

McGILL UNIVERSITY

DOCTORAL THESIS

**Intersections of closed geodesics
on Shimura curves**

Author:

James RICKARDS

Supervisor:

Henri DARMON

Department of Mathematics and Statistics,
McGill University, Montreal

January 13, 2021

*A thesis submitted to McGill University in partial fulfillment of the
requirements of the degree of Doctor of Philosophy.*

© James Rickards 2020

Abstract

Let Γ be a discrete subgroup of $\mathrm{PSL}(2, \mathbb{R})$, and consider closed geodesics on $\Gamma \backslash \mathbb{H}$. In this thesis, we study how these geodesics intersect when Γ is the group of units of norm 1 in an Eichler order of an indefinite quaternion algebra over \mathbb{Q} , i.e. over a Shimura curve. We start by developing some theory for a general Γ , providing a pathway to interpret the geometry of the situation (intersection point, angle, etc.) in terms of the algebra of Γ . The next focus is on $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$, where we relate the work to Conway's topograph, as well as work by Duke, Imamoglu, and Tóth on the linking number of modular knots. We then detail some background on quaternion algebras, before diving in to the Shimura curve case. We reinterpret intersection numbers in terms of x -linking of optimal embeddings of real quadratic orders, and produce formulas which count the total amount of x -linking in a given Eichler order. These formulas are essentially a real quadratic analogue to classical results of Gross and Zagier. We define Hecke operators acting on optimal embeddings, and using the signed intersection pairing, produce formal q -series, which are proven to be weight two modular forms on $\Gamma_0(N)$. The thesis is concluded with a conjectural relation to work of Darmon and Vonk on a real quadratic analogue to the difference of j -values, a brief description of the practical algorithms used to compute with intersection numbers, and a short survey of future projects.

Abrégé

Soit Γ un sous-groupe discret de $\mathrm{PSL}(2, \mathbb{R})$, et considérons les géodésiques fermées sur $\Gamma \backslash \mathbb{H}$. Dans cette thèse, nous étudions comment ces géodésiques s'intersectent lorsque Γ est le groupe des unités de norme 1 dans un ordre d'Eichler d'une algèbre de quaternions indéfinie sur \mathbb{Q} , c'est-à-dire sur une courbe de Shimura. Nous commençons par développer la théorie pour un groupe Γ général, fournissant un moyen d'interpréter la géométrie de la situation (points d'intersection, angle, etc.) en termes de l'algèbre de Γ . L'accent est ensuite mis sur $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$, où nous relierons notre travail au topographe de Conway, ainsi qu'aux travaux de Duke, Imamoglu et Tóth sur le nombre de liaison de nœuds modulaires. Nous détaillons ensuite quelques informations sur les algèbres de quaternions, avant de nous plonger dans le cas des courbes de Shimura. Nous réinterprétons les nombres d'intersections en termes de x -liaisons de plongements optimaux d'ordres quadratiques réels, et produisons des formules qui comptent le nombre total de x -liaison dans un ordre d'Eichler donné. Ces formules sont essentiellement un analogue quadratique réel des résultats classiques de Gross et Zagier. Nous définissons des opérateurs de Hecke agissant sur des plongements optimaux, et en utilisant l'appariement d'intersection signé, nous produisons des séries de puissance formelles, que nous prouvons sont des formes modulaires de poids deux sur $\Gamma_0(N)$. La thèse se termine par une relation conjecturale avec les travaux de Darmon et Vonk sur un analogue quadratique réel de la différence de valeurs de la fonction j , une brève description des algorithmes pratiques utilisés pour calculer les nombres d'intersections, et un bref aperçu de futurs projets.

Acknowledgments

I will start off by thanking my parents, for having always supported my mathematics hobby. In elementary school I found that I enjoyed math, so they supplied me with books and online courses, and I was off to the races. During middle school, my teacher Ms. Susan Gavett (now Mrs. King) introduced me to math contests through Mathcounts, and my school (Clinton Central School) held a “math contest awards dinner” every year. Encouraging excellence at a young age has undoubtedly influenced many of their students, including me.

During high school, Professors Barry Jessup and Pieter Hofstra of the University of Ottawa took time out of their days to mentor me, and they were exceptional at introducing me to university mathematics. On the contest side, I developed my proof writing skills primarily due to Professor Ed Barbeau of the University of Toronto. He ran “Olymon”, a program where students sent in solutions to problems, and he would provide feedback on the writeups. A one person army, he did an incredible job introducing proof writing skills to many students. This interaction also led to my first research discovery, first LaTeX writeup, and first published paper, none of which would have happened without his guidance.

The support provided by Trinity College and the University of Cambridge during my undergraduate degree is unparalleled. The high quality of students, two on one supervisions, and the interactions I had with my Directors of Study, Professors David Tong and Imre Leader, provided a great atmosphere to study mathematics. Without support from the Blyth Cambridge Commonwealth Scholarship, I would not have been able to study at Cambridge, so I am very thankful to have been a recipient of the scholarship.

Coming to the present day, I would like to thank my advisor, Prof. Henri Darmon for having me look at the paper that blossomed into my thesis project, as well as countless helpful conversations about the directions that I could take my research. His view of the “bigger

picture” at work has given me many ideas, all of which have been spot-on. I have greatly enjoyed collaborating with Dr. Jan Vonk, who introduced me to the Conway topograph, and to whom I sent a 600 page document of intersection numbers to compare with his own calculations. Montreal has been a great place to study number theory, with a multitude of professors, students, courses, and seminars. I would be remiss in not also mentioning David Lilienfeldt, with whom I have undoubtedly had the most conversations with in the last four years, by virtue of sharing an office and an advisor!

Finally, I am very fortunate to have been financially supported for my entire time at McGill. During my first two years I held a Schulich Graduate Fellowship, and my last two years were supported by an NSERC Vanier Scholarship.

Contents

| | |
|--|------------|
| Abstract | i |
| Abrégé | ii |
| Acknowledgments | iii |
| 1 Introduction | 2 |
| 2 Closed geodesics and intersection numbers | 5 |
| 2.1 Roots of hyperbolic matrices | 5 |
| 2.2 Closed geodesics | 6 |
| 2.3 The intersection number | 8 |
| 2.4 Alternate interpretations of the intersection number | 9 |
| 2.5 Intersection point and angle | 12 |
| 3 Intersection numbers for $\mathrm{PSL}(2, \mathbb{Z})$ | 16 |
| 3.1 Binary quadratic forms | 16 |
| 3.2 Intersection numbers of binary quadratic forms | 18 |
| 3.3 Intersection numbers as linking numbers | 21 |
| 3.4 Conway's topograph | 23 |
| 3.4.1 The action of $\mathrm{PSL}(2, \mathbb{Z})$ on an infinite 3-regular graph | 23 |
| 3.4.2 Definition of the topograph | 24 |
| 3.4.3 Key properties of the topograph | 26 |
| 3.4.4 The topograph of indefinite forms | 27 |

