \), there exists an Eichler order \( \mathcal{O} \) of level \( N \).

We now give a characterization of Eichler orders in a quaternion algebra over \( \mathbb{Q} \).

**Proposition 2.6.7.** Let \( \mathcal{O} \) be an order in a \( \mathbb{Q} \)-quaternion algebra \( B \) of discriminant \( D \). Let \( N \) be a positive integer relatively prime to \( D \). Then the following conditions are equivalent:

1. \( \mathcal{O} \) is an Eichler order of level \( N \).
2. For each prime number, the localization \( \mathcal{O}_p \) of \( \mathcal{O} \) at \( p \), is maximal if \( p \nmid N \); it is isomorphic to the order \( \left( \mathbb{Z}_p \mathbb{Z}_p \mathbb{Z}_p \right) \) if \( p \mid N \).
3. For each prime number, the localization \( \mathcal{O}_p \) of \( \mathcal{O} \) at \( p \) is maximal if \( p \mid D \) and \( \mathcal{O}_p \) is isomorphic to the order \( \left( \mathbb{Z}_p \mathbb{Z}_p \mathbb{Z}_p \mathbb{Z}_p \right) \) if \( p \nmid D \).

**Proposition 2.6.8.** Let \( \mathcal{O} \) be an order in a \( \mathbb{Q} \)-quaternion algebra \( B \) of discriminant \( D \).

1. If \( \mathcal{O} \) is an Eichler order, then \( D_\mathcal{O} = DN_\mathcal{O} \) with \( \gcd(D, N_\mathcal{O}) = 1 \).
2. If \( D_\mathcal{O} = DN \) is a square-free integer, then \( \mathcal{O} \) is an Eichler order of level \( N \).
3. Let \( \mathcal{O} \) and \( \mathcal{O}' \) be orders in \( B \) and they are conjugate. Then \( \mathcal{O} \) is an Eichler order of level \( N \) if and only if \( \mathcal{O}' \) is an Eichler order of level \( N \).

2.6.3 Class numbers and type numbers

**Definition 2.6.2.** Let \( I \) and \( J \) be two ideals of a quaternion algebra \( B \). We say that \( I \) and \( J \) are **left equivalent** if \( I = hJ \), for some \( h \in B^* \). The equivalent classes of the left ideals of an order \( \mathcal{O} \) under this equivalence relation are called **left ideal classes** of \( \mathcal{O} \). The right ideal classes are similarly defined.

We have the following correspondences between ideal classes, which provides that the number of left ideal classes of \( \mathcal{O} \) is the same as the number of right ideal classes of \( \mathcal{O} \).

22
Lemma 2.6.9. Let $I, J$ be ideals. Then

(1) The map $I \mapsto I^{-1}$ gives a bijection between the left ideal classes of $O_\ell(I)$ and the right ideal classes of $O_r(I)$.

(2) The map $I \mapsto JI$ gives a bijection between the left ideal classes of $O_\ell(I) = O_r(J)$ and the right ideal classes of $O_\ell(J)$.

Definition 2.6.3. The class number of an order $O$ is the number of left (or right) ideal classes of $O$. The class number of a quaternion algebra is the class number of its maximal orders.

Theorem 2.6.10. The class number of a quaternion algebra $B$ over a number field $K$ is finite.

For more details about the finiteness of the class number, please refer for instance to Vignéras’ book [66]: chapter 5.

We have seen in section 2.2.2 that if the ring of integers of $K$ is a principal ideal domain, then all maximal orders in the quaternion algebra $M(2, K)$ are conjugate to each other. However, this property does not hold in general. We now determine the number of conjugacy classes of an given order, which is finite.

Definition 2.6.4. Two orders are of the same type if they are conjugate by an inner automorphism of $B$.

Lemma 2.6.11. Let $O$ and $O'$ be two orders of $B$. Then the followings are equivalent.

(1) $O$ and $O'$ are of the same type.

(2) $O$ and $O'$ are related by a principal ideal. The sentence $O$ is related to $O'$ means that there exists a left ideal of $O$ that is also a right ideal of $O'$.

(3) $O$ and $O'$ are related, and if $I$ is a left ideal of $O$ and $J$ is a right ideal of $O'$, then $Ih = J(A)$, for some $h \in B^*$, some 2-sided ideal $A$ of $O$, and $(A)$ is an ideal of the form $I^{-1}AI$ with $O_\ell(I) = O$.

The number of types of orders that are related to a given order $O$ is called the type number of $O$. In other words, the type number is defined as the number of conjugacy classes in the set of related orders.

Corollary 2.6.12. The number of types of orders that are related to a given order $O$ is less than or equal to the ideal class number of $O$, and hence is finite.
2.7 Groups of Quaternion Transformations

From now, we will focus on the indefinite quaternion algebra over a totally real number field, especially the rational field.

Let $B$ be a quaternion algebra over a totally real number field $K$ such that $B$ splits exactly at one infinite place. That is,

$$B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \text{M}(2, \mathbb{R}) \times \mathbb{H}^{|K:Q|^{-1}},$$

where $\mathbb{H}$ is Hamilton’s quaternions. Notice that we have a natural embedding from $B$ into $B \otimes_{\mathbb{Q}} \mathbb{R}$, we now let $i_{\infty} : B \mapsto \text{M}(2, \mathbb{R})$ be the projection onto the first factor. Let $O$ be an order of $B$, define

$$O^1 = \{ \gamma \in O : N(\gamma) = 1 \},$$

and $\Gamma(O) = i_{\infty}(O^1)$.

Then $\Gamma(O)$ is a discrete subgroup of $\text{SL}(2, \mathbb{R})$, and hence it acts on the upper half plane $\mathfrak{H} = \{ \tau : \mathbb{C} : \text{Im}(\tau) > 0 \}$ by the usual fractional linear transformations.

2.7.1 Linear fractional transformations

We first recall the well-known properties of the linear fractional transformation of $\mathbb{P}^1(\mathbb{C})$ given by

$$\gamma : \tau \mapsto \frac{a\tau + b}{c\tau + d}, \quad a, b, c, d \in \mathbb{R}, \quad ad - bc > 0.$$ 

Denote by $\text{GL}(2, \mathbb{R})^+$ the group of $2 \times 2$ real matrices of positive determinant. Observe that a linear fractional transformation $\gamma$ determines the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{R})^+$ up to a scalar multiplication. Hence, dividing by a suitable scalar, we may represent $\gamma$ by a matrix of determinant 1. The group $\text{SL}(2, \mathbb{R})$ contains two elements $\pm 1$ which act trivially, and the factor group

$$\text{PSL}(2, \mathbb{R}) = \text{SL}(2, \mathbb{R})/\{\pm 1\}$$

is identified with the group of linear fractional transformations.

Furthermore, the space $\mathbb{P}^1(\mathbb{C})$ splits into three invariant subspace of $\text{SL}(2, \mathbb{R})$, namely, the upper half-plane $\mathfrak{H}$, the lower half-plane $\bar{\mathfrak{H}}$, and the real axis $\mathbb{P}^1(\mathbb{R})$. Moreover, we have

$$(\text{Im} \gamma \tau)^{-1} |d\gamma \tau| = (\text{Im} \tau)^{-1} |d\tau|.$$
Consequently, the differential form

\[ ds^2 = y^{-2}(dx^2 + dy^2) \]

is invariant under the action of \( \text{SL}(2, \mathbb{R}) \). With the metric derived from this differential the upper half-plane becomes a Riemannian manifold.

The upper half-plane \( \mathcal{H} \) is equipped with the metric is the Poincaré model of a hyperbolic plane (curvature \(-1\)). Furthermore, the metric \( ds^2 = y^{-2}(dx^2 + dy^2) \) implies that the hyperbolic measure on \( \mathcal{H} \) is \( dx\,dy/y^2 \).

### 2.7.2 Quaternion transformations

Recall that a nonidentity element \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) of \( \text{SL}(2, \mathbb{R}) \) is called **parabolic**, **hyperbolic**, or **elliptic** if \( \gamma \) has one fixed point, 2 distinct points on \( \mathbb{P}^1(\mathbb{R}) \), or a pair of conjugate complex numbers, respectively. The points \( \tau \) fixed by \( \gamma \) are the roots of

\[ c\tau^2 + (d - a)\tau - b = 0. \]

Suppose that the element \( \gamma \) lies in \( \Gamma(\mathcal{O}) \). Then its determinant is 1 and the trace is an integer. Hence, it can be simplified that \( \gamma \) is parabolic, elliptic, or hyperbolic, corresponding to whether \( |\text{Tr}(\gamma)| = 2 \), \( |\text{Tr}(\gamma)| < 2 \), or \( |\text{Tr}(\gamma)| > 2 \).

**Definition 2.7.1.** Let \( \gamma \) be an element of \( \Gamma(\mathcal{O}) \).

1. The fixed point of a parabolic element is called a **cusp**.
2. The point \( \tau \) in the upper half-plane fixed by an elliptic element is called an **elliptic point** of order \( e \), where \( e \) is the number of elements in \( \Gamma(\mathcal{O})/\pm 1 \) that fixes \( \tau \). In other words, \( e \) is the order of the isotropy subgroup of \( \tau \) in \( \Gamma(\mathcal{O})/\pm 1 \).

**Remark 2.7.1.** For an elliptic element \( \gamma \in \Gamma(\mathcal{O}) \), \( \gamma \) is of order 2 if and only if \( \text{Tr}(\gamma) = 1 \); \( \gamma \) is elliptic of order 3 if and only if \( |\text{Tr}(\gamma)| = 1 \).

**Proposition 2.7.2.** If \( \Gamma(\mathcal{O}) \) has a parabolic element, then the related quaternion algebra must be \( \mathbb{M}(2, \mathbb{Q}) \).

This proposition tells us that the cusps are precisely the elements of \( \mathbb{P}^1(\mathbb{Q}) \). This is because that \( \mathbb{M}(2, \mathbb{Z}) \) is the unique maximal order in \( \mathbb{M}(2, \mathbb{Q}) \), up to conjugation.
2.8 Shimura Curves

Given an order \(O\) in an indefinite quaternion algebra \(B\) over a totally real number field \(K\), fix an embedding \(i_\infty : B \hookrightarrow \text{M}(2, \mathbb{R})\). From above discussions, the action of \(\Gamma(O) = i_\infty(O^1)\) on the upper-half plane gives us the structure of Riemann surface, i.e., a non-singular irreducible projective algebraic curve.

Note that cusps can only appear when the quaternion algebra is \(\text{M}(2, \mathbb{Q})\). Therefore, while \(B \neq \text{M}(2, \mathbb{Q})\), the quotient space \(\Gamma(O) \backslash \mathfrak{H}\) has a complex structure as a compact Riemann surface; for the matrix algebra \(B = \text{M}(2, \mathbb{Q})\), we compactify the Riemann surface \(\Gamma(O) \backslash \mathfrak{H}\) by adding cusps. We denote \(X(O)\) the quotient space \(\Gamma(O) \backslash \mathfrak{H}\), or \(\Gamma(O) \backslash \mathfrak{H}^*\) if \(B = \text{M}(2, \mathbb{Q})\), where \(\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})\). This is the so-called Shimura curve associated to \(O\). In the case of \(B = \text{M}(2, \mathbb{Q})\), the curves \(X(O)\) are known as the classical modular curves.

Example 2.8.1. (1) Let \(B = \text{M}(2, \mathbb{Q})\). If \(O = \text{M}(2, \mathbb{Z})\), then \(\Gamma(O) = \text{SL}(2, \mathbb{Z})\) and \(X(O)\) is the modular curve \(X(1) = X_0(1)\). In particular, the modular curve \(X_0(N)\) is associated to the Eichler order \(O = (\frac{\mathbb{Z}}{NZ}, \frac{\mathbb{Z}}{Z})\), \(N \in \mathbb{Z}_{\geq 0}\).