| | | |
|----------|---|-----------|
| 3.4.5 | Intersection numbers in terms of the topograph | 30 |
| 3.5 | Continued fractions and explicit computation of the intersection number . . | 34 |
| 3.6 | Examples | 37 |
| 3.7 | Filling in the trefoil knot | 39 |
| 4 | Quaternionic background | 40 |
| 4.1 | Local and global quaternion algebras | 40 |
| 4.2 | Normalizer of an Eichler order | 43 |
| 4.3 | Towers of Eichler orders | 46 |
| 4.4 | Optimal embeddings | 47 |
| 4.4.1 | Existence of optimal embeddings | 49 |
| 4.4.2 | Orientations of optimal embeddings | 52 |
| 4.5 | Action of the narrow class group on optimal embeddings | 58 |
| 4.5.1 | Determining the quadratic form | 61 |
| 4.5.2 | Narrow class group action | 64 |
| 5 | Intersection numbers for Shimura curves | 69 |
| 5.1 | Basic facts on intersections | 69 |
| 5.2 | Intersection weights | 74 |
| 6 | Existence of x-linking | 76 |
| 6.1 | Simultaneous conjugation | 77 |
| 6.2 | Orders containing pairs of optimal embeddings | 79 |
| 6.3 | Local x-linking | 82 |
| 6.4 | Global x-linking | 85 |
| 6.5 | Local Eichler orders containing x-linked pairs | 86 |
| 6.6 | Local x-linking with level | 91 |
| 7 | Counting intersection numbers | 97 |
| 7.1 | Total x-linking count into a given Eichler order | 97 |
| 7.2 | Orientations and sign of intersection | 101 |
| 7.3 | Specializing to pairs of embeddings and summing over x | 105 |

| | | |
|-----------|---|------------|
| 7.4 | Examples | 106 |
| 8 | Hecke operators and modularity | 113 |
| 8.1 | Naïve Hecke operators | 114 |
| 8.2 | Good Hecke operators | 116 |
| 8.3 | Atkin-Lehner and general Hecke operators | 118 |
| 8.4 | Discriminants of conjugated embeddings | 120 |
| 8.5 | Prime power Hecke graph | 125 |
| 8.6 | Properties of Hecke operators | 130 |
| 8.7 | Quaternionic modular forms | 134 |
| 8.8 | Weight 2 classical modular forms | 136 |
| 8.9 | Proof of modularity | 138 |
| 8.10 | Examples | 141 |
| 9 | Connection to a real quadratic analogue of the j-function | 146 |
| 10 | Algorithms | 150 |
| 10.1 | Solving the representation problem for binary quadratic forms | 150 |
| 10.2 | Computing optimal embeddings | 151 |
| 10.3 | Computing the intersection number | 153 |
| 10.3.1 | Intersection numbers via intersecting root geodesics | 154 |
| 10.3.2 | Intersection numbers via x-linking | 156 |
| 10.3.3 | Intersection numbers via fundamental domains | 157 |
| 10.3.4 | Running times | 159 |
| 11 | Future research | 161 |
| 11.1 | A more general topograph | 161 |
| 11.2 | More modularity | 162 |
| 11.3 | Distribution questions | 162 |
| 11.3.1 | Distribution of intersection points and angles | 162 |
| 11.3.2 | Distribution of the total intersection number | 164 |
| 11.4 | Towards explicit class field theory for real quadratic fields | 166 |

| | |
|---|------------|
| A Extra proofs | 170 |
| A.1 Pell's equation over p-adics | 170 |
| A.2 Proofs for the prime 2 | 174 |
| A.3 Hermite normal form calculation | 180 |
| References | 186 |
| Index | 189 |

Chapter 1

Introduction

Let Γ be a Fuchsian group, i.e. a discrete subgroup of $\mathrm{PSL}(2, \mathbb{R})$. The action of Γ on the upper half plane \mathbb{H} turns the quotient space $\Gamma \backslash \mathbb{H}$ into a Riemann surface, which links the arithmetic world with the geometric world. Closed geodesics of $\Gamma \backslash \mathbb{H}$ arise from hyperbolic conjugacy classes in Γ , and are a classical object of study (for example, their distribution in the case of $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$ is studied in [Duk88]). In this thesis, we will examine how pairs of these closed geodesics intersect, with the main focus being when $\Gamma \backslash \mathbb{H}$ is a Shimura curve.

In Chapter 2, we introduce the foundations for studying intersection numbers of closed geodesics. We produce general results that transfer the geometry of closed geodesics of $\Gamma \backslash \mathbb{H}$ into the algebra of Γ .

Chapter 3 concerns the case of $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$. These intersection numbers directly correspond to linking numbers of modular knots in the space $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathrm{SL}(2, \mathbb{R})$, as studied by Duke, Imamoglu, and Tóth in [DIT17]. Using the connection between indefinite binary quadratic forms and hyperbolic matrices, we rephrase our results in terms of indefinite binary quadratic forms. By finding an interpretation of the intersection number in terms of Conway's topograph, we produce an efficient algorithm to compute the intersection number.

In Chapter 4, we introduce the quaternionic background required to study intersection numbers for Shimura curves. The geometry of closed geodesics is replaced by the algebra of optimal embeddings, and we describe the structure of the embeddings. Optimal embeddings have been studied before (for example, see [Voi21]), but we go more in depth with regards to explicitly describing orientations of optimal embeddings and the action of the class group.

Chapter 5 is where we apply the results of Chapter 2 to the language of Shimura curves, setting the stage for the rest of the thesis. Theorem 5.1.4 is the key theorem that allows us to switch between hyperbolic geometry and algebra.

Chapter 6 studies x -linking, which is intrinsically related to intersecting geodesics, via the aforementioned Theorem 5.1.4. Instead of focusing on one Eichler order, we fix a pair of embeddings and consider the set of Eichler orders which they embed optimally into. By using the local-global principle, we are able to characterize this setup and count the Eichler orders. The main theorem of this section is Theorem 6.6.5, which gives the count.

In Chapter 7, we invert backwards to focusing on one Eichler order. Given a pair of positive discriminants D_1, D_2 and an Eichler order O , in Theorem 7.1.2 we compute how many x -linked optimal embeddings of discriminants D_1, D_2 into O exist. We also consider how they divide amongst orientations, and briefly consider how they distribute across the equivalence classes of optimal embeddings. The formulae in Theorem 7.1.2 are a real quadratic analogue of a result of Gross and Zagier relating to the factorization of the differences of singular moduli (Proposition 6.1 of [GZ85]). We finish the chapter with explicit examples, demonstrating the results.

Chapter 8 defines Hecke operators on optimal embeddings, and the corresponding intersection power series. We study in detail how the Hecke operator acts, by considering the weights and discriminants of the resulting forms. The resulting prime power Hecke graphs in Section provide a very nice visual component to the study. Next, we show that the Hecke operators respect passing from optimal embeddings to root geodesics to quaternionic modular forms (via Eichler-Shimura). Using Jacquet-Langlands, we can pass to weight two cuspforms on $\Gamma_0(N)$, and thus prove in Theorem 8.0.4 that the series we constructed are in fact classical modular forms. We provide several explicit examples as illustration.

Chapter 9 introduces the work of Darmon and Vonk ([DV20]) on a real quadratic analogue to the difference of j -values. We make a conjectural connection between their work and p -weighted intersection numbers for Shimura curves. The motivation for the connection is the work of Gross and Zagier, where the factorization of $j(\tau_1) - j(\tau_2)$ can be interpreted as a quaternionic intersection involving the quaternion algebra ramified at p, ∞ . In the setup of Darmon and Vonk, there are now two primes p, q , so the analogue would be intersections in

the (indefinite) quaternion algebra ramified at p, q . We give a numerical example as evidence (for more examples, see [DV20]).

Chapter 10 covers some algorithms used in the computation and study of intersection numbers. In particular, we have three distinct ways to compute the intersection number, and we compare the efficiency of the three methods.

Chapter 11 covers some future projects relating to this thesis that I plan to undertake. One of the projects is a conjectural approach to remove the cohomology from the work of Darmon and Vonk described in Chapter 9.

Finally, the appendix contains several proofs which do not fit well into the main text. We detail explicit conditions for a general Pell's equation to have a solution over \mathbb{Z}_p , and give proofs of a number of results for $p = 2$ (the corresponding proofs for p odd are found in the main text).

Chapter 2

Closed geodesics and intersection numbers

Let $\overline{\mathbb{H}} := \mathbb{H} \cup \mathbb{R} \cup i\infty$ be the upper half plane with its boundary. For $z_1, z_2 \in \overline{\mathbb{H}}$, the oriented hyperbolic geodesic segment connecting z_1, z_2 is either a vertical line segment between z_1 and z_2 , or the segment between z_1 and z_2 of the unique circle with centre on the real line which passes through z_1 and z_2 . Denote this segment by ℓ_{z_1, z_2} , where we do not include the endpoints z_1, z_2 . The orientation comes from labeling the start point of the geodesic to be z_1 , and the end point to be z_2 . We are implicitly taking all geodesics to be oriented. Define $\dot{\ell}_{z_1, z_2}$ to mean $\ell_{z_1, z_2} \cup \{z_1\}$, and $\ddot{\ell}_{z_1, z_2}$ to mean $\ell_{z_1, z_2} \cup \{z_1, z_2\}$.

Recall that Möbius maps act on \mathbb{H} and $\overline{\mathbb{H}}$, and they take geodesic segments to geodesic segments. In particular, if $\gamma \in \text{SL}(2, \mathbb{Z})$ and $z_1, z_2 \in \overline{\mathbb{H}}$, then we have

$$\gamma(\ell_{z_1, z_2}) = \ell_{\gamma z_1, \gamma z_2}.$$

When working explicitly with hyperbolic matrices in $\text{PSL}(2, \mathbb{R})$, we need to lift them to $\text{SL}(2, \mathbb{R})$. By convention, we will always take the lift with positive trace.

2.1 Roots of hyperbolic matrices

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}(2, \mathbb{R})$ be a hyperbolic matrix, so that the equation $\gamma(x) = x$ has two distinct real solutions called roots. We label one root to be the first (attracting) root γ_f , and

the other to be the second (repelling) root γ_s , via the equations

$$\lim_{n \rightarrow \infty} \gamma^n(x) := \gamma_f, \quad \lim_{n \rightarrow \infty} \gamma^{-n}(x) := \gamma_s,$$

for any $x \in \mathbb{P}^1(\mathbb{R})$ that is not a root of γ . In particular, γ^{-1} has the same roots as γ , but with the first and second roots swapped. We can algebraically express the first root as

$$\gamma_f = \begin{cases} \frac{a - d + \sqrt{(a + d)^2 - 4}}{2c}, & \text{if } c \neq 0; \\ \infty, & \text{if } c = 0 \text{ and } a > 1; \\ \frac{b}{d - a}, & \text{if } c = 0 \text{ and } a < 1. \end{cases}$$

If $\sigma \in \text{PSL}(2, \mathbb{R})$, then $\sigma\gamma\sigma^{-1}$ has roots $\sigma(\gamma_f), \sigma(\gamma_s)$. It follows from the definition that the “firstness” of γ_f is preserved, i.e.

$$(\sigma\gamma\sigma^{-1})_f = \sigma(\gamma_f), \quad (\sigma\gamma\sigma^{-1})_s = \sigma(\gamma_s).$$

As we will typically be working with conjugacy classes of elements, we write $\gamma_1 \sim \gamma_2$ if γ_1, γ_2 are Γ -conjugate. Write $[\gamma_1]$ for the conjugacy class of γ_1 .

2.2 Closed geodesics

Define a closed geodesic of $\Gamma \backslash \mathbb{H}$ to be a closed path that lifts to a geodesic in \mathbb{H} . The geodesic is said to be prime if it traces out its image exactly once. To construct closed prime geodesics, start with a primitive hyperbolic element $\gamma \in \Gamma$ (so that $\gamma \neq \sigma^n$ for any $\sigma \in \Gamma, n \geq 2$). Define the *root geodesic* of γ to be the upper half plane oriented geodesic running from γ_s to γ_f , i.e.

$$l_\gamma := l_{\gamma_s, \gamma_f}.$$

In particular, the root geodesic of γ^{-1} coincides with the root geodesic for γ , but is run in reverse.

Since γ fixes γ_s, γ_f , γ fixes the geodesic l_γ . For any $x \in l_\gamma$, the geodesic $\dot{l}_{x, \gamma x}$ will thus descend to a closed geodesic in $\Gamma \backslash \mathbb{H}$, which is prime since γ is primitive. Define this closed geodesic to be \tilde{l}_γ ; the image of l_γ runs over \tilde{l}_γ continuously. Furthermore, note that \tilde{l}_γ is constant across the Γ -conjugacy class of γ . If l_1, l_2 are root geodesics, we write $l_1 \sim l_2$ if $l_1 = \sigma(l_2)$ for some $\sigma \in \Gamma$, and we call them similar geodesics.

Proposition 2.2.1. *The map $\gamma \rightarrow \tilde{\ell}_\gamma$ gives a bijection between prime closed geodesics on $\Gamma \backslash \mathbb{H}$ and primitive hyperbolic conjugacy classes of Γ .*

Proof. We already have the map from primitive hyperbolic conjugacy classes to prime closed geodesics via taking $\gamma \rightarrow \tilde{\ell}_\gamma$ for any γ in the conjugacy class. To go the other way, start with a prime geodesic ℓ and lift it to $\dot{\ell}_{x,y}$ for some $x, y \in \mathbb{H}$. Let the full extension of this geodesic in \mathbb{H} be $\ell_{x',y'}$, where $x', y' \in \mathbb{P}_1(\mathbb{R})$. As we started with a closed geodesic, we necessarily have $y = \gamma x$ for some $\gamma \in \Gamma$. Furthermore, if we lift ℓ to start at γx , it will lift $\ell_{\gamma x, \gamma^2 x}$, which is also on $\ell_{x',y'}$. In particular, γ fixes the geodesic $\ell_{x',y'}$ and does not change the orientation, whence x', y' are the second and first roots of γ respectively. This implies that γ is a hyperbolic element of Γ . If γ were not primitive, then $\gamma = \sigma^n$, and ℓ would trace out the path $\tilde{\ell}_\sigma$ n times, and would not be prime.

It is a straightforward check that maps are inverse to each other, and the bijection follows. □

The curve $\tilde{\ell}_\gamma$ can have self-intersection points, hence it is important to consider a point on $\tilde{\ell}_\gamma$ as lying on the curve, and not just in $\Gamma \backslash \mathbb{H}$.

Since we will be studying intersections of geodesics, it is important to take into account the orientations of the geodesics at intersections. To this aim, we define the sign of an intersection (which is not completely canonical, as one could negate the definition).

Definition 2.2.2. Let $y_1, y_2, z_1, z_2 \in \mathbb{P}_1(\mathbb{R})$ be such that $\ell_1 = \ell_{y_1, y_2}$ and $\ell_2 = \ell_{z_1, z_2}$ are geodesics that intersect transversely in the upper half plane. Travel along ℓ_1 from y_1 to y_2 , and consider which side z_1 lies on. If it is on the right hand side of ℓ_1 , then the sign of the *ordered* intersection of ℓ_1, ℓ_2 , denoted $\text{sg}(\ell_1, \ell_2)$, is $+1$. Otherwise, the sign is -1 .