(2) Let \(O\) be the order \(\mathbb{Z} + Zi + Zj + Z \frac{1+i+i+j}{2}\) in the quaternion algebra \(B = \left(\begin{smallmatrix} -1 & 3 \\ -3 & -1 \end{smallmatrix}\right)\). The quaternion algebra is ramified at the finite places 2 and 3. An embedding \(i_\infty : B \to \text{M}(2, \mathbb{R})\) is given by \(i_\infty : B \to \text{M}(2, \mathbb{R})\) is

\[
\begin{align*}
i &\mapsto \left(\begin{array}{cc}
0 & -1 \\
1 & 0
\end{array}\right), \\
j &\mapsto \left(\begin{array}{cc}
\sqrt{3} & 0 \\
0 & -\sqrt{3}
\end{array}\right)
\end{align*}
\]

and

\[
i_\infty(O^1) = \left\{ \left(\begin{array}{cc}
\alpha & \beta \\
-\beta & \alpha
\end{array}\right) : \alpha\bar{\alpha} + \beta\bar{\beta} = 1, \ \alpha, \beta \in \mathbb{Z}[\sqrt{3}] \right\}.
\]

In the case of \(B = \text{M}(2, \mathbb{Q})\), we are most interested in the congruence subgroup of \(\text{SL}(2, \mathbb{Z})\), that is, the subgroup of \(\text{SL}(2, \mathbb{Z})\) contains the principal congruence subgroup

\[
\Gamma(N) = \left\{ \gamma \in \text{SL}(2, \mathbb{Z}) : \gamma = 1 \mod N \right\}
\]

for some positive integer \(N\), especially the Hecke congruence group

\[
\Gamma_0(N) = \left\{ \left(\begin{array}{cc}
a & b \\
cN & d
\end{array}\right) \in \text{SL}(2, \mathbb{Z}) : a = 1 \mod N \right\},
\]

26
which is corresponding to the Eichler order $\mathcal{O} = \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right).$ The related modular curve is denoted by $X_0(N)$. For the compact Riemann surface $X(\mathcal{O})$, its genus can be formulated by

$$g(X(\mathcal{O})) = 1 + \frac{\text{Vol}(X(\mathcal{O}))}{2} - \frac{1}{2} \sum e_i \left( 1 - \frac{1}{e_i} \right).$$

where the sum runs over all the elliptic points and cusps with $e_i$ being their respective orders (write $e_i = \infty$ for a cusp). If we are considering the modular curves, we can simplify the formula.

**Proposition 2.8.2.** Let $\Gamma(\mathcal{O})$ be a subgroup of $\text{SL}(2, \mathbb{Z})$ of index $m$. Let $v_2$, $v_3$, $v_\infty$ be the numbers of $\Gamma(\mathcal{O})$-inequivalent elliptic points of order 2, elliptic points of order 3, and cusps, respectively. Then the genus $g$ of $X(\mathcal{O})$ is given by the formula

$$g = 1 + \frac{m}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}.$$

### 2.9 Automorphic Forms on Shimura Curves

Let $X(\mathcal{O})$ be the Shimura curve associated to the order $\mathcal{O}$ in an indefinite quaternion algebra $B$. In this section, we let $k \in 2\mathbb{Z}$, and use the notation $\Gamma$ to be the group $\Gamma(\mathcal{O})$ for short.

**Definition 2.9.1.** An automorphic form of weight $k$ on $\Gamma$ is a holomorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ such that

$$f \left( \frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^k f(\tau),$$

for all $\tau \in \mathcal{H}$ and all $(a\ b\ c\ d) \in \Gamma$.

If $f$ is meromorphic and $k = 0$, then $f$ is called an automorphic function.

For the quaternion algebra $B = M(2, \mathbb{Q})$, we also need additional conditions at cusps.

**Definition 2.9.2.** Let $\Gamma$ be a subgroup of $\text{SL}(2, \mathbb{Z})$ of a finite index. A holomorphic function $f : \mathcal{H} \rightarrow \mathbb{C}$ is a modular form (automorphic form) of weight $k$ with respect to $\Gamma$ if
(1) \( f \left( \frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^k f(\tau), \) for all \( \tau \in \mathcal{H} \) and all \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \).

(2) \( f(\tau) \) is holomorphic at every cusp.

If, in addition to (1) and (2), the function also satisfies

(3) \( f \) vanishes at every cusp,

then the function \( f \) is a \textbf{cusp form} of weight \( k \) with respect to \( \Gamma \).

Sometimes we may relax the holomorphic condition in the definition of a modular form to only meromorphic. In this case, we call such a function a \textbf{meromorphic modular form}. A meromorphic modular form of weight 0 is called a \textbf{modular function}.

By observation, the automorphic forms of a given weight \( k \) forms a complex vector space. We denote it by \( M_k(\Gamma) \); the space of all cusp forms of weight \( k \) on \( \Gamma \) is denoted by \( S_k(\Gamma) \).

It is easy to see that the weight 0 automorphic forms on \( \Gamma \) are exactly the constant functions. Using the Riemann-Roch Theorem, one can figure out the dimension formulae.

\[ \text{Proposition 2.9.1.} \quad \text{Assume that} \quad B \neq M(2, \mathbb{Q}) \quad \text{and the genus of} \quad X(O) \quad \text{is} \quad g. \quad \text{Then the dimension of the space of automorphic forms of weight} \quad k \quad \text{on} \quad \Gamma \quad \text{is} \]

\[ \dim M_k(\Gamma(O)) = \begin{cases} 0, & \text{if} \quad k < 0, \\ 1, & \text{if} \quad k = 0, \\ g, & \text{if} \quad k = 2, \\ (g - 1)(k - 1) + \sum_j \left\lfloor \frac{k}{2} \left( 1 - \frac{1}{e_j} \right) \right\rfloor, & \text{if} \quad k \geq 4, \end{cases} \]

where the number \( e_j \) runs over all orders of \( \Gamma \)-inequivalent elliptic points.

The dimension formula for the case \( B = M(2, \mathbb{Q}) \) is slightly different.

\[ \text{Proposition 2.9.2.} \quad \text{Let} \quad \Gamma \quad \text{be a subgroup of finite index of} \quad \text{SL}(2, \mathbb{Z}). \quad \text{Assume} \quad \text{that the genus of} \quad X(O) \quad \text{is} \quad g. \quad \text{Let} \quad c \quad \text{be the number of inequivalent cusps of} \quad \Gamma, \quad \text{and} \quad e_1, \ldots, e_r \quad \text{be the orders of inequivalent elliptic points. We have} \]

\[ \dim M_k(\Gamma) = \begin{cases} 0, & \text{if} \quad k < 0, \\ 1, & \text{if} \quad k = 0, \\ g + c - 1, & \text{if} \quad k = 2, \\ (k - 1)(g - 1) + \sum_{i=1}^r \left\lfloor \frac{k}{2} \left( 1 - \frac{1}{e_i} \right) \right\rfloor + \frac{k^2}{2} & \text{if} \quad k > 2, \end{cases} \]
and

\[
\dim S_k(\Gamma) = \begin{cases} 
0, & \text{if } k \leq 0, \\
g, & \text{if } k = 2, \\
\dim M_k(\Gamma) - c, & \text{if } k > 2.
\end{cases}
\]

### 2.10 Construction of Modular Forms

There are many methods to construct modular forms, for example, using Eisenstein series, Dedekind eta function, theta series and so on. Most of the ways are dependent on the Fourier expansions of modular forms. However, because of the lack of cusps in the case \( B \not= M(2, \mathbb{Q}) \), there are very few explicit methods for constructing automorphic forms on Shimura curves. More recently, Yang [69] gave a method to construct automorphic forms on Shimura curves of genus 0. The key ingredient is to express automorphic forms using the solutions of certain differential equation.

In this section, I would like to introduce a way for constructing modular forms on \( \Gamma_0(N) \) from Dedekind eta function.

#### 2.10.1 Fourier expansion of a modular form

For the modular group \( \text{SL}(2, \mathbb{Z}) \), all rational numbers are equivalent to the point \( \infty \) and hence \( \text{SL}(2, \mathbb{Z}) \) has only one cusp, represented by \( \infty \). More precisely, there exists a matrix \( \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \) sending \( \infty \) to the rational number \( a/c \) with \( \gcd(a, c) = 1 \). Given a subgroup \( \Gamma \) of \( \text{SL}(2, \mathbb{Z}) \), a function \( f \) satisfies

\[
f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau)
\]

if and only if the function

\[
g(\tau) = f| [\sigma]_k(\tau) = (c\tau + d)^{-k} f \left( \frac{a\tau + b}{c\tau + d} \right)
\]

is invariant under the action of \( \sigma^{-1}\Gamma\sigma \). In particular, \( g(\tau) \) is invariant under the substitution \( \tau \mapsto \tau + h \), where \( h \) is the smallest positive integer so that \( (\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}) \in \pm \Gamma \), namely the width of the cusp \( a/c \). Therefore, if we assume that the modular form \( f \) is holomorphic at \( \infty \), then \( f \) has a Fourier expansion

\[
f(\tau) = \sum_{n \geq 0} a_n q^n, \quad \text{where } q = e^{2\pi i \tau/h}.
\]

Moreover, if \( f \) is a cusp form, the coefficient \( a_0 \) is equal to 0.
2.10.2 Dedekind eta function

Definition 2.10.1. Let $\tau \in \mathbb{H}$, and write $q = e^{2\pi i \tau}$. The Dedekind eta function $\eta(\tau)$ is defined by

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

To consider the action of $\text{PSL}(2, \mathbb{Z})$ on the Dedekind eta function, we have the following transformation law for $\eta(\tau)$.

Proposition 2.10.1. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$, the transformation formula for $\eta(\tau)$ is given by, for $c = 0$,

$$\eta(\tau + b) = e^{\pi ib/12} \eta(\tau),$$

and, for $c > 0$,

$$\eta(\gamma \tau) = \epsilon(a, b, c, d) \sqrt{\frac{ct + d}{i}} \eta(\tau)$$

with

$$\epsilon(a, b, c, d) = \begin{cases} 
\left( \frac{d}{c} \right) e^{\pi i (c(1-c)/2 + d(a+c+1)/12)}, & \text{if } c \text{ is odd}, \\
\left( \frac{c}{d} \right) e^{\pi i (ac(1-d^2)+d(b-c+3))/12}, & \text{if } d \text{ is odd},
\end{cases}$$

where $\left( \frac{d}{c} \right)$ is the Legendre-Jacobi symbol and when $d$ is negative $\left( \frac{c}{d} \right)$ is set to be $\left( \frac{c}{|d|} \right)$.

This simple transformation formula for $\eta(\tau)$ enables us to establish a sufficient condition for a product of $\eta(r\tau)$ to be modular on $\Gamma_0(N)$.

Theorem 2.10.2. (Newman) Let $N$ be a positive integer. If

$$f(\tau) = \prod_{h|N} \eta(h\tau)^{e_h}$$

satisfies
(1) \( \sum_{h|N} e_h \equiv 0 \mod 4 \),
(2) \( \prod_{h|N} h^{e_h} \) is a square of a rational number,
(3) \( \sum_{h|N} e_h h \equiv 0 \mod 24 \),
(4) \( \sum_{h|N} e_h N/h \equiv 0 \mod 24 \),

then \( f(\tau) \) is a meromorphic modular form of weight \( \sum_{h|N} e_h/2 \) on \( \Gamma_0(N) \).

Example 2.10.3. Let us look some examples for \( N = 6 \) and \( N = 37 \).

(1) There are 2 cusps of the group \( \Gamma_0(37) \), represented by 0 and \( \infty \). The product of eta functions \( \eta(\tau)^2 \eta(37\tau)^{-2} \) is a modular function on \( \Gamma_0(37) \) having poles only at \( \infty \) of order 3.
(2) The cusps of \( \Gamma_0(6) \) are \( \infty \), 0, 1/2, and 1/3. The functions

\[ \frac{\eta(3\tau)^3 \eta(6\tau)^3}{\eta(\tau)\eta(2\tau)} \quad \frac{\eta(\tau)^2 \eta(6\tau)^{12}}{\eta(2\tau)^4 \eta(3\tau)^6} \quad \text{and} \quad \frac{\eta(2\tau)^4 \eta(6\tau)^4}{\eta(\tau)^2 \eta(3\tau)^2} \]

are modular forms of weight 2 on \( \Gamma_0(6) \). Moreover, we have the equality

\[ \frac{\eta(3\tau)^3 \eta(6\tau)^3}{\eta(\tau)\eta(2\tau)} + \frac{\eta(\tau)^2 \eta(6\tau)^{12}}{\eta(2\tau)^4 \eta(3\tau)^6} = \frac{\eta(2\tau)^4 \eta(6\tau)^4}{\eta(\tau)^2 \eta(3\tau)^2}. \]
Chapter 3

Orders of $\text{M}(2, K)$ over a Non-Archimedean Local Field

The aim of this chapter is to classify the orders which are the intersections of finitely many maximal orders in the matrix algebra $\text{M}(2, K)$ over a non-Archimedean local field $K$.

The chapter is followed by the article [63] and it is organized as follows. In section 3.1, I will say a few words about our goal, state the main theorems, and give some examples of the orders that are not obtained by the intersection of maximal orders. In section 3.2, we introduce an algorithm for obtaining intersection orders. In Section 3.3, we present a proof of the main lemma, Lemma 3.2.4. Finally, in the last section, we will complete the classification of the intersections of maximal orders in $\text{M}(2, K)$.

3.1 Introduction

3.1.1 Motivation

Our motivation to study orders in $\text{M}(2, K)$ arises from their connection to the arithmetic of quaternion algebras over global fields, which in turn has applications to the theory of modular forms. For example, if $B$ is a definite quaternion algebra of discriminant $q$ over $\mathbb{Q}$ and $\mathcal{O}$ is the intersection of two maximal orders in $B$, then we can associate theta series to the order $\mathcal{O}$. These theta series are modular forms on $\Gamma_0(qN)$ for a suitable integer $N$. To be more precise, take an Eichler order $\mathcal{O}$ of level $N$ in a definite quaternion
algebra over \( \mathbb{Q} \), we let \( I \) denote a left ideal of \( \mathcal{O} \). The theta series associated to \( I \) defined by
\[
\theta_I(\tau) = \sum_{x \in I} e^{2\pi i \tau N(x)/N(I)}, \quad \text{Im} \tau > 0
\]
is a modular form of weight 2 of level \( qN \), where \( N(x) \) means the reduced norm of the element \( x \) and \( N(I) = \gcd\{N(x) : x \in I\} \). Then works of Eichler [23], Higitaka, Pizer, Shemanske, [38] and others showed that the action of Hecke operators on theta series can be described in terms of Brauer matrices. These results enabled them to solve a basis problem for the space of modular forms on \( \Gamma_0(qN) \). Moreover, linear relations among these theta series have deep arithmetic meaning in terms of \( L \)-functions of cusp forms (See [15, 31, 32, 34, 51]). In view of these results, it is natural to address the following question:

*If we take the intersections of finitely many maximal orders in a definite quaternion algebra over \( \mathbb{Q} \), what kind of orders do we get, and what kind of modular forms are the theta series associated to these orders?*

According to the local-global correspondence, we should first consider the intersection of maximal orders in \( M(2, \mathbb{Q}_p) \). Thus, the goal of this chapter is to classify all intersection orders.

### 3.1.2 Main results

At the first sight, this problem may look a formidable task to accomplish because of the sheer amount of possibilities. The following surprising property about orders greatly reduces the problem.

**Theorem 3.1.1.** Let \( K \) be a non-Archimedean local field with valuation ring \( R \). Then given any set of finitely many maximal orders \( \mathcal{O}_1, \ldots, \mathcal{O}_r \) in \( M(2, K) \), there exist \( i_1, i_2, \) and \( i_3, 1 \leq i_1, i_2, i_3 \leq r \), such that
\[
\bigcap_{i=1}^{r} \mathcal{O}_i = \mathcal{O}_{i_1} \cap \mathcal{O}_{i_2} \cap \mathcal{O}_{i_3}.
\]
(Note that the indices \( i_1, i_2, i_3 \) need not be distinct.)
In fact, given any finite number of maximal orders $O_1, \ldots, O_r$, we can explicitly determine the three maximal orders $O_{i1}, O_{i2}, O_{i3}$ that give the intersection $\cap_{i=1}^r O_i$. However, in order to describe the procedure, we need to recall some notions related to maximal orders first. We will give the refined statement of Theorem 3.1.1 in the next section.

Using Theorem 3.1.1, we obtain the following classification of orders in $M(2, K)$ that are the intersections of maximal orders.

**Theorem 3.1.2.** Let $K$ be a non-Archimedean local field with valuation ring $R$ with respect to the valuation $\nu$. Fix a uniformizer $\pi$ so that $\nu(\pi) = 1$. If an order in $M(2, K)$ is the intersection of finitely many maximal orders in $M(2, K)$, then it is conjugate by an element in $GL(2, K)$ to exactly one of the following orders

\[
\begin{align*}
\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}, \\
\left\{ \begin{pmatrix} a & b \\ \pi^n c & d \end{pmatrix} : a, b, c, d \in R \right\}, \quad n > 0, \\
\left\{ \begin{pmatrix} a & b \\ \pi^k c & a + \pi^\ell d \end{pmatrix} : a, b, c, d \in R \right\}, \quad k \geq 2 \ell > 0,
\end{align*}
\]

corresponding to a maximal order, an Eichler order, and the intersection of three or more maximal orders, respectively.

**Remark 3.1.3.** Note that if $K = \mathbb{Q}_p$ with $R = \mathbb{Z}_p$ and $\pi = p$, then we have

\[
\begin{align*}
SL(2, \mathbb{Z}) \cap \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_p \right\} &= SL(2, \mathbb{Z}), \\
SL(2, \mathbb{Z}) \cap \left\{ \begin{pmatrix} a & b \\ p^n c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_p \right\} &= \Gamma_0(p^n), \\
SL(2, \mathbb{Z}) \cap \left\{ \begin{pmatrix} a & b \\ p^k c & a + p^\ell d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_p \right\} &= \Gamma_0(p^k) \cap \Gamma_1(p^\ell).
\end{align*}
\]

So the three types of orders correspond to the full modular group, congruence subgroups of type $\Gamma_0(N)$, and congruence subgroups of type $\Gamma_0(N) \cap \Gamma_1(M)$ with $M \mid N$, respectively. We expect that the theta series attached to ideals of the orders, which are mentioned before, will have close relations to modular forms in a parallel way. Note that if $k = 2\ell$, then $\Gamma_0(p^{2\ell}) \cap \Gamma_1(p^\ell)$ is conjugate to $\Gamma(p^\ell)$, the principal congruence subgroup of level $p^\ell$. 

34
Remark 3.1.4. In section 2.3, we have discussed that a quaternion algebra over a non-Archimedean local field $K$ is either isomorphic to $M(2, K)$ or the unique division $K$-quaternion algebra. For the unique division algebra, there is exactly one maximal order, which is the associated valuation ring. Therefore, the intersection of maximal orders is just the maximal order itself. This is the reason why we only discuss the case in matrix algebra.

3.1.3 Orders which are non-intersection orders

Originally, the basic problem is to classify all the orders in $M(2, K)$, which is questioned by Professor Hashimoto. Professor Hashimoto also conjectured that the intersection of three maximal orders in $M(2, \mathbb{Q}_p)$ is related to the principal congruence subgroup of $SL(2, \mathbb{Z})$.

Fortunately, we completed a part of the question and verified the conjecture of Professor Hashimoto is true. For the rest part of this basic problem, it still need to be solved. Here are two examples for the existence of orders in $M(2, K)$ that are not the intersection of maximal orders. These examples are given by Professor Yang.

Let $p$ be an odd prime and $\epsilon$ be a quadratic nonresidue modulo $p$. Let

$$\mathcal{O} = \left\{ \gamma \in M(2, \mathbb{Z}_p) : \gamma \equiv \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \mod p \text{ for some } a, b \in \mathbb{Z}_p \right\}.$$  

It is easy to check that $\mathcal{O}$ is an order of index $p^2$ in $M(2, \mathbb{Z}_p)$.

To see why it is not the intersection of maximal orders, we remark that $\mathcal{O}$ has the property that the set

$$\{ \alpha \in \mathcal{O} : \det \alpha \equiv 0 \mod p \}$$

is closed under addition. (In fact, the set is precisely $pM(2, \mathbb{Z}_p)$.) However, from the explicit description of intersection of maximal orders given in Theorem 3.1.2, it is plain that if a suborder of index $p^2$ in $M(2, \mathbb{Z}_p)$ is an intersection of maximal orders, then it does not have this property.

Another example of orders that are not the intersections of maximal orders in $M(2, \mathbb{Z}_p)$ is

$$\left\{ \begin{pmatrix} a & b \\ pc & a + pd \end{pmatrix} : a, b, c, d \in \mathbb{Z}_p \right\}.$$
3.2 Explicit Way to Obtain an Intersection Order

In this section, we recall the tree of maximal orders, which provides a convenient platform for discussion related to maximal orders. For more details, please see Section 2.4 or [56].

Define a graph $X$ of maximal orders as follows. The vertices of $X$ are the maximal orders and two vertices are connected by a simple edge if the two corresponding maximal orders have distance 1. Then the graph $X$ is a $(q+1)$-regular tree.

**Notation 3.2.1.** Let $O_1$ and $O_2$ be two maximal orders in $M(2, K)$. We let $d(O_1, O_2)$ denote the distance between $O_1$ and $O_2$.

**Notation 3.2.2.** If $S$ is a set of maximal orders in $M(2, K)$, then we let

$$d_3(S) = \max_{O_1, O_2, O_3 \in S} (d(O_1, O_2) + d(O_2, O_3) + d(O_3, O_1)).$$

(Note that $O_1, O_2, O_3$ need not be distinct.)

We are now in a position to give a refined version of Theorem 3.1.1.

**Theorem 3.2.3.** Let $K$ be a non-Archimedean local field. Assume that $O_1, \ldots, O_r$ are maximal orders in $M(2, K)$. Let $O_{i_1}, O_{i_2},$ and $O_{i_3}$ be a triplet of maximal orders such that

$$d(O_{i_1}, O_{i_2}) + d(O_{i_2}, O_{i_3}) + d(O_{i_3}, O_{i_1})$$

is equal to the maximum among all $d(O_i, O_j) + d(O_j, O_k) + d(O_k, O_i)$, $1 \leq i, j, k \leq n$. Then

$$\bigcap_{i=1}^{r} O_i = O_{i_1} \cap O_{i_2} \cap O_{i_3}.$$

(Note that the indices $i_1, i_2, i_3$ need not be distinct.)

This gives an algorithm to get three maximal orders to obtain a given intersection order in $M(2, K)$. Moreover, this can be verified immediately from the following lemma.
Lemma 3.2.4. Let \( S = \{ \mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3 \} \) be a set of three maximal orders in \( M(2, K) \). Then for any maximal order \( \mathcal{O}_4 \) such that

\[
d_3(S \cup \{ \mathcal{O}_4 \}) = d_3(S),
\]

we have

\[
\mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3 \subset \mathcal{O}_4.
\]

Proof of Theorem 3.2.3. Let \( S = \{ \mathcal{O}_1, \ldots, \mathcal{O}_r \} \) be a finite set of maximal orders in \( M(2, K) \). Assume that \( \mathcal{O}_{i_1}, \mathcal{O}_{i_2}, \mathcal{O}_{i_3} \in S \) are maximal orders such that

\[
d_3(S) = d(\mathcal{O}_{i_1}, \mathcal{O}_{i_2}) + d(\mathcal{O}_{i_2}, \mathcal{O}_{i_3}) + d(\mathcal{O}_{i_3}, \mathcal{O}_{i_1}).
\]

Then for all \( \mathcal{O} \in S \), we have

\[
d_3(\{ \mathcal{O}_{i_1}, \mathcal{O}_{i_2}, \mathcal{O}_{i_3}, \mathcal{O} \}) = d_3(\{ \mathcal{O}_{i_1}, \mathcal{O}_{i_2}, \mathcal{O}_{i_3} \}).
\]

By the lemma above, this implies that

\[
\mathcal{O}_{i_1} \cap \mathcal{O}_{i_2} \cap \mathcal{O}_{i_3} \subset \mathcal{O}
\]

and consequently,

\[
\bigcap_{\mathcal{O} \in S} \mathcal{O} = \mathcal{O}_{i_1} \cap \mathcal{O}_{i_2} \cap \mathcal{O}_{i_3}.
\]

This proves the theorem. \( \square \)

3.3 Proof of Lemma 3.2.4

Here we make some remarks about the tree of maximal orders. These remarks will be instrumental in our subsequent discussion.

Remark 3.3.1. (1) For each pair of maximal orders \( \mathcal{O}_1 \) and \( \mathcal{O}_2 \), there is one and only one path from \( \mathcal{O}_1 \) to \( \mathcal{O}_2 \), and the intermediate vertices on this path are uniquely determined by the pair \( \mathcal{O}_1 \) and \( \mathcal{O}_2 \).

(2) The group \( \text{PGL}(2, K) \) acts on the set

\[
\mathcal{L}^{(n)} = \{ (\mathcal{O}_1, \mathcal{O}_2) \in X \times X : d(\mathcal{O}_1, \mathcal{O}_2) = n \}
\]

transitively by conjugation.
To continue our discussion on the intersection of maximal orders of $M(2, K)$, let us introduce some definitions.

**Definition 3.3.1.** Let $X$ be a tree. Given a finite number of vertices $v_1, \ldots, v_n$, the smallest finite subtree $C(v_1, \ldots, v_n)$ containing $v_1, \ldots, v_n$ as vertices is called the **convex hull** of $v_1, \ldots, v_n$. Moreover, we say a vertex $v$ of a subtree $Y$ of $X$ is a **branching vertex** of $Y$ if it has at least three neighbors in $Y$, i.e., if there are at least three edges of $Y$ connecting to $v$.

**Proof of Lemma 3.2.4.** Let $X$ be the tree of maximal orders in $M(2, K)$. There are two cases to consider.

1. The convex hull of the vertices $O_1, O_2, O_3$ has no branching vertex. That is, one of the vertices lies on the path between the other two vertices.

2. The convex hull of the vertices $O_1, O_2, O_3$ has one branching vertex $O_0$. That is, the convex hull is of star-shape with $O_0$ being the center of the star.