It is important to check that this definition of sign has well-founded properties. To this end, we have the following proposition.

Proposition 2.2.3. *Let ℓ_1, ℓ_2 be geodesics that intersect in a unique point in the upper half plane, and let ℓ_1^{-1} denote the geodesic ℓ_1 run backwards. Then*

$$\text{sg}(\ell_1, \ell_2) = -\text{sg}(\ell_2, \ell_1) = -\text{sg}(\ell_1^{-1}, \ell_2),$$

i.e. swapping the order of the inputs or traveling along one of the geodesics backwards negates the sign. Furthermore, if $\gamma \in \text{PSL}(2, \mathbb{R})$, then

$$\text{sg}(\ell_1, \ell_2) = \text{sg}(\gamma\ell_1, \gamma\ell_2).$$

Proof. The first result is immediate from the definition of the sign. It suffices to check the second half for the matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for $x \in \mathbb{R}$, as these matrices generate $\text{PSL}(2, \mathbb{R})$. This is straightforward. \square

2.3 The intersection number

For $\gamma_1, \gamma_2 \in \Gamma$ primitive and hyperbolic, the geodesics $\tilde{\ell}_{\gamma_1}$ and $\tilde{\ell}_{\gamma_2}$ either intersect in finitely many places, or completely overlap. Furthermore, they completely overlap if and only if γ_1 is Γ -conjugate to either γ_2 or γ_2^{-1} .

Definition 2.3.1. The pair $\gamma_1, \gamma_2 \in \Gamma$ is called a *strongly inequivalent* pair if γ_1 is not conjugate to either γ_2 or γ_2^{-1} in Γ . This concept extends to pairs of Γ -conjugacy classes of matrices.

To get rid of issues when γ_1, γ_2 are not strongly inequivalent, we refer to *transversal* intersections.

Definition 2.3.2. Given primitive hyperbolic matrices $\gamma_1, \gamma_2 \in \Gamma$, denote

$$\tilde{\ell}_{\gamma_1} \pitchfork \tilde{\ell}_{\gamma_2}$$

to be the (finite) set of transversal intersections of $\tilde{\ell}_{\gamma_1}$ and $\tilde{\ell}_{\gamma_2}$.

Let f be any function defined on transversal intersections. The weighted intersection number of γ_1, γ_2 is defined to be

$$\text{Int}_{\Gamma}^f(\gamma_1, \gamma_2) := \sum_{z \in \tilde{\ell}_{\gamma_1} \pitchfork \tilde{\ell}_{\gamma_2}} f(z).$$

In practice, the subscript Γ will normally be dropped, as it is typically fixed and clear from context.

The most natural choices of f are $f = 1$, the *unweighted intersection number*, and f equals the sign of the intersection (as defined in Definition 2.2.2), the *signed intersection number*. These choices are denoted by $\text{Int}(\gamma_1, \gamma_2)$ and $\text{Int}^\pm(\gamma_1, \gamma_2)$ respectively. The advantage of the signed intersection number is it is now well defined in homology of the surface (see Section 0.4 of [GH78] for a more general discussion of the signed intersection number), whereas the unsigned intersection number depends on the actual geodesics. However, when the genus of $\Gamma \backslash \mathbb{H}$ is 0, this implies that the signed intersection number is always zero! In the case of Shimura curves, we will define a third weight function, the q -weighted intersection number for any prime q (see below Definition 5.2.2). In Chapter 11, we will briefly explore other weight functions.

Remark 2.3.3. To formalize Definition 2.3.2, let $\phi_1(t)$ and $\phi_2(t)$ for $t \in [0, 1]$ parametrize the geodesics $\tilde{\ell}_{\gamma_1}$ and $\tilde{\ell}_{\gamma_2}$, respectively. Then

$$\tilde{\ell}_{\gamma_1} \pitchfork \tilde{\ell}_{\gamma_2} = \{(t_1, t_2) \in [0, 1]^2 : \phi_1(t_1) = \phi_2(t_2) \text{ and } \phi_1'(t_1), \phi_2'(t_2) \text{ are linearly independent.}\}.$$

In particular, if γ_1, γ_2 are not strongly inequivalent and $\tilde{\ell}_{\gamma_1}$ passes n times through a point on $\Gamma \backslash \mathbb{H}$, then this contributes $n(n-1)$ transversal intersections. Similarly, if γ_1, γ_2 are strongly inequivalent, then a point on $\Gamma \backslash \mathbb{H}$ passed through m times by $\tilde{\ell}_{\gamma_1}$ and n times by $\tilde{\ell}_{\gamma_2}$ contributes mn transversal intersections.

2.4 Alternate interpretations of the intersection number

When working with intersection numbers, lifting from the quotient space $\Gamma \backslash \mathbb{H}$ to \mathbb{H} makes matters more tractable. Let γ_1, γ_2 be primitive hyperbolic matrices, pick any $z \in \ell_{\gamma_2}$, and the curve $\tilde{\ell}_{\gamma_2}$ lifts uniquely and bijects with $\dot{\ell}_{z, \gamma_2(z)}$. Lifting each transversal intersection $\tilde{P} \in \tilde{\ell}_{\gamma_1} \pitchfork \tilde{\ell}_{\gamma_2}$ to $\dot{\ell}_{z, \gamma_2(z)}$ produces a unique point $P \in \ell_\gamma \pitchfork \dot{\ell}_{z, \gamma_2(z)}$, where ℓ_γ is formed by lifting $\tilde{\ell}_{\gamma_1}$ locally around \tilde{P} to P and extending this so the endpoints lie on $\mathbb{P}_1(\mathbb{R})$. We necessarily have $\gamma \in \Gamma$ and γ is Γ -conjugate to γ_1 .

Given a pair (P, γ) satisfying these properties, it will correspond to a transverse intersection $\tilde{P} \in \Gamma \backslash \mathbb{H}$, and this correspondence is a bijection. Therefore, we can rewrite the formula

for the intersection number.

Proposition 2.4.1. *Let γ_1, γ_2 be primitive hyperbolic matrices and $z \in \ell_{\gamma_2}$. Then*

$$\text{Int}_{\Gamma}^f(\gamma_1, \gamma_2) = \sum_{\substack{\gamma \sim \gamma_1 \\ |\ell_{\gamma} \cap \ell_{z, \gamma_2 z}|=1}} f(\gamma, \gamma_2).$$

Let $\Gamma_i := \gamma_i^{\mathbb{Z}}$ be the automorph group of ℓ_{γ_i} inside Γ for $i = 1, 2$. Instead of the condition that γ is conjugate to γ_1 , we could set $\gamma = \sigma\gamma_1\sigma^{-1}$ for a unique $\sigma \in \Gamma/\Gamma_1$. Similarly, the intersection point lying on $\dot{\ell}_{z, \gamma_2 z}$ can be lifted to ℓ_{γ_2} by passing to the double coset $\sigma \in \Gamma_2 \backslash \Gamma / \Gamma_1$. This gives us the next interpretation.