In Case (1), assume that $O_2$ is on the path connecting the vertices $O_1$ and $O_3$. By a suitable conjugation, we may assume that

$$O_1 = M(2, R), \quad O_3 = \gamma^{-n}O_1\gamma^n, \quad \gamma = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.$$  

Then $O_2 = \gamma^{-m}O_1\gamma^m$ for some integer $m$ satisfying $0 \leq m \leq n$. (See Remark 3.3.1(2).) Thus,

$$O_1 \cap O_2 \cap O_3 = \begin{pmatrix} R & R \\ \pi^nR & R \end{pmatrix} = O_1 \cap O_3,$$

which is an Eichler order. Now the assumption $d_3(S) = d_3(S \cup \{O_4\})$ implies that $O_4$ also lies on the path from $O_1$ to $O_3$. Thus, $O_4 = \gamma^{-k}O_1\gamma^k$ for some integer $k$ with $0 \leq k \leq n$. Then $O_4 = \begin{pmatrix} R & R \\ \pi^kR & R \end{pmatrix}$ and $O_1 \cap O_2 \cap O_3 \subset O_4$.  

We next consider Case (2). Set \( m = d(O_0, O_1) \), \( n = d(O_0, O_2) \), and \( \ell = d(O_0, O_3) \). We suppose that 

\[
m \geq n \geq \ell.
\]

By a suitable conjugation, we may assume that

\[
O_1 = \gamma^{-m} O_0 \gamma^m, \quad O_2 = \gamma^n O_0 \gamma^{-n}, \quad \gamma = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.
\]

Then \( O_0 \) is \( M(2, R) \) and \( O_3 \) must be of the form \( O_3 = \left( \frac{1}{0} \pi \right)^{-1} O_0 \left( \frac{1}{0} \pi \right) \) for some \( c \in \mathbb{R}^* \). To see why it is so, we note that \( O_3 \) cannot equal to the conjugate of \( O_0 \) by a matrix of the form \( \left( \pi^a 0 \ \pi^{-a} \right) \), \( a > 0 \), because the path from \( O_0 \) to such a maximal order must pass through the order \( \gamma^{-a} O_0 \gamma^a \), which is also on the path from \( O_0 \) to \( O_1 \). This contradicts to the assumption that \( O_0 \) is the center in the star-shaped convex hull of \( O_1, O_2, O_3 \). By the same token, \( c \) cannot be in \( \pi R \) because \( c \in \pi R \) implies that the maximal order \( \gamma O_0 \gamma^{-1} \) is on both the path from \( O_0 \) to \( O_3 \) and the path from \( O_0 \) to \( O_2 \), which again is a contradiction.

Now assume that \( O_4 \) is a maximal order such that \( d_3(S \cup \{ O_4 \}) = d_3(S) \). By the property of a tree, there is a unique maximal order \( O' \) on the subgraph through which \( O_4 \) is connected to the convex hull of \( O_1, O_2, O_3 \). We have three sub-cases depending on where \( O' \) lies.

(i) The vertex \( O' \) is on the path from \( O_0 \) to \( O_1 \),

(ii) The vertex \( O' \) is on the path from \( O_0 \) to \( O_2 \),

(iii) else.

In Case (i), the assumption \( d_3(S \cup \{ O_4 \}) = d_3(S) \) immediately implies that

\[
d(O_0, O_4) \leq d(O_0, O_1) = m.
\]
A less obvious consequence of the assumption $d_3(S \cup \{O_4\}) = d_3(S)$ is the inequality

$$d(O', O_4) \leq d(O_0, O_3) = \ell.$$ 

To see why this inequality holds, we observe that if $d(O', O_4) > d(O_0, O_3)$, then setting $u = d(O_0, O')$ and $v = d(O', O_4)$, we have

$$O_2 \quad O_0 \quad u \quad O' \quad m - u \quad O_1
\ell \quad O_3 \quad v \quad O_4$$

and

$$d_3(S \cup \{O_4\}) = d(O_1, O_4) + d(O_4, O_2) + d(O_2, O_1)$$
$$= (m - u + v) + (n + u + v) + (m + n) = 2(m + n + v)$$
$$> 2(m + n + \ell) = d(O_1, O_2) + d(O_2, O_3) + d(O_3, O_1)$$
$$= d_3(S),$$

which is a contradiction.

It follows that $O_4 = (\pi^u \quad d/\pi^u)^{-1} M(2, R) (\pi^u \quad d/\pi^u)$ for some unit $d \in R/(\pi^u)$ and integers $u$ and $v$ satisfying $u > 0$, $v \geq 0$, $u + v \leq m$ and $v \leq \ell$. Now we have

$$O_4 = R \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) + R \left( \begin{array}{cc} 0 & \pi^{v-u} \\ 0 & 0 \end{array} \right) + \pi^{-v} R \left( \begin{array}{cc} -d/\pi^u & -d^2/\pi^u \\ \pi^u & d \end{array} \right) + R \left( \begin{array}{cc} 0 & -d/\pi^u \\ 0 & 1 \end{array} \right).$$

Thus,

$$O_1 \cap O_2 \cap O_3 = R \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) + R \left( \begin{array}{cc} 0 & \pi^n \\ 0 & 0 \end{array} \right) + R \left( \begin{array}{cc} 0 & 0 \\ \pi^m & 0 \end{array} \right) + R \left( \begin{array}{cc} 0 & 0 \\ 0 & \pi^\ell \end{array} \right) \subset O_4.$$

We next consider Case (ii). By a similar argument as above, we find

$$O_4 = \left( \begin{array}{cc} 1 & d\pi^u \\ \pi^u & 0 \end{array} \right)^{-1} M(2, R) \left( \begin{array}{cc} 1 & d\pi^u \\ \pi^u & 0 \end{array} \right)$$
$$= R \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) + R \left( \begin{array}{cc} 0 & \pi^{u+v} \\ 0 & 0 \end{array} \right) + \pi^{-v} R \left( \begin{array}{cc} -d/\pi^{-u} & -d^2/\pi^u \\ \pi^{-u} & d \end{array} \right) + R \left( \begin{array}{cc} 0 & -d\pi^u \\ 0 & 1 \end{array} \right).$$
for some $d \in R/(\pi^v)$ and integers $u$ and $v$ satisfying $u > 0$, $v \geq 0$, $u + v \leq n$ and $v \leq \ell$. It follows that $\mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3 \subset \mathcal{O}_4$.

Finally, the last case implies that $\mathcal{O}_4$ has distance to $\mathcal{O}_0$ less than or equal to $\ell$. That is,

$$
\mathcal{O}_4 = \begin{pmatrix} 1 & t + d\pi^u \\ \pi^{u+v} & 1 \end{pmatrix}^{-1} M(2, R) \begin{pmatrix} 1 & t + d\pi^u \\ \pi^{u+v} & 1 \end{pmatrix}
$$

$$
= R \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + R \begin{pmatrix} 0 & \pi^{u+v} \\ 0 & 0 \end{pmatrix}
$$

$$
+ \pi^{-v-u} R \begin{pmatrix} -t + d\pi^u & -(t + d\pi^u)^2 \\ 1 & t + d\pi^u \end{pmatrix} + R \begin{pmatrix} 0 & -t - d\pi^u \\ 0 & 1 \end{pmatrix},
$$

where $t \in c + (\pi)$, $\nu(t - c) \leq u$, $d \in R/(\pi^v)$ and some nonnegative integers $u$ and $v$ satisfying $u + v \leq \ell$. It is clear that $\mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3 \subset \mathcal{O}_4$. This completes the proof of the lemma.

\[ \square \]

### 3.4 Classification of Orders Arising from Intersection

In this section, we shall prove Theorem 3.1.2, which classifies orders of $M(2, K)$ that are the intersections of maximal orders. We first prove a lemma, which shows that the orders listed in Theorem 3.1.2 are mutually nonisomorphic.

**Lemma 3.4.1.** For $k \geq 2\ell \geq 0$, set

$$
\mathcal{O}_{k,\ell} = \left\{ \begin{pmatrix} a & b \\ \pi^{k\ell}c & a + \pi^{\ell}d \end{pmatrix} : a, b, c, d \in R \right\}.
$$

Then these sets are orders in $M(2, K)$ and mutually nonisomorphic.

**Proof.** It is easy to check that $\mathcal{O}_{k,\ell}$ is an order in $M(2, K)$. We are now required to show that if $(k_1, \ell_1) \neq (k_2, \ell_2)$, then $\mathcal{O}_{k_1,\ell_1}$ is not isomorphic to $\mathcal{O}_{k_2,\ell_2}$. For this purpose, we consider the invariant $h(\mathcal{O})$ of an order $\mathcal{O}$ defined as the smallest nonnegative integer $h$ such that the ring

$$
R[h] = \{ (\alpha, \beta) \in R \oplus R : \alpha \equiv \beta \mod \pi^h \}
$$

41
can be embedded in \( \mathcal{O} \). This integer \( h(\mathcal{O}) \) clearly depends only on isomorphism classes of orders. We shall show that \( h(\mathcal{O}_{k,\ell}) = \ell \), under the condition that \( k \geq 2\ell \).

It is clear that the order \( \mathcal{O}_{k,\ell} \) contains a subring \( R(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) + R(\begin{pmatrix} 0 & \pi^\ell \\ 0 & 0 \end{pmatrix}) \) isomorphic to \( R[\ell] \). Thus, \( h(\mathcal{O}_{k,\ell}) \leq \ell \).

Now assume that \( h \) is a nonnegative integer such that \( h < \ell \). The element \((0, \pi^h)\) in \( R[h] \) has minimal polynomial \( x^2 - \pi^hx \). We will show that the order \( \mathcal{O}_{k,\ell} \) does not contain any element with this minimal polynomial. Then we are done.

Assume that \( \begin{pmatrix} a & b \\ \pi^k c & a + \pi^\ell d \end{pmatrix} \) is an element in \( \mathcal{O}_{k,\ell} \) with characteristic polynomial \( x^2 - \pi^hx \). We have

\[
2a + \pi^\ell d = \pi^h, \quad a^2 + \pi^\ell ad - \pi^k bc = 0. \tag{3.1}
\]

Substituting \( \pi^\ell d = \pi^h - 2a \) from the first equation into the second equation, we get \( a(\pi^h - a) - \pi^kbc = 0 \) and hence \( a(\pi^h - a) \equiv 0 \mod \pi^k \). Because \( h \) is assumed to be less than \( \ell \), we have

\[
v(a) \geq k - h \quad \text{or} \quad \begin{cases} v(a) = h, \\ v(a - \pi^h) \geq k - h. \end{cases}
\]

In view of the first equation of (3.1) and assumption \( k \geq 2\ell > 2h \), the first case \( v(a) \geq k - h \) cannot occur. If the second case \( v(a) = h \) and \( v(a - \pi^h) \geq k - h \) occurs, then we write the first equation of (3.1) as

\[
a + (a - \pi^h) + \pi^\ell d = 0.
\]

Since \( v(a) = h, v(a - \pi^h) = k - h > h, \) and \( \ell > h \), the left-hand side cannot vanish, which is a contradiction. Therefore, we conclude that \( h(\mathcal{O}_{k,\ell}) \) must be at least \( \ell \), and in fact \( h(\mathcal{O}_{k,\ell}) = \ell \). This shows that if \( k_1, k_2, \ell_1, \ell_2 \) are positive integers such that \( \mathcal{O}_{k_1,\ell_1} \) is isomorphic to \( \mathcal{O}_{k_2,\ell_2} \), then \( \ell_1 = \ell_2 \). Considering the indices of \( \mathcal{O}_{k_1,\ell_1} \) and \( \mathcal{O}_{k_2,\ell_2} \) in \( M(2, R) \), we find that \( k_1 \) must also be equal to \( k_2 \).

**Proof of Theorem 3.1.2.** In view of Lemma 3.4.1, it remains to prove that if an order in \( M(2, K) \) is the intersection of finitely many maximal orders, then it is conjugate to one of the orders listed in the statement.
Let $S$ be a finite set of maximal orders in $M(2, K)$. Let $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ be the maximal orders in $S$ with $d_3(S) = d(\mathcal{O}_1, \mathcal{O}_2) + d(\mathcal{O}_2, \mathcal{O}_3) + d(\mathcal{O}_3, \mathcal{O}_1)$ so that

$$\bigcap_{\mathcal{O} \in S} \mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3.$$ 

There are three cases to consider.

(1) $d_3(S) = 0$, i.e., $|S| = 1$.

(2) $d_3(S) > 0$, and the convex hull of the orders $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ is a straight line.

(3) $d_3(S) > 0$, and the convex hull of the orders $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ has a branching vertex $\mathcal{O}_0$.

The first case simply means that $S$ has only one element, and thus the intersection is a maximal order and is conjugate to $M(2, R)$.

Assume that the second case occurs. This is Case (1) in the proof of Lemma 3.2.4, where we find that, up to conjugation, the intersection is $(\pi^n R \pi^n \pi^m R \pi^m)$, for some positive integer $n$.

Now assume that the third case occurs. Set $m = d(\mathcal{O}_1, \mathcal{O}_0), n = d(\mathcal{O}_2, \mathcal{O}_0), \ell = d(\mathcal{O}_3, \mathcal{O}_0)$, and assume that $m \geq n \geq \ell$. By a proper conjugation by a matrix in $GL(2, K)$, we may assume that

$$\mathcal{O}_0 = M(2, R), \quad \mathcal{O}_1 = \gamma^{-m} \mathcal{O}_0 \gamma^m, \quad \mathcal{O}_2 = \gamma^n \mathcal{O}_0 \gamma^{-n}, \quad \gamma = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.$$ 

Then $\mathcal{O}_3$ must be of the form $\mathcal{O}_3 = \begin{pmatrix} 1 & c \\ 0 & \pi^\ell \end{pmatrix}^{-1} \mathcal{O}_0 \begin{pmatrix} 1 & c \\ 0 & \pi^\ell \end{pmatrix}$ for some $c \in R^*$. (See the proof of Lemma 3.2.4 for details.) Then

$$\mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3 = R \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + R \begin{pmatrix} 0 & \pi^n \\ 0 & 0 \end{pmatrix} + R \begin{pmatrix} 0 & 0 \\ \pi^m & 0 \end{pmatrix} + R \begin{pmatrix} 0 & 0 \\ 0 & \pi^\ell \end{pmatrix}.$$ 

Conjugating this order by $\gamma^m$, we find that $\mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathcal{O}_3$ is conjugate to the order

$$\left\{ \begin{pmatrix} a & b \\ \pi^k c & a + \pi^\ell d \end{pmatrix} : a, b, c, d \in R \right\},$$ 

where $k = m + n \geq 2\ell$ because $\ell$ is assumed to be the smallest among $\ell, m,$ and $n$. This completes the classification of orders in $M(2, K)$ that are intersections of maximal orders. \hfill $\square$
Chapter 4

Lattice Packing from Quaternion Algebras

A lattice in the Euclidean space $\mathbb{R}^n$ is a pair $(\Lambda, b)$ of a free $\mathbb{Z}$-module $\Lambda$ of rank $n$, and a positive definite symmetric $\mathbb{Z}$-bilinear form $b$. Lattice packing problem is one of the classical sphere packing problem. In mathematics, the theory of lattice packing is a useful tool for many areas, such as number theory and coding theory.

There are many ways to construct lattices, and one of them is using ideals from certain number fields [5, 6, 7, 9, 10]. We call such lattices ideal lattices.

As the ideal lattices from a number field, we can also construct lattices from the ideals of a definite quaternion algebra over a totally real number field [3, 4, 52, 60, 61, 62, 65]. By a suitable scaled trace construction, the reduced trace of such kind quaternion algebra gives a non-degenerate symmetric bilinear form.

The purpose of this chapter is to use this construction of ideal lattices to construct the densest known lattices in dimension 4, 8, 12, 16, 24, and 32. In particular, they are the root lattices $D_4$, $E_8$, the Coxeter-Todd lattice $K_{12}$, laminated lattice $\Lambda_{16}$, the Leech lattice $\Lambda_{24}$, and a lattice of rank 32 with center density $3^{16}/2^{24}$, which has the best known density in dimension 32.

In the rest part, we first recall lattice packing, ideal lattices from number fields. We will sequentially introduce lattice construction from quaternion algebras, and then establish a determinant formula. Finally, let us look the famous lattices with highest known density from ideal lattices of quaternion algebras.
4.1 Lattice Packing from Number Fields

In this section, we briefly recall the definitions of lattice packing and the ideal lattices, which are related to our work. For the details, please refer to other materials. For lattice packing, one of the references is the book written by Conway and Sloane [17]; for ideal lattice, see for instance the works of Bayer-Fluckiger, Nebe, and Suarez [7, 8, 10, 12, 13, 14].

4.1.1 Lattice packing

A lattice is a pair \((\Lambda, b)\), where \(\Lambda\) is a free \(\mathbb{Z}\)-module of finite rank and \(b : \Lambda \times \Lambda \rightarrow \mathbb{R}\) is a positive definite symmetric \(\mathbb{Z}\)-bilinear form. Suppose that the \(\mathbb{Z}\)-module \(\Lambda\) has a \(\mathbb{Z}\)-basis \(\{v_1, \ldots, v_n\}\). Then the Gram matrix \(M = (M_{ij})\) for the lattice \((\Lambda, b)\) is the \(n \times n\) matrix with entries \(M_{ij} = b(v_i, v_j)\). The packing radius of the lattice is defined to be the value

\[
\rho := \inf\{b(v, v)^{1/2} \mid v \in \Lambda, v \neq 0\}/2.
\]

The center density of the lattice \((\Lambda, b)\) is given by

\[
\delta_\Lambda := \frac{\rho^n}{\sqrt{\det \Lambda}} = \frac{||v||^n}{2^n \sqrt{\det \Lambda}},
\]

where \(v\) is a nonzero vector in \(\Lambda\) with the smallest norm \(||v|| = b(v, v)^{1/2}\), and \(\det \Lambda = \det M\) is called the determinant or discriminant of the lattice \(\Lambda\).

We say that a lattice \((\Lambda, b)\) is even if the norm of each element is even. A lattice \((\Lambda, b)\) is called integral if \(b(x, y)\) is an integer for any \(x, y \in \Lambda\), or equivalently, its Gram matrix has integer entries. In other words, a lattice is integral if and only if it is contained in its dual lattice

\[
\Lambda^* = \{v \in \Lambda \otimes \mathbb{Z} \mathbb{R} : b(v, \Lambda) \subseteq \mathbb{Z}\}.
\]

Moreover, an integral lattice \(\Lambda\) with \(\Lambda = \Lambda^*\) is called unimodular.

Here, we make a table for the densest lattice packings presently known in dimensions \(n = 4, 8, 12, 16, 24, 32\),

<table>
<thead>
<tr>
<th>(n)</th>
<th>Best known (\delta)</th>
<th>Lattice</th>
<th>Bound for (\delta)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1/8</td>
<td>(D_4 \cong \Lambda_4)</td>
<td>0.13127</td>
</tr>
<tr>
<td>8</td>
<td>1/16</td>
<td>(E_8 \cong \Lambda_8)</td>
<td>0.06326</td>
</tr>
<tr>
<td>12</td>
<td>1/27</td>
<td>(K_{12})</td>
<td>0.06559</td>
</tr>
<tr>
<td>16</td>
<td>1/16</td>
<td>(\Lambda_{16})</td>
<td>0.11774</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>(\Lambda_{24})</td>
<td>1.27421</td>
</tr>
<tr>
<td>32</td>
<td>(3^{16}/2^{24})</td>
<td>(Q_{32}, MW_{32}, \text{or, } B_{32})</td>
<td>5.52</td>
</tr>
</tbody>
</table>
where $D_4$, $E_8$ are root lattices, $\Lambda_n$ is the Laminated lattice in dimension $n$ ($\Lambda_{24}$ is the same as the Leech lattice.), $K_{12}$ is the 12-dimensional Coxeter-Todd lattice, $Q_{32}$ denotes the Quebbemann lattice, $MW$ is the Mordell-Weil lattice, and $B_{32}$ is the Bachoc’s lattice. In particular, $D_4$ is proved as the unique lattice structure with this highest known density for a 4-dimensional lattice, and the lattice $E_8$ is the unique lattice in dimension 8 with density $1/8$ and its minimal norm is 2.

### 4.1.2 Ideal lattices

Let $K$ be a totally real number field or a CM field over $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. Let $\sigma : K \to K$ be the identity map if $K$ is a totally real number field, and $\sigma : K \to K$ be the complex conjugation if $K$ is a CM field. Denote $F$ the fixed subfield of $K$ of $\sigma$. Assume that $I$ is a fractional ideal of $K$ and we have a positive definite symmetric bilinear form $b : I \times I \to \mathbb{R}$ satisfying

$$b(ax, y) = b(x, a^\sigma y), \quad \forall x, y \in I, \forall a \in \mathcal{O}_K.$$ 

We call the pair $(I, b)$ an ideal lattice over $K$. Moreover, there exists a totally positive element $\alpha \in F$ so that

$$b(x, y) = b_\alpha(x, y) = \text{Tr}_{K_R}^{K}(\alpha xy^\sigma),$$

where $K_R = K \otimes \mathbb{Q} \mathbb{R}$. In this case, we let the pair $(I, \alpha)$ denote the ideal lattice associated to the bilinear form $b_\alpha$.

From the construction of the ideal lattice, one can easily get the relation

$$\det I = |d_K|N_K(I)^2N_K(\alpha).$$

Bayer-Fluckiger used this to construct the root lattice $E_8$, the Coxeter-Todd lattice $K_{12}$, and the Leech lattice $\Lambda_{24}$ [7], and so on [8, 13]. Besides, she gave a criterion to determine whether a number field of class number one is Euclidean [7], and discussed upper bounds of Euclidean minima of algebraic number fields [11, 12, 14].

### 4.2 Lattices from Quaternion Algebras

In this section, we will discuss lattices from a definite quaternion algebra, and then construct lattices have the highest densities known in their own dimensions 4, 8, 12, 16, 24, and 32.
4.2.1 From quaternion algebra to ideal lattices

Let $B$ be a quaternion algebra over a number field $K$. In the followings, the ring of integers of $K$ and the discriminant of $K$ are denoted by $O_K$ and $d_K$, respectively. Also, the maps $\text{Tr}_K$, $N_K$ mean the trace map and the norm map defined on $K$.

Recall that the reduce trace on a definite quaternion algebra $B$ gives a positive definite bilinear form $\langle x, y \rangle := \text{Tr}(x\bar{y})$ on $B$. Now, if $\alpha$ is a totally positive element in $K$, for a chosen ideal $I$ of a definite $K$-quaternion algebra $B$, we then have a positive definite symmetric $\mathbb{Z}$-bilinear form $b_\alpha : I \times I \rightarrow \mathbb{Q}$ on $I$ given by

$$b_\alpha(x, y) = \text{Tr}_K(\alpha\text{Tr}(x\bar{y})),$$

where $\bar{x}$ is the conjugate of $x$ in $B$. In this case, we let $(I, \alpha)$ denote the lattice associated to $b_\alpha$. For example, the maximal order $O = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}^{1+i+j+i^2}$ in the $\mathbb{Q}$-quaternion algebra $(-1, -1)$, and the number 1 forms a lattice $(O, 1)$ with density $1/8$. In particular, this lattice is isomorphic to $D_4$.

4.2.2 Determinant formula

As the determinant formula in the case of ideal lattice $(I, \alpha)$ from number field, we have a similar result for the lattices obtained by quaternion algebra.

**Proposition 4.2.1.** Let $K$ be a totally real algebraic number field of degree $n$ over $\mathbb{Q}$ with discriminant $d_K$. Let $B$ be a quaternion algebra over $K$ and $O$ be a maximal order of $B$. If $I$ is a right ideal of $O$ and $\alpha$ is a totally positive element in $K$ so that $(I, \alpha)$ is an ideal lattice. Then we have the following identity

$$\det I = N_K(D_B)^2d_K^4N_K(\alpha)N_K(N(I))^4,$$

where $N(I)$ is norm of the ideal $I$, $N_K$ is the norm map defined on $K$ over $\mathbb{Q}$, and $D_B$ is the discriminant of $B$.