Proposition 2.4.2 (Double coset interpretation). *Let $\gamma_1, \gamma_2 \in \Gamma$ be primitive hyperbolic matrices. Then*

$$\text{Int}_{\Gamma}^f(\gamma_1, \gamma_2) = \sum_{\substack{\tilde{\sigma} \in \Gamma_2 \backslash \Gamma / \Gamma_1 \\ |\ell_{\sigma\gamma_1\sigma^{-1}} \cap \ell_{\gamma_2}|=1}} f(\sigma\gamma_1\sigma^{-1}, \gamma_2),$$

where σ is any lift of $\tilde{\sigma} \in \Gamma_2 \backslash \Gamma / \Gamma_1$ to Γ .

A way to rephrase the above proposition is we are looking for intersecting root geodesics of conjugates of γ_1, γ_2 modulo the automorphs. A cleaner interpretation is the following proposition.

Proposition 2.4.3. *Define an equivalence relation on pairs (σ_1, σ_2) of primitive hyperbolic matrices in Γ by simultaneous conjugation, i.e.*

$$(\sigma_1, \sigma_2) \sim (\alpha\sigma_1\alpha^{-1}, \alpha\sigma_2\alpha^{-1}),$$

for all $\alpha \in \Gamma$. Let f be a function defined on pairs of primitive hyperbolic matrices that is constant across a simultaneous equivalence class. Then

$$\text{Int}_{\Gamma}^f(\gamma_1, \gamma_2) = \sum_{\substack{(\sigma_1, \sigma_2) \in ([\gamma_1] \times [\gamma_2]) / \sim \\ |\ell_{\sigma_1} \cap \ell_{\sigma_2}|=1}} f(\sigma_1, \sigma_2).$$

The interpretation found in Proposition 2.4.3 will be the most useful theoretical interpretation for us. We now record one final interpretation, which is used in Section 10.3.1 to produce an algorithm to compute intersection numbers.

Proposition 2.4.4. *Let $\gamma_1, \gamma_2 \in \Gamma$ be primitive hyperbolic matrices, and let $r \in \mathbb{P}_1(\mathbb{R}) - \{\gamma_{2,f}, \gamma_{2,s}\}$. Let*

$$S = \{\sigma \in \Gamma : \sigma \sim \gamma_1, |\ell_\sigma \cap \ell_{\gamma_2}| = |\dot{\ell}_\sigma \cap \dot{\ell}_{r, \gamma_2 r}| = 1\},$$

so that S is the set of conjugates of γ_1 whose closed root geodesic intersects both ℓ_{γ_2} and $\dot{\ell}_{r, \gamma_2 r}$. Then

$$\text{Int}_\Gamma^f(\gamma_1, \gamma_2) = \sum_{\sigma \in S} f(\sigma, \gamma_2).$$

Proof. The root geodesic ℓ_{γ_2} divides $\mathbb{P}_1(\mathbb{R})$ into two regions, and the set $\{\gamma_2^n r : n \in \mathbb{Z}\}$ will lie entirely in one region. Furthermore, in thinking of $\mathbb{P}_1(\mathbb{R})$ as a circle, this set will be ordered properly (i.e. if $n_1 < n_2 < n_3$, then $\gamma_2^{n_1} r, \gamma_2^{n_2} r, \gamma_2^{n_3} r$ lie in that order on the circle), and will completely partition the side since

$$\lim_{n \rightarrow \infty} \gamma_2^n r = \gamma_{2,f}, \quad \lim_{n \rightarrow -\infty} \gamma_2^n r = \gamma_{2,s}.$$

Figure 2.1 demonstrates this claim when r lies outside ℓ_{γ_2} .

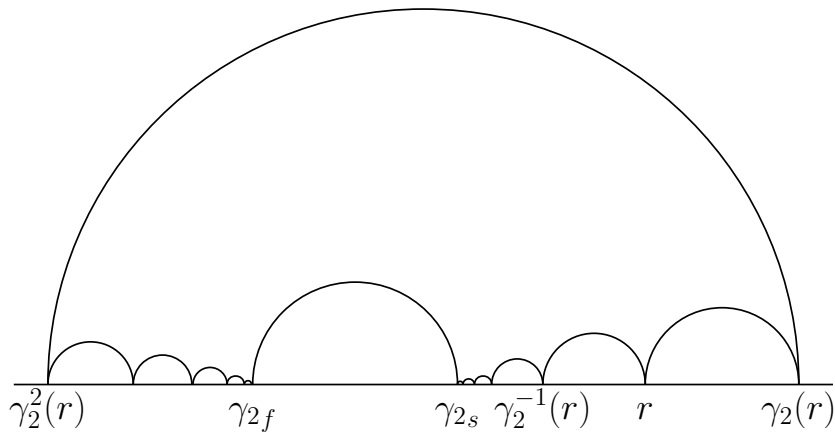


Figure 2.1: The geodesics $\ell_{\gamma_2^n r, \gamma_2^{n+1} r}$

In particular, any geodesic $\dot{\ell}$ that transversely intersects ℓ_{γ_2} will transversely intersect a unique geodesic $\dot{\ell}_{\gamma_2^n r, \gamma_2^{n+1} r}$. This can be scaled uniquely by a power of γ_2 to intersect $\dot{\ell}_{r, \gamma_2 r}$. The situation is analogous to in Proposition 2.4.1, and the result follows. \square

2.5 Intersection point and angle

By lifting an intersection into the upper half plane, we get a Γ -equivalence class of points. Furthermore, since Möbius maps preserve angles, the intersection corresponds to a unique angle. This motivates studying the intersection point and angle of pairs of $\mathrm{PSL}(2, \mathbb{R})$ matrices.

Definition 2.5.1. For any matrix $M \in \mathrm{PSL}(2, \mathbb{R})$, define $Z_M = M - \frac{\mathrm{Tr}(M)}{2}\mathrm{Id}$ to be the unique matrix of trace 0 related to M by a multiple of the identity matrix.

As we will see later, the matrix Z_M is often simpler in structure than M (for example, consider Z_{γ_q} , which is defined in Definition 3.1.1).

Theorem 2.5.2. *Let $M_1, M_2 \in \mathrm{PSL}(2, \mathbb{R})$ be hyperbolic matrices with corresponding non-overlapping root geodesics ℓ_1, ℓ_2 , and let $Z_{M_i} = Z_i$ for $i = 1, 2$. Then*

(i) ℓ_1, ℓ_2 intersect in the upper half plane if and only if

$$\det(M_1M_2 - M_2M_1) > 0.$$

(ii) We have

$$\det(M_1M_2 - M_2M_1) = \det(Z_1Z_2 - Z_2Z_1) = 4 \det(Z_1Z_2) - (\mathrm{Tr}(Z_1Z_2))^2.$$

(iii) If ℓ_1, ℓ_2 intersect transversely in the upper half plane, then

(a) the sign of the intersection is given by

$$\mathrm{sign}((M_1M_2 - M_2M_1)_{21}) = \mathrm{sign}((Z_1Z_2 - Z_2Z_1)_{21}).$$

(b) the intersection point is the fixed point of Z_1Z_2 that lies in the upper half plane.