**Proof.** First, we need to determine a $\mathbb{Z}$-basis for $\Lambda$. A $\mathbb{Z}$-basis for $I$ is $\beta = \{\beta_i\}$, where $\{\beta_i\}_{1 \leq i \leq n}$ is a $\mathbb{Z}$-basis for $O_K$ and $\{v_j\}_{1 \leq j \leq 4}$ is an $O_K$-basis for $I$. Then the Gram matrix associated to $\Lambda$ with respect to $\beta$ is $M = (A_{ij})$, where $A_{ij} = (a_{tm})$ is an $n$ by $n$ matrix with entries

$$a_{tm} = \text{Tr}_K(\alpha\text{Tr}(\beta_t\bar{v}_i\beta_m\bar{v}_j)).$$
Consequently, one can expand \( a_{\ell m} \) as

\[
a_{\ell m} = \sum_{k=1}^{n} \sigma_k(\beta_\ell) \sigma_k(\alpha \text{Tr}(v_i v_j)) \sigma_k(\beta_m),
\]

where \( \{\sigma_k\} \) are embeddings of \( K \) in \( \mathbb{C} \) which fix \( \mathbb{Q} \) pointwise. Therefore, this Gram matrix is a product of these three matrices

\[
M = \begin{pmatrix}
C & 0 & 0 & 0 \\
0 & C & 0 & 0 \\
0 & 0 & C & 0 \\
0 & 0 & 0 & C
\end{pmatrix}
\begin{pmatrix}
D_{11} & \cdots & \cdots & D_{14} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
D_{41} & \cdots & \cdots & D_{44}
\end{pmatrix}
\begin{pmatrix}
C^t & 0 & 0 & 0 \\
0 & C^t & 0 & 0 \\
0 & 0 & C^t & 0 \\
0 & 0 & 0 & C^t
\end{pmatrix},
\]

where \( C = (\sigma_k(\beta_\ell)) \), \( C^t \) is the transpose of \( C \), and

\[
D_{ij} = \begin{pmatrix}
\sigma_1(\alpha \text{Tr}(v_i v_j)) \\
\vdots \\
\sigma_n(\alpha \text{Tr}(v_i v_j))
\end{pmatrix}
\]

is an \( n \) by \( n \) diagonal matrix. Thus, the determinant of \( M \) is equal to \((\det CC^t)^4 \det D\) with \( D = (D_{ij}) \). In order to consider the determinant of \( D \), we exchange the rows and columns of the matrix \( D \) so that

\[
\det D = \det \begin{pmatrix}
D_1 \\
\vdots \\
D_n
\end{pmatrix}, \quad D_\ell = (\sigma_\ell(\alpha \text{Tr}(v_i v_j)))_{i,j}
\]

\[
= \prod_{\ell=1}^{n} \sigma_\ell(\det(\alpha \text{Tr}(v_i v_j))) = N_K(\alpha)^4 N_K(\det(\text{Tr}(v_i v_j))).
\]

Notice that \( \det CC^t = d_K \) and \( \det(\text{Tr}(v_i v_j)) \) is equal to \( N_K(N(I)^4 \text{disc}(\mathcal{O})^2) \). By the fact that \( \text{disc}(\mathcal{O}) = D_B \), hence we have

\[
\det I = \det M = d_K^4 N_K(\alpha)^4 N_K(N(I))^4 N_K(D_B^2).
\]

This formula provides us some information and conditions for \( I \) and \( \alpha \). In the next subsection, we will introduce how we use it to find the lattice which has the best known center density.
4.2.3 Examples

Notice that if the field $K$ over $\mathbb{Q}$ is of degree $n$ then the lattice has rank $4n$. So, for example, if we wish to find $E_8$ lattice, we must find a real quadratic extension over $\mathbb{Q}$. Here, we construct $E_8$ lattice using the ideal lattice via the quaternion algebra $B = \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})}\right)$.

**Example 4.2.2. The $E_8$ lattice.** Let $I$ be the ideal

$$I = \mathcal{O}_K + \mathcal{O}_K \frac{1 + i}{\sqrt{2}} + \mathcal{O}_K \frac{1 + j}{\sqrt{2}} + \mathcal{O}_K \frac{1 + i + j + ij}{2}$$

of the quaternion algebra $B = \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})}\right)$ and choose $\alpha = \frac{2 + \sqrt{2}}{4}$. Then $(I, \alpha)$ forms a lattice with a free $\mathbb{Z}$-basis

$$\left\{ 1, \sqrt{2}, \frac{1 + i}{\sqrt{2}}, \frac{1 + j}{\sqrt{2}}, 1 + i, 1 + j, \frac{1 + i + j + ij}{2}, \frac{1 + i + j + ij}{\sqrt{2}} \right\}.$$

Observe that the norm of the elements $1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+ij}{2}$ are integers, and the trace of $\frac{2+\sqrt{2}}{4}$ is $1$. Hence, the value of $b(x, x) = 2\text{Tr}_K(\alpha N(x))$ is even for any $x \in I$. It is known that an even definite unimodular lattice having rank 8 is isomorphic to $E_8$ lattice. Therefore, the lattice $(I, \frac{2+\sqrt{2}}{4})$ is isomorphic to $E_8$ and its center density is $1/16$.

The following constructions are concerned with totally real subfields of cyclotomic fields. Here, we let $\zeta_m$ denote a primitive $m$th root of unity, $\eta_m = \zeta_m + \zeta_m^{-1}$, for $m > 1$, and $\mathbb{Q}(\zeta_m)^+$ the maximal real subfield of $\mathbb{Q}(\zeta_m)$. We also use Magma to find ideal lattices.

**Example 4.2.3. The Coxeter-Todd lattice $K_{12}$.** In order to find a lattice isomorphic to $K_{12}$, we choose a quaternion algebra over the totally real field $\mathbb{Q}(\zeta_7)^+$, which has three real infinity places and $d_K = 49$. According to the determinant formula and the center density for $K_{12}$, we have

$$\frac{1}{36} = \delta^2 = \frac{(\text{minimal norm}^2)^{12}}{2^{24} \cdot 7^8 \cdot N_K(\alpha)^4 N_K(N(I))^4 N_K(\text{disc}(\mathcal{O}))^2)}.$$

Since the square of the minimal norm is a rational number, comparing the RHS and LHS, we shall choose the quaternion algebra to be $\left(\frac{-1,-3}{K}\right)$, which...
is ramified at all of 3 real infinity places and the finite place 3. Hence, we have the equality

\[
\frac{1}{3^6} = \frac{\text{(minimal norm)}^2}{2^{24} \cdot 7^8 \cdot 3^6 \cdot N_K(\alpha)^4 N_K(N(I))}\]

This gives us the condition for \((I, \alpha)\). Finally, we find that we can choose \(I\) to be

\[
I = \mathcal{O}_K \langle \eta^2 - \eta - 2, (\eta^2 - \eta - 2)i, \frac{-3 + 4i + j}{2}, \frac{4 + 3i + k}{2} \rangle
\]

with \(N_K(N(I)) = 7\), \(\eta = \eta_7\), and \(\alpha = 1/7\). Essentially, the ideal \(I\) is a right unimodular \(\mathbb{Z}[\frac{1+k}{2}]\)-lattice of rank 6 and the theta series associated to \(I\) is

\[
\theta_I(\tau) = 1 + 756q^2 + 4032q^3 + 20412q^4 + \cdots, \quad q = e^{2\pi i \tau}.
\]

According to the results in [16], we conclude that the Coxeter-Todd lattice \(K_{12}\) can be realized as the ideal lattice \((I, 1/7)\).

**Example 4.2.4. The \(\Lambda_{16}\) lattice.** Let \(K\) be the totally real subfield of \(\mathbb{Q}(\zeta_{17})\) of degree 4 over \(\mathbb{Q}\) and the quaternion algebra is \(B = \left(\frac{-1,-1}{K}\right)\). Set \(K = \mathbb{Q}(\omega)\), where the minimal polynomial of \(\omega\) is \(x^4 + x^3 - 6x^2 - x + 1\). A \(\mathbb{Z}\)-basis for \(\mathcal{O}_K\) is \(\{1, \omega, \omega^2, \frac{1+\omega}{2}\}\). The ideal we chosen is

\[
I = \mathcal{O}_K \langle 1+\omega, (1+\omega)j, \frac{\omega^3 + 4 + i}{2}, \frac{(3\omega^3 - 42\omega + 78) - 17i + (3\omega^3 + 6)j + k}{6} \rangle
\]

with \(N_K(N(I)) = 4\); the totally positive element we picked is \(\alpha = 3 + \omega - \frac{1+\omega}{2}\) with minimal polynomial \(x^4 - 17x^3 + 68x^2 - 85x + 17\). Then the minimal norm of this ideal lattice \((I, \alpha/17)\) is 4, and the lattice is a 2-elementary totally even lattice. Hence, we can conclude that it is just the \(\Lambda_{16}\)-lattice from [53, 55].

**Example 4.2.5. The Leech lattice \(\Lambda_{24}\).** Here, we let \(K = \mathbb{Q}(\zeta_{13})^+\), \(B = \left(\frac{-1,-1}{K}\right)\), and \(I\) be the ideal of \(B\) with the free \(\mathcal{O}_K\)-basis

\[
\eta^2 - \eta - 2, \quad (\eta^2 - \eta - 2)i, \quad \frac{(\eta^4 + \eta^3 + 2) + (\eta^4 + \eta^3 + 7)i + j}{2}, \quad \frac{(\eta^4 + \eta^3 + 7) + (\eta^4 + \eta^3 + 2)i + k}{2},
\]

\[50\]
with $N_K(N(I)) = 13$. We find that the ideal lattice $(I, 1/13)$ is an even unimodular lattice and has no vector with norm 2. Up to isomorphism, the Leech lattice is the unique even, unimodular definite lattice of rank 24 and has no vectors with norm 2. That is, the lattice $(I, 1/13)$ is the Leech lattice.

**Example 4.2.6.** For a rank 32 lattice. We choose the quaternion algebra $B = \left( \frac{-1,-1}{K} \right)$ with $K = \mathbb{Q}(\zeta_{17})^+$, and $I$ the $\mathcal{O}_K$-module generated by

$$(2\eta^5 - 8\eta^3 + 2\eta^2 + 6\eta - 4),$$
$$(\eta^5 - 4\eta^3 + \eta^2 + 3\eta - 2)(1 + i),$$
$$\left(\eta^6 + \eta^4 - 32\eta^3 + 64\eta^2 + 74\eta - 7\right) + (\eta^6 + \eta^4 + 2\eta^3 - 4\eta^2 + 6\eta + 27)i + j,$$
$$\frac{2}{3\eta^6 + 3\eta^4 + 23\eta^3 + 56\eta^2 - 50\eta + 64}$$
$$+ \frac{2}{(3\eta^6 + 3\eta^4 + 57\eta^3 - 12\eta^2 + 18\eta + 98)i + 3j + k},$$

with $N_K(N(I)) = 4096$, and $\alpha$ be an element with minimal polynomial

$$x^8 - 68x^7 + 1190x^6 - 5202x^5 + 7871x^4 - 5406x^3 + 1819x^2 - 289x + 17.$$

Then the lattice $(I, \alpha)$ has the highest known center density in dimension 32.
Chapter 5

Defining Equation of Modular Curves $X_0(2^{2n})$

In this chapter, we will present defining equation of modular curves $X_0(2^{2n})$. The key ingredient is a recursive formula for certain generators of the field of modular functions on $\Gamma_0(2^{2n})$. The contents are mainly followed by the joint work with Professor Yang [64].

5.1 Introduction

For a congruence subgroup $\Gamma$ of $\text{SL}(2, \mathbb{R})$ commensurable with $\text{SL}(2, \mathbb{Z})$, the modular curve $X(\Gamma)$ has a complex structure as a compact Riemann surface, and the polynomials defining the Riemann surface are called defining equations of $X(\Gamma)$. The problem of explicitly determining the equations of modular curves has been addressed by several authors. For instance, Galbraith [29], Murabayashi [44], and Shimura [59] used the so-called canonical embeddings to find equations of $X_0(N)$ that are non-hyperelliptic. For hyperelliptic $X_0(N)$, we have results of Galbraith [29], González [30], Hibino [35], Hibino-Murabayashi [36], and Shimura [59]. In [54] Reichert used the fact that $X_1(N) = X(\Gamma_1(N))$ is the moduli space of isomorphism classes of elliptic curves with level $N$ structure to compute equations of $X_1(N)$ for $N = 11, 13, \ldots, 18$. Furthermore, in [41] Ishida and Ishii proved that for each $N$ two certain products of the Weierstrass $\sigma$-functions generate the function field on $X_1(N)$, and thus the relation between these two functions defines $X_1(N)$. A similar method was employed in [40] to obtain equations...
of $X(N) = X(\Gamma(N))$. Yang [67, 68] also devised a new method for obtaining defining equations of $X_0(N)$, $X_1(N)$, and $X(N)$, in which the required modular functions are constructed using the generalized Dedekind eta functions.

When $\Gamma_1$ and $\Gamma_2$ are two congruence subgroups such that $\Gamma_2$ is contained in $\Gamma_1$ and a defining equation of $X(\Gamma_1)$ is known, one may attempt to deduce an equation for $X(\Gamma_2)$ using the natural covering $X(\Gamma_2) \to X(\Gamma_1)$. Of course, the main difficulty in this approach lies at finding an explicit description of the covering map. Our key point is to figure out descriptions of the maps $X_0(2^{(n+1)}) \to X_0(2^n)$ recursively.

In the following, we will first recall some information of modular curve $X_0(2^n)$, and construct certain modular forms on $X_0(2^2n)$. Finally, we will prove a recursive formula for the coverings $X_0(2^{(n+1)}) \to X_0(2^n)$, from which we easily obtain defining equations of $X_0(2^n)$ for positive integers $n$.