(c) the intersection angle θ (measured counterclockwise from the tangent to ℓ_1 to the tangent to ℓ_2) satisfies

$$\tan(\theta) = \frac{\sqrt{\det(Z_1Z_2 - Z_2Z_1)}}{\mathrm{Tr}(Z_1Z_2)}.$$

Proof. Consider conjugating M_1, M_2 by some $N \in \text{PSL}(2, \mathbb{R})$, i.e. do

$$M_i \rightarrow NM_iN^{-1} \text{ for } i = 1, 2.$$

Then ℓ_i is taken to $N\ell_i$ and Z_i is taken to NZ_iN^{-1} . It follows that proving the theorem for M_1, M_2 is equivalent to proving it for NM_1N^{-1}, NM_2N^{-1} , except for possibly the sign of intersection (which will be treated in due course). Therefore we can replace M_1, M_2 by the conjugated pair, and since M_1, M_2 are diagonalizable over \mathbb{R} , choose N to diagonalize M_2 . Thus it can be assumed that

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M_2 = \begin{pmatrix} e & 0 \\ 0 & \frac{1}{e} \end{pmatrix},$$

for real numbers a, b, c, d, e , with $e > 1$ and $ad - bc = 1$. The root geodesic corresponding to M_2 is $\ell_{0, \infty}$, so the root geodesic of M_1 intersects this if and only if the product of the roots of M_1 is negative. This product is $-\frac{b}{c}$, so the geodesics intersect in the upper half plane if and only if $\frac{b}{c} > 0$ (which includes the hypothesis that $c \neq 0$). For the determinant, we calculate

$$\det(M_1M_2 - M_2M_1) = \det \begin{pmatrix} 0 & b(\frac{1}{e} - e) \\ c(e - \frac{1}{e}) & 0 \end{pmatrix} = bc \left(e - \frac{1}{e} \right)^2, \quad (2.5.1)$$

Since $e \neq \pm 1$, this is positive if and only if $bc > 0$, which is equivalent to $\frac{b}{c} > 0$, which is the first part.

For the second part, as $\frac{\text{Tr}(M_i)}{2}\text{Id}$ is a multiple of the identity, it commutes with all matrices.

Thus

$$M_1M_2 - M_2M_1 = Z_1Z_2 - Z_2Z_1. \quad (2.5.2)$$

Since Z_i has trace 0, its adjugate is $-Z_i$, and therefore

$$\begin{aligned} \det(Z_1Z_2 - Z_2Z_1) &= \frac{1}{2} \text{Tr}((Z_1Z_2 - Z_2Z_1)\text{adj}(Z_1Z_2 - Z_2Z_1)) \\ &= 2 \det(Z_1Z_2) - \frac{1}{2} \text{Tr}(Z_1Z_2\text{adj}(Z_1)\text{adj}(Z_2) + Z_2Z_1\text{adj}(Z_2)\text{adj}(Z_1)) \\ &= 2 \det(Z_1Z_2) - \text{Tr}((Z_1Z_2)^2) \\ &= 4 \det(Z_1Z_2) - (\text{Tr}(Z_1Z_2))^2, \end{aligned}$$

which completes the second point.

From now on, assume that the root geodesics of M_1, M_2 intersect. Since the second root of M_2 is 0,

$$\text{sg}(M_1, M_2) = +1 \Leftrightarrow M_{1,f} > 0 \Leftrightarrow M_{1,f} > M_{1,s} \Leftrightarrow c > 0.$$

Since

$$\text{sign}((M_1M_2 - M_2M_1)_{21}) = \text{sign}(c(e - \frac{1}{e})) = \text{sign}(c),$$

the result follows for the matrices M_1, M_2 . To complete the proof for all matrices, it suffices to show that the sign of $(M_1M_2 - M_2M_1)_{21}$ is constant when we conjugate M_1, M_2 . To do this, note that $M_1M_2 - M_2M_1$ has trace 0, hence

$$M = M_1M_2 - M_2M_1 = \begin{pmatrix} A & B \\ C & -A \end{pmatrix},$$

where $-A^2 - BC > 0$ as the root geodesics intersect. Let $N = \begin{pmatrix} E & F \\ G & H \end{pmatrix}$ be any matrix in $\text{PSL}(2, \mathbb{R})$, and then

$$((NM_1N^{-1})(NM_2N^{-1}) - (NM_2N^{-1})(NM_1N^{-1}))_{21} = (NMN^{-1})_{21} = CH^2 + 2AGH - BG^2.$$

This is a quadratic form in G, H with discriminant $4A^2 + 4BC < 0$, so it is a positive definite form. Thus the values it takes on pairs $(G, H) \neq (0, 0)$ all have the same sign, equal to the sign of $C = M_{21}$, as claimed. Equation 2.5.2 completes this point.

For the last two points, we do the explicit calculation. The semi-circle ℓ_1 has equation

$$\left(x - \frac{a-d}{2c}\right)^2 + y^2 = \frac{(a+d)^2 - 4}{4c^2}, \quad y \geq 0, \quad (2.5.3)$$

and the line ℓ_2 has equation $x = 0$ and $y \geq 0$. Thus the intersection point is given by $(x, y) = \left(0, \sqrt{\frac{b}{c}}\right)$. We calculate that

$$Z_1Z_2 = \frac{1}{4} \begin{pmatrix} (a-d)(e - \frac{1}{e}) & 2b(\frac{1}{e} - e) \\ 2c(e - \frac{1}{e}) & (a-d)(e - \frac{1}{e}) \end{pmatrix}, \quad (2.5.4)$$

and this has fixed points $\pm\sqrt{\frac{b}{c}}i$, as desired.

For the angle, we have that $\cot(\theta)$ is the slope of the tangent to ℓ_1 at the intersection point. The slope of tangent to the circle $(x - A)^2 + y^2 = R^2$ at (x_0, y_0) is $\frac{A-x_0}{y_0}$, so Equation 2.5.3 gives us

$$\tan(\theta) = \frac{1}{\cot(\theta)} = \frac{\sqrt{b/c}}{(a-d)/(2c)} = \frac{2\sqrt{bc}}{a-d}.$$

Equation 2.5.1 combined with Equation 2.5.2 and Equation 2.5.4 give that

$$\frac{\sqrt{\det(Z_1 Z_2 - Z_2 Z_1)}}{\operatorname{Tr}(Z_1 Z_2)} = \frac{\sqrt{bc} \left(e - \frac{1}{e}\right)}{\frac{1}{2}(a-d) \left(e - \frac{1}{e}\right)} = \frac{2\sqrt{bc}}{a-d} = \tan(\theta),$$

as desired. □

By applying Theorem 2.5.2 to the case of Shimura curves, we will generate very appealing and simple expressions for the intersection point and angle.

Chapter 3

Intersection numbers for $\mathrm{PSL}(2, \mathbb{Z})$

While much of the machinery and results for intersection numbers on Shimura curves will work for $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$ (as this is the image of the units of norm 1 in the quaternion algebra $\mathrm{Mat}(2, \mathbb{Z})$), the reverse is not true. In this chapter we will recast the intersection number for $\mathrm{PSL}(2, \mathbb{Z})$ in terms of quadratic forms, and relate this to work by Duke, Imamoğlu, and Tóth on the linking number of modular knots ([DIT17]). The crowning achievement of this section is an interpretation of the intersection number in terms of Conway's topograph, which also produces an efficient algorithm for computation. For an expanded exposition on quadratic forms, see any standard reference, for example [Bue89].

3.1 Binary quadratic forms

Let $q(x, y) = Ax^2 + Bxy + Cy^2 = [A, B, C]$ be a primitive integral binary quadratic form (i.e. $A, B, C \in \mathbb{Z}$ and $\gcd(A, B, C) = 1$) of discriminant $D = B^2 - 4AC$. The group $\mathrm{PSL}(2, \mathbb{Z})$ acts on q (on the right) via

$$\gamma \circ q(x, y) := q(ax + by, cx + dy), \text{ where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Write $q \sim q'$ if the quadratic forms q, q' are related by an element of $\mathrm{PSL}(2, \mathbb{Z})$. We can extend the equivalence to n -tuples of quadratic forms as follows:

$$(q_1, q_2, \dots, q_n) \sim_n (q'_1, q'_2, \dots, q'_n)$$

if there exists a $\gamma \in \mathrm{PSL}(2, \mathbb{Z})$ such that $\gamma \circ q_i = q'_i$ for all $1 \leq i \leq n$.

Call a quadratic form indefinite if $D > 0$ and D is not a perfect square, positive definite if $D < 0$ and $A > 0$, and negative definite if $D < 0$ and $A < 0$. Note that this definition is consistent across equivalence classes of quadratic forms. For a fixed discriminant D , the equivalence relation separates the primitive integral quadratic forms of discriminant D into finitely many classes. The set of equivalence classes of indefinite/positive definite forms of discriminant D forms a natural abelian group $\mathrm{Cl}^+(D)$ of size $h^+(D)$, called the narrow class group and narrow class number respectively. There is a natural bijection between indefinite/positive definite equivalence classes primitive binary quadratic forms of discriminant D and the narrow class group of \mathcal{O}_D , the unique order of discriminant D living in $\mathbb{Q}(\sqrt{D})$ (see Chapter 5 of [Coh93] for a full exposition).

For the rest of this section, we will work with primitive indefinite binary quadratic forms, abbreviated as “PIBQF”s. Given a PIBQF q , the *reciprocal* form is $-q$, where all the coefficients are negated. Call q reciprocal if $q \sim -q$. Write $q \not\sim_{\pm} q'$ if q is not equivalent to either q' or $-q'$, and call q, q' a *strongly inequivalent* pair. Note that quadratic forms with distinct discriminants are strongly inequivalent, and the notion of strong inequivalence extends to pairs of equivalence classes.

To shift our language from primitive hyperbolic matrices to PIBQFs, we need a way to pass between the two. The solution is to consider the action of $\mathrm{PSL}(2, \mathbb{Z})$ on q : this is an infinite cyclic group, generated by an invariant automorph.

Definition 3.1.1. Let $q = [A, B, C]$ be a PIBQF, and define

$$\gamma_q := \begin{pmatrix} \frac{T-BU}{2} & -CU \\ AU & \frac{T+BU}{2} \end{pmatrix},$$

where (T, U) are the smallest positive integer solutions to Pell’s equation

$$t^2 - Du^2 = 4.$$

Then γ_q generates the stabilizer of q in $\mathrm{PSL}(2, \mathbb{Z})$, and we call γ_q the invariant automorph of q .

Going from primitive hyperbolic matrices to PIBQFs is even easier.

Definition 3.1.2. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{Z})$ be a primitive hyperbolic matrix, taken with positive trace. The equation $Mx = x$ translates to $cx^2 + (d - a)x - b = 0$, so let $g = \gcd(c, d - a, b)$. The PIBQF associated to M is defined to be

$$q_M := \left[\frac{c}{g}, \frac{d - a}{g}, \frac{-b}{g} \right].$$

It can be checked that the operations $q \rightarrow \gamma_q$ and $M \rightarrow q_M$ are inverse operations, whence we have the bijection

$$\text{PIBQFs} \leftrightarrow \text{primitive hyperbolic matrices of } \mathrm{PSL}(2, \mathbb{Z}).$$

The action of $\mathrm{PSL}(2, \mathbb{Z})$ on PIBQFs corresponds to conjugation on primitive hyperbolic matrices as follows:

$$\gamma_{Mq} = M^{-1}\gamma_q M \text{ for all } M \in \mathrm{PSL}(2, \mathbb{Z}). \quad (3.1.1)$$

In particular, equivalence classes of PIBQFs corresponds to conjugacy classes of primitive hyperbolic matrices. Furthermore, taking the reciprocal acts as taking the inverse, i.e. $\gamma_{-q} = \gamma_q^{-1}$.

Using this bijection, we can consider the intersection numbers as taking in pairs of equivalence classes of PIBQFs. Note that the theory could have been developed for $\mathrm{PSL}(2, \mathbb{Z})$ and PIBQFs completely independently of the automorph and the bijection. Indeed, write $q = [A, B, C]$, and then the equation $q(x, 1) = 0$ has two real solutions, the roots of q . Let the *first root* and *second root* be

$$q_f := \frac{-B + \sqrt{D}}{2A}, \quad q_s := \frac{-B - \sqrt{D}}{2A},$$

respectively. Then the first and second roots of q are equal to the first and second roots of γ_q respectively. By replacing “matrix conjugacy” with “equivalence of PIBQFs” everywhere, statements can be refashioned using just quadratic forms.

3.2 Intersection numbers of binary quadratic forms

Recasting Theorem 2.5.2 with $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$ and quadratic forms produces very appealing statements. Let $q_i = [A_i, B_i, C_i]$ ($i = 1, 2$) be a pair of PIBQFs of discriminants D_1, D_2 , and

define

$$B_{\Delta}([A_1, B_1, C_1], [A_2, B_2, C_2]) := B_1B_2 - 2A_1C_2 - 2A_2C_1.$$

The notation B_{Δ} comes from Gross-Zagier in [GZ85].

Theorem 3.2.1. *We have*

(i) *The root geodesics of q_1, q_2 intersect uniquely in the upper half plane if and only if*

$$|B_{\Delta}(q_1, q_2)| < \sqrt{D_1D_2}.$$

(ii) *If the root geodesics intersect uniquely, let $x = B_{\Delta}(q_1, q_2)$. Then*

(a) *the sign of the intersection is given by*

$$\mathrm{sg}(q_1, q_2) = \mathrm{sign}(B_1A_2 - B_2A_1) = \mathrm{sign}(B_2C_1 - B_1C_2).$$

(b) *the point of intersection is the upper half plane root of*

$$[-A_1B_2 + A_2B_1, -2A_1C_2 + 2A_2C_1, -B_1C_2 + B_2C_1],$$

which is a (not necessarily primitive) quadratic form of discriminant $x^2 - D_1D_2$.

(c) *the angle of intersection θ satisfies*

$$\tan(\theta) = \frac{\sqrt{D_1D_2 - x^2}}{x}.$$

Proof. Let $T_i^2 - D_iU_i^2 = 4$ be the smallest solution to Pell's equation ($i = 1, 2$), and then

$$Z_i := Z_{\gamma_{q_i}} = \frac{U_i}{2} \begin{pmatrix} -B_i & -2C_i \\ 2A_i & B_i \end{pmatrix}.$$

The determinant is $\det(Z_i) = \frac{U_i^2}{4}(-B_i^2 + 4A_iC_i) = -\frac{U_i^2D_i}{4}$, and

$$Z_1Z_2 = \frac{U_1U_2}{4} \begin{pmatrix} B_1B_2 - 4A_2C_1 & 2B_1C_2 - 2B_2C_1 \\ -2A_1B_2 + 2A_2B_1 & B_1B_2 - 4A_1C_2 \end{pmatrix}.$$

Thus

$$\mathrm{Tr}(Z_1Z_2) = \frac{U_1U_2}{2}(B_1B_2 - 2A_1C_2 - 2A_2C_1) = \frac{U_1U_2}{2}B_{\Delta}(q_1, q_2).$$

Theorem 2.5.2 says that the root geodesics intersect if and only if $(\mathrm{Tr}(Z_1 Z_2))^2 < 4 \det(Z_1 Z_2)$, which translates to $|B_\Delta(q_1, q_2)| < \sqrt{D_1 D_2}$.