### 5.2 Modular Curve $X_0(2^n)$

The modular curve $X_0(N)$ is the quotient space of $\mathfrak{H}^*$ by the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) : a = 1 \mod N \right\}.$$

In this section, we first give the genus formula of $X_0(2^n)$, explicit non-equivalent cusps of $\Gamma_0(2^n)$, and then we construct modular function satisfying certain conditions with respect to the curve $X_0(2^n)$.

#### 5.2.1 Signature of $X_0(2^n)$

Here we recall the index of the subgroup $\Gamma_0(N)$ in $\text{SL}(2, \mathbb{Z})$, the standard representatives of inequivalent elliptic points, and the standard representatives of inequivalent cusps on $\Gamma_0(N)$.

For a fixed positive integer $N$, the index of $\Gamma_0(N)$ is equal to

$$N \prod_{p|N} (1 + 1/p).$$

A set of inequivalent cusps for $\Gamma_0(N)$ is given by

$$\left\{ \frac{a}{c} : c \mid N, \ a = 0, \ldots, \gcd(c, N/c) - 1, \ \gcd(a, c) = 1 \right\},$$

53
and hence the number of inequivalent cusps is
\[
\sum_{c \mid N} \phi(gcd(c, N/c)),
\]
where \(\phi\) is the Euler totient function. Moreover, the width of the cusp \(a/c\) on \(\Gamma_0(N)\) is
\[
N \frac{gcd(c, N/c)}{c}, \quad \text{where } gcd(a, c) = 1, \text{ and } c \mid N.
\]
The number of inequivalent elliptic points of order 2 is given by
\[
v_2 = \begin{cases} 
0, & \text{if } 4 \mid N, \\
\prod_{p \mid N, p > 2} \left(1 + \left(\frac{-1}{p}\right)\right), & \text{if } 4 \nmid N;
\end{cases}
\]
the number \(v_3\) of inequivalent elliptic points of order 3 is equal to
\[
v_3 = \begin{cases} 
0, & \text{if } 9 \mid N, \\
\prod_{p \mid N} \left(1 + \left(\frac{-3}{p}\right)\right), & \text{if } 9 \nmid N,
\end{cases}
\]
where \(\left(\frac{\cdot}{p}\right)\) is the Jacobi symbol.

Therefore, in the case of \(X_0(2^n)\), we can easily find that the cusps on \(\Gamma_0(2^n)\) and their widths are
\[
\{a/2^k \mid k = 0, \ldots, n, \ 0 \leq a \leq s - 1, \ gcd(2^k, a) = 1\},
\]
and
\[
h_{n,k} = \begin{cases} 
1, & \text{if } n < 2k \\
2^{n-2k}, & \text{if } n \geq 2k,
\end{cases}
\]
respectively, where
\[
s = \begin{cases} 
2^k, & \text{if } 1 \leq k \leq \lfloor n/2 \rfloor \\
2^{n-k}, & \text{if } \lfloor n/2 \rfloor < k < n.
\end{cases}
\]
According to Proposition 2.8.2, as a conclusion, the genus of the curve \(X_0(2^n)\) is
\[
g = 1 + 2^{n-3} - \begin{cases} 
2^{(n-1)/2}, & \text{if } n \equiv 1 \mod 2, \\
3 \cdot 2^{n/2 - 2}, & \text{if } n \equiv 0 \mod 2.
\end{cases}
\]
54
5.2.2 Modular functions on $\Gamma_0(2^n)$

By the criteria of Newman [45], a product
\[
\prod_{k=0}^{n} \eta(2^k \tau)^{e_k}
\]
of Dedekind eta functions is a modular function on $\Gamma_0(2^n)$ if the conditions

1. $\sum_k e_k = 0$,
2. $\sum_k ke_k \equiv 0 \pmod{2}$,
3. $\sum_k e_k 2^k \equiv \sum_k e_k 2^{n-k} \equiv 0 \pmod{24}$,

are satisfied.

Our goal is finding modular functions, which have poles only at infinity and are holomorphic at other cusps, with respect to $\Gamma_0(2^n)$. Using transformation law of Dedekind $\eta$-functions (Proposition 2.10.1), one can verify that the order of an eta function $\eta(2^m \tau)$ with $0 \leq m \leq n$ at the cusp $a/2^k$ is

\[
2^t h_{n,k}/24, \quad \text{where} \quad t = \begin{cases} m, & \text{if } k \geq m, \\ 2k - m, & \text{if } m > k. \end{cases}
\]

Therefore, to find modular functions is equivalently deduced to solve an integer programming problem.

Let us look an example for the case of $\Gamma_0(64)$. The cusps of $\Gamma_0(64)$ are

\[
\{0, \infty, 1/2, 1/4, 3/4, 1/8, 3/8, 5/8, 7/8, 1/16, 3/16, 1/32\}
\]

and the orders of the $\eta$-functions at each cusp multiple by 24 are as follows.

<table>
<thead>
<tr>
<th>$\times 24$</th>
<th>$\eta(\tau)$</th>
<th>$\eta(2\tau)$</th>
<th>$\eta(4\tau)$</th>
<th>$\eta(8\tau)$</th>
<th>$\eta(16\tau)$</th>
<th>$\eta(32\tau)$</th>
<th>$\eta(64\tau)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>64</td>
<td>32</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1/2</td>
<td>16</td>
<td>32</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$a/4$</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$a/8$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$a/16$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>1/32</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>$\infty$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>64</td>
</tr>
</tbody>
</table>
Therefore, to find a modular function \( \prod_{m=0}^{6} \eta(2^m \tau)^{x_0} \) with only pole at \( \infty \) of order \( k \) on \( \Gamma_0(64) \), is replaced by solving the integer programming problem

\[
\begin{align*}
64x_0 &+ 32x_1 + 16x_2 + 8x_3 + 4x_4 + 2x_5 + x_6 \geq 0, \\
16x_0 &+ 32x_1 + 16x_2 + 8x_3 + 4x_4 + 2x_5 + x_6 \geq 0, \\
4x_0 &+ 8x_1 + 16x_2 + 8x_3 + 4x_4 + 2x_5 + x_6 \geq 0, \\
x_0 &+ 2x_1 + 4x_2 + 8x_3 + 4x_4 + 2x_5 + x_6 \geq 0, \\
x_0 &+ 2x_1 + 4x_2 + 8x_3 + 16x_4 + 8x_5 + 4x_6 \geq 0, \\
x_0 &+ 2x_1 + 4x_2 + 8x_3 + 16x_4 + 32x_5 + 16x_6 \geq 0, \\
x_0 &+ 2x_1 + 4x_2 + 8x_3 + 16x_4 + 32x_5 + 64x_6 = -24k,
\end{align*}
\]

\[ \sum_{m=0}^{6} x_m = 0, \text{ and } \sum_{m=0}^{6} mx_m \equiv 0 \mod 2. \]

Using the tool `lp_solve`, we find that for \( k = 3 \), \((x_0, x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, 0, -2, 6, 4)\) is a solution. Thus, on \( \Gamma_0(64) \),

\[
\frac{\eta(32\tau)^6}{\eta(16\tau)^2\eta(64\tau)^4}
\]

is a modular function having poles only at \( \infty \) of order 3. For \( k = 4 \), we have a solution \((x_0, x_1, x_2, x_3, x_4, x_5, x_6) = (0, 0, 0, -1, 2, 1, -2)\) and thus

\[
\frac{\eta(16\tau)^2\eta(32\tau)}{\eta(8\tau)\eta(64\tau)^2}
\]

is modular on \( \Gamma_0(64) \) and has poles at \( \infty \) of order 4.

### 5.3 Defining Equations and the Fermat Curves

#### 5.3.1 Main result

In order to state our result for defining equations of \( X_0(2^{2n}) \), I would to recall the definition of the Jacobi theta functions

\[
\theta_2(\tau) = \sum_{n \in \mathbb{Z}} q^{(2n+1)^2}/8 = \frac{2\eta(2\tau)^2}{\eta(\tau)},
\]
\[ \theta_3(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2/2} = \frac{\eta(\tau)^5}{\eta(\tau/2)^2 \eta(2\tau)^2}, \]

and

\[ \theta_4(\tau) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2/2} = \frac{\eta(\tau/2)^2}{\eta(\tau)}, \]

where \( q = e^{2\pi i \tau}, \tau \in \mathbb{H}. \)

The main result is stated as follows.

**Theorem 5.3.1.** Let \( P_0(x, y) = y^4 - x^3 - 4x, \) and for \( n \geq 7 \) define polynomials \( P_n(x, y) \) recursively by

\[ P_n(x, y) = P_{n-1} \left( \frac{\sqrt{x^2 + 4}}{\sqrt{x}}, \frac{y}{\sqrt{x}} \right) P_{n-1} \left( -\frac{\sqrt{x^2 + 4}}{\sqrt{x}}, \frac{y}{\sqrt{x}} \right) x^{2n-5}. \]

Then \( P_{2n}(x, y) = 0 \) is a defining equation of the modular curve \( X_0(2^{2n}) \) for \( n \geq 3. \)

To be more precise, for \( n \geq 1, \) let

\[ x_n = \frac{2\theta_3(2^{n-1}\tau)}{\theta_2(2^{n-1}\tau)}, \quad y_n = \frac{\theta_2(8\tau)}{\theta_2(2^{n-1}\tau)}. \]

Then,

1. for \( n \geq 2, \) we have \( x_{n-1} = \sqrt{(x_n^2 + 4)/x_n} \) and \( y_{n-1} = y_n/\sqrt{x_n}; \)
2. for \( n \geq 6, \) \( P_n(x_n, y_n) = 0, \) and \( P_n(x, y) \) is irreducible over \( \mathbb{C}; \)
3. when \( n \) is an even integer greater than 4, \( x_n \) and \( y_n \) are modular functions on \( \Gamma_0(2^n) \) that are holomorphic everywhere except for a pole of order \( 2^{n-4} \) and \( 2^{n-4} - 1, \) respectively, at \( \infty. \) (Thus, they generate the field of modular functions on \( \Gamma_0(2^n) \) and the relation \( P_n(x_n, y_n) = 0 \) between them is a defining equation for \( X_0(2^n). \))

**Remark 5.3.2.** Using geometric arguments, Elkies [27] showed that the curve \( X_0(\ell^n) \) can be embedded in \( X_0(\ell^2)^{n-1}. \) When \( \ell = 2, \) the curve \( X_0(2^n) \) is of genus zero and thus possesses a Hauptmodul \( \xi(\tau). \) Then the embedding is explicitly given as

\[ \tau \mapsto (\xi(\tau), \xi(2\tau), \ldots, \xi(2^{n-2}\tau)), \]
and the equations of $X_0(2^n)$ are defined in terms of the relations between $\xi(2^{i-1}\tau)$ and $\xi(2^i\tau)$.

Elkies’ equations and ours are both recursive in nature. Note that, however, Elkies’ method is a generalization of the classical modular equations where a defining equation for $X_0(N)$ is given in terms of $j(\tau)$ and $j(N\tau)$, while our method emphasizes on explicit construction of generators of the field of modular functions. Moreover, since our starting point is the genus 3 modular curve $X_0(64)$, our equations are more comparable to Elkies’ equations for $X_0(6^n)$, where the starting point is the genus 1 modular curve $X_0(36)$.

We remark that it can be easily shown by induction that $P_n(x,y)$ is contained in $\mathbb{Z}[x,y]$ for $n \geq 7$ and has a degree $2^{n-4} - 1$ in $x$ and a degree $2^{n-4}$ in $y$. We also remark that when $n$ is odd, the polynomial $P_n(x,y)$ fails to be a defining equation of $X_0(2^n)$ because in this case

$$y_n(\tau) = \frac{\eta(16\tau)^2\eta(2^{n-1}\tau)}{\eta(2\tau)\eta(2^n\tau)^2}$$

is not modular on $\Gamma_0(2^n)$. In fact, one can show that when $n$ is odd,

$$y_n\left(\frac{a\tau + b}{c\tau + d}\right) = \left(\frac{2}{d}\right) y_n(\tau), \quad \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \Gamma_0(2^n),$$

where $\left(\frac{\cdot}{d}\right)$ is the Jacobi symbol.

**Example 5.3.3.** (1) For the modular curve $X_0(64)$,

$$x_6 = \frac{2\theta_3(4\tau)}{\theta(4\tau)} = q^{-4} + 2q^{12} - q^{28} - 2q^{44} + 3q^{60} + \cdots,$$

and

$$y_6 = \frac{\theta_2(8\tau)}{\theta_2(4\tau)} = q^{-3} + q^5 + q^{21} - q^{29} - q^{37} + \cdots,$$

are modular functions on $\Gamma(64)$, where $q = e^{2\pi i\tau}$ is a local parameter at $\infty$. By observation of the behaviors of $x_6$ and $y_6$, we have the relation between $x_6$ and $y_6$,

$$x_6^3 - y_6^4 + 4x_6 = 0$$

and hence obtain a defining equation of the modular curve $X_0(64)$. 58
According to Theorem 5.3.1, we find that a defining equation of $X_0(256)$ is
\[ y^{16} - 16x(x + 2)^4(x^2 + 4)y^8 - x(x + 2)^4(x - 2)^8(x^2 + 4) = 0, \]
and an equation for $X_0(1024)$ is
\[ y^{64} - 2^{12}uvy^{56} - 2^8 \cdot 241uvy^{48} - 2^9uv(11 \cdot 23u + 2^8 \cdot 7 \cdot 17v)y^{40} \\
- 2^4uv(31 \cdot 149u^2 - 2^8 \cdot 2053uv + 2^6 \cdot 7 \cdot 73v^2)y^{32} \\
- 2^9uv(31u^3 + 2^7 \cdot 3^2 \cdot 31u^2v + 3 \cdot 2^7uv^2 + 2^{23}v^3)y^{24} \\
- 2^5u^3v(47u^2 - 2^9 \cdot 5^4uv + 2^{15} \cdot 17 \cdot 31v^2)y^{16} \\
- 2^6u^3v(u^3 + 2^7 \cdot 41u^2v + 2^{18} \cdot 5uv^2 + 2^{26}v^3)y^8 - u^7v = 0, \]
where $u = (x - 2)^8$ and $v = x(x + 2)^4(x^2 + 4)$.

5.3.2 The modular curve $X_0(2^{2n}+2)$ and the Fermat curve $x^{2^n} + y^{2^n} = 1$

Our interest in the modular curves $X_0(2^{2n})$ stems from the following remarkable observation of Hashimoto. When $n = 3$, it is known that the curve $X_0(64)$ is non-hyperelliptic (see [47]) of genus 3. Then the theory of Riemann surfaces says that it can be realized as a plane quartic. Indeed, it can be shown that the space of cusp forms of weight 2 on $\Gamma_0(64)$ is spanned by
\[ x = \eta(4\tau)^2\eta(8\tau)^2, \quad y = 2\eta(8\tau)^2\eta(16\tau)^2, \quad z = \frac{\eta(8\tau)^8}{\eta(4\tau)^2\eta(16\tau)^2}, \]
and the map $X_0(64) \to \mathbb{P}^2(\mathbb{C})$ defined by $\tau \mapsto [x(\tau) : y(\tau) : z(\tau)]$ is an embedding. Then the relation
\[ x^4 + y^4 = z^4 \]
among $x$, $y$, $z$ is a defining equation of $X_0(64)$ in $\mathbb{P}^2$. In Theorem 5.3.1, the curve defined by $y^4 - x^3 - 4x = 0$ is birationally equivalent to the Fermat curve $X^4 + Y^4 = 1$ via the map
\[ X = \frac{x - 2}{x + 2}, \quad Y = \frac{2y}{x + 2}. \]
Then Professor Hashimoto pointed out the curious fact that the Fermat curve
\[ F_{2^n} : x^{2^n} + y^{2^n} = 1 \]
and the modular curve \( X_0(2^{2n+2}) \) have the same genus \( \frac{(2^n-1)(2^n-2)}{2} \) for all positive integers \( n \). In fact, there are more similarities between these two families of curves. For instance, the obvious covering \( F_{2^{n+1}} \to F_{2^n} \) given by \([x : y : z] \to [x^2 : y^2 : z^2]\) branches at \( 3 \cdot 2^n \) points, each of which is of order 2. On the other hand, the congruence subgroup \( \Gamma_0(2^{2n+2}) \) is conjugate to \( \Gamma_0(2^n+1) \) by an element (can choose \( \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix} \)) in \( \text{GL}(2, \mathbb{R}) \), and the natural covering \( X_0'(2^{2n+2}) \to X_0'(2^{2n+1}) \) also branches at \( 3 \cdot 2^n \) cusps of \( X_0'(2^{2n+1}) \). These observations naturally lead us to consider the problem whether the modular curve \( X_0(2^{2n+2}) \) is birationally equivalent the Fermat curve \( F_{2^n} \). It turns out that this problem can be answered easily as follows.

According to [26, 42, 46], when a modular curve \( X_0(N) \) has genus \( \geq 2 \), any automorphism of \( X_0(N) \) will arise from the normalizer of \( \Gamma_0(N) \) in \( \text{SL}(2, \mathbb{Z}) \), with \( N = 37, 63 \) being the only exceptions. Now by [2, Theorem 8], for all \( n \geq 7 \), the index of \( \Gamma_0(2^n) \) in its normalizer in \( \text{SL}(2, \mathbb{R}) \) is 128. Therefore, the automorphism group of \( X_0(2^{2n+2}) \) has order 128 for all \( n \geq 3 \). On the other hand, it is clear that the automorphism group of any Fermat curve contains \( S_3 \). Thus, we conclude that the modular curve \( X_0(2^{2n+2}) \) cannot be birationally equivalent to the Fermat curve \( F_{2^n} \) when \( n \geq 3 \). Still, it would be an interesting problem to study the exact relation between these two families of curves.

### 5.4 Proof of Theorem 5.3.1

To prove \( x_{n-1} = \sqrt{(x_n^2 + 4)/x_n} \), we first verify the case \( n = 2 \) by comparing the Fourier expansions for enough terms, and then the general case follows since \( x_n(\tau) \) is actually equal to \( x_1(2^{n-1} \tau) \). The proof of \( y_{n-1} = y_n/\sqrt{x_n} \) is equally simple. We have

\[
\frac{y_{n-1}^2}{y_n^2} = \frac{\eta(2^{n-1} \tau)^2}{\eta(2^{n-2} \tau)^2} = \frac{\eta(2^{n-2} \tau)^2 \eta(2^n \tau)^4}{\eta(2^{n-1} \tau)^6} = \frac{\theta_2(2^{n-1} \tau)}{2 \theta_3(2^n \tau)} = \frac{1}{x_n}.
\]
This proves the recursion part of the theorem. We now show that when \( n \geq 6 \) is an even integer, \( x_n \) and \( y_n \) are modular functions on \( \Gamma_0(2^n) \) that have a pole of order \( 2^{n-4} \) and \( 2^{n-4} - 1 \), respectively, at \( \infty \) and are holomorphic everywhere.

It is clear that when \( n \) is an even integer greater than 2, the conditions of the criterion of Newman are all satisfied for the functions

\[
x_n = \frac{\eta(2^{n-1} \tau)^6}{\eta(2^{n-2} \tau)^2 \eta(2^{n-1} \tau)^4} \quad \text{and} \quad y_n = \frac{\eta(16 \tau)^2 \eta(2^{n-1} \tau)}{\eta(8 \tau) \eta(2^{n-1} \tau)^2}.
\]

We now show that \( x_n \) and \( y_n \) have poles only at \( \infty \) of the claimed order.

Still assume that \( n \geq 4 \) is an even integer. Since \( x_n \) and \( y_n \) are \( \eta \)-products, they have no poles nor zeros in \( \mathcal{H} \). Also, it can be checked directly that \( x_n \) and \( y_n \) have a pole of order \( 2^{n-4} \) and \( 2^{n-4} - 1 \), respectively, at \( \infty \). It remains to consider other cusps. For an odd integer \( a \) and \( k \in \{0, 1, \ldots, n - 1\} \), choosing a matrix \( \sigma = \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \) in \( \text{SL}(2, \mathbb{Z}) \), a local parameter at \( a/2^k \) is

\[
e^{2\pi i \sigma^{-1} \tau / h_{n,k}}.
\]

Therefore, the order of a function \( f(\tau) \) at \( a/2^k \) is the same as the order of \( f(\sigma \tau) \) at \( \infty \), multiplied by \( h_{n,k} \).

Now recall that, for \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \), we have

\[
\theta_2(\tau)|\alpha = \begin{cases} 
\epsilon q^{1/8} + \cdots, & \text{if } 2 | c, \\
\epsilon + \cdots, & \text{if } 2 \nmid c,
\end{cases}
\]

and

\[
\theta_3(\tau)|\alpha = \begin{cases} 
\epsilon + \cdots, & \text{if } 2 | ac, \\
\epsilon q^{1/8} + \cdots, & \text{if } 2 \nmid ac,
\end{cases}
\]

where \( \epsilon \) represents a nonzero complex number, but may not be the same at each occurrence. (Up to multipliers, if \( \alpha \) is congruent to the identity matrix or \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) modulo 2, then the action of \( \alpha \) fixes \( \theta_2 \). Any other matrices will send \( \theta_2 \) to either \( \theta_3 \) or \( \theta_4 \). This explains the fact about \( \theta_2 \). The fact about \( \theta_3 \) can be explained similarly.) When \( k = n - 1 \), we have

\[
2^{n-1} \begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix} \tau = \frac{a(2^{n-1} \tau) + 2^{n-1}b}{(2^{n-1} \tau) + d} = \begin{pmatrix} a & 2^{n-1}b \\ 1 & d \end{pmatrix} (2^{n-1} \tau)
\]

61
and
\[
8 \begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix} \tau = \frac{a(8\tau) + 8b}{2^{n-1}(8\tau) + d} = \begin{pmatrix} a & 8b \\ 2^{n-1} & d \end{pmatrix} (8\tau).
\]

It follows that
\[
x_n \begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix} \tau = \frac{\epsilon_2 q^{n-4} + \cdots}{\epsilon_2 + \cdots} = \epsilon q^{n-4} + \cdots,
\]
and
\[
y_n \begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix} \tau = \frac{\epsilon_1 q + \cdots}{\epsilon_2 + \cdots} = \epsilon q + \cdots,
\]
where \(\epsilon, \epsilon_1, \) and \(\epsilon_2\) are nonzero complex numbers. That is, \(x_n\) and \(y_n\) have a zero of order \(2^{n-4}\) and 1, respectively, at \(a/2^{n-1}\).

When \(k = 4, \ldots, n-2\), we have
\[
2^{n-1} \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \begin{pmatrix} 2^{n-k}a & -1 \\ 1 & 0 \end{pmatrix} (2^{2k-1} \tau + 2^{k-1}d),
\]

and
\[
8 \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \frac{a(8\tau) + 8b}{2^{k-3}(8\tau) + d} = \begin{pmatrix} a & 8b \\ 2^k & d \end{pmatrix} (8\tau).
\]

Therefore,
\[
x_n \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \frac{\epsilon_1 + \cdots}{\epsilon_2 + \cdots} = \epsilon + \cdots,
\]
and
\[
y_n \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \frac{\epsilon_1 q + \cdots}{\epsilon_2 + \cdots} = \epsilon q + \cdots,
\]
where \(\epsilon, \epsilon_1, \) and \(\epsilon_2\) are nonzero complex numbers. In other words, \(x_n\) has no poles nor zeros at \(a/2^k\) for \(k = 4, \ldots, n-2\), while \(y_n\) has zeros of order \(h_{n,k}\) at those points.

When \(k = 0, \ldots, 3\), we have
\[
2^{n-1} \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \begin{pmatrix} 2^{n-k}a & -1 \\ 1 & 0 \end{pmatrix} (2^{2k-1} \tau + 2^{k-1}d),
\]

and
\[
8 \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix} \tau = \begin{pmatrix} 2^{3-k}a & -1 \\ 1 & 0 \end{pmatrix} (2^{2k-3} \tau + 2^{k-3}d),
\]
and we find that \(x_n\) and \(y_n\) have no zeros nor poles at \(a/2^k\), \(k = 0, \ldots, 3\).
In summary, we have shown that $x_n$ and $y_n$ have a pole of order $2^{n-4}$ and $2^{n-4} - 1$, respectively, at $\infty$ and are holomorphic at any other points. Since $2^{n-4}$ and $2^{n-4} - 1$ are clearly relatively prime, $x_n$ and $y_n$ generate the field of modular functions on $X_0(2^n)$. It remains to show that $P_n$ is irreducible over $\mathbb{Q}$ and $P_n(x_n, y_n) = 0$.

When $n = 6$, we verify by a direct computation that $y_6^4 - x_6^3 - 4x_6 = 0$. Then the recursive formulas for $x_n$ and $y_n$ implies that $P_n(x_n, y_n) = 0$ for all $n \geq 6$. Finally, by the theory of algebraic curve (see [28, p.194]), the field of modular functions on $X_0(2^n)$ is an extension field of $\mathbb{C}(x_n)$ of degree $2^{n-4}$. In other words, the minimal polynomial of $y_n$ over $\mathbb{C}(x_n)$ has degree $2^{n-4}$. Now it is easy to see that $P_n(x, y)$ is a polynomial of degree $2^{n-4}$ in $y$ with leading coefficient 1. We therefore conclude that $P_n$ is irreducible. This completes the proof of Theorem 1.
Bibliography


List of Papers by Fang-Ting Tu