For the sign of the intersection, Theorem 2.5.2 gives

$$\mathrm{sg}(q_1, q_2) = \mathrm{sign}(Z_1 Z_2 - Z_2 Z_1)_{21} = \mathrm{sign}((U_1 U_2)(B_1 A_2 - A_1 B_2)) = \mathrm{sign}(B_1 A_2 - B_2 A_1).$$

The equality with $\mathrm{sign}(B_2 C_1 - B_1 C_2)$ comes from applying $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ to q_1, q_2 ; the sign of the intersection remains the same, and we start with PIBQFs $[C_i, -B_i, A_i]$ instead.

The intersection point and angle come directly from plugging in these calculations into Theorem 2.5.2. □

Remark 3.2.2. There exist alternate interpretations/proofs of various results in the case of quadratic forms, and we share a few here.

1. If the root geodesics of q_1, q_2 intersect, then an alternate interpretation of the sign of the intersection is the sign of $q_1(q_2, f, 1)$.
2. The discriminant of the quadratic form $q_1 x + q_2 y$ is

$$D_1 x^2 + 2B_\Delta(q_1, q_2)xy + D_2 y^2,$$

so B_Δ appears as the “cross term” of this expression. The intersection condition of $|B_\Delta(q_1, q_2)| < \sqrt{D_1 D_2}$ can also be recast as

$$B_\Delta(q_1, q_2)^2 < B_\Delta(q_1, q_1)B_\Delta(q_2, q_2).$$

3. The root geodesics intersect if and only if the cross-ratio $(q_{1,f}, q_{1,s}; q_{2,f}, q_{2,s})$ is negative.

A messy computation shows that this cross-ratio is equal to

$$\frac{B_\Delta(q_1, q_2) - \sqrt{D_1 D_2}}{B_\Delta(q_1, q_2) + \sqrt{D_1 D_2}},$$

which provides an alternative proof of Theorem 3.2.1i.

In particular, we have the following theorem.

Theorem 3.2.3. *The unweighted intersection number of q_1, q_2 of discriminants D_1, D_2 is the size of the set*

$$\left\{ (q'_1, q'_2) : q_1 \sim q'_1, q_2 \sim q'_2, |B_\Delta(q'_1, q'_2)| < \sqrt{D_1 D_2} \right\} / \sim_2.$$

Intersection points of pairs of geodesics are always quadratic irrational numbers, so it makes sense to also consider fixing such a point, and finding all possible root geodesics that pass through the point (i.e. all ways for which the point can appear as an intersection). It turns out that this is quite easy to characterize!

Proposition 3.2.4. *Let τ be a quadratic irrational in \mathbb{H} , the upper half plane root of the positive definite integral binary quadratic form q_1 , and let q_2 be a PIBQF. Then τ lies on the root geodesic of q_2 if and only if*

$$B_{\Delta}(q_1, q_2) = 0.$$

Proof. Let $q_i = [A_i, B_i, C_i]$ have discriminant D_i for $i = 1, 2$. Then τ is on γ_{q_2} if and only if

$$\begin{aligned} (x, y) &= \left(\frac{-B_1}{2A_1}, \frac{\sqrt{-D_1}}{2A_1} \right) \text{ satisfies } \left(x + \frac{B_2}{2A_2} \right)^2 + y^2 = \frac{D_2}{4A_2^2} \\ &\Leftrightarrow \left(\frac{A_1B_2 - A_2B_1}{2A_1A_2} \right)^2 - \frac{D_1}{4A_1^2} = \frac{D_2}{4A_2^2} \\ &\Leftrightarrow (A_1B_2 - A_2B_1)^2 = A_1^2D_2 + A_2^2D_1 \\ &\Leftrightarrow A_1^2B_2^2 - 2A_1A_2B_1B_2 + A_2^2B_1^2 = A_1^2B_2^2 - 4A_1^2A_2C_2 + A_2^2B_1^2 - 4A_2^2A_1C_1 \\ &\Leftrightarrow B_1B_2 = 2A_1C_2 + 2A_2C_1, \end{aligned}$$

which is equivalent to $B_{\Delta}(q_1, q_2) = 0$. □

3.3 Intersection numbers as linking numbers

This thesis project started by considering the work of Duke, Imamoglu, and Tóth in [DIT17]. They consider links in the space $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathrm{SL}(2, \mathbb{R})$, which is diffeomorphic to the complement of a trefoil knot in S^3 (see [Mil71]). Let $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ be a primitive hyperbolic matrix with positive trace, and take M_{γ} to diagonalize γ , so that

$$\gamma M_{\gamma} = M_{\gamma} \begin{pmatrix} \epsilon & 0 \\ 0 & \frac{1}{\epsilon} \end{pmatrix},$$

where $\epsilon > 1$ is the larger eigenvalue of γ . Let $\phi(t) := \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}$, and then

$$\tilde{\gamma}_+(t) := M_{\gamma}\phi(t) \quad \text{and} \quad \tilde{\gamma}_-(t) := M_{\gamma}S\phi(t) \quad \text{for } 0 \leq t \leq \log(\epsilon)$$

define closed paths in the space $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathrm{SL}(2, \mathbb{R})$. The knot $[\tilde{\gamma}_+]$ is null-homologous if and only if γ is reciprocal, i.e. it is conjugate to γ^{-1} . Thus we consider the link

$$[\tilde{\gamma}] := [\tilde{\gamma}_+] + [\tilde{\gamma}_-],$$

which is null-homologous in $\mathrm{SL}(2, \mathbb{Z}) \backslash \mathrm{SL}(2, \mathbb{R})$. Furthermore, this link remains constant over a $\mathrm{SL}(2, \mathbb{Z})$ conjugacy class, as well as replacing γ by γ^{-1} .

In Section 3 of [Ghy07], Ghys studied the linking number of $[\tilde{\gamma}_{\pm}]$ with the removed trefoil. His answer is expressed in terms of the Rademacher function, which is directly related to the classical Dedekind η function. In [DIT17], they instead consider the linking number of pairs of the knots. Specifically, given a pair of strongly inequivalent conjugacy classes of primitive hyperbolic matrices $[\sigma], [\gamma]$, their linking number $\mathrm{Lk}([\sigma], [\gamma])$ is the linking number of the null-homologous links associated to the classes. Duke, Imamoglu, and Tóth produce similar results to Ghys, by relating their answer to a modular cocycle (as opposed to a modular form). However, the final linking number formula produced is not particularly amenable to explicit computation. Furthermore, it is necessary to add $[\tilde{\gamma}_+]$ with $[\tilde{\gamma}_-]$ to produce null-homologous links. Ideally, the removed trefoil would be filled in, and the linking number of $[\tilde{\gamma}_+]$ with $[\tilde{\sigma}_+]$ would be computed. In Theorem 3.3.1 we prove that the linking number $\mathrm{Lk}([\sigma], [\gamma])$ corresponds to our $\mathrm{PSL}(2, \mathbb{Z})$ intersection number, and combining this with Algorithm 3.5.3 gives an efficient way to compute the linking number. Using the Conway topograph interpretation of the intersection number, a conjecture for the linking number of $[\tilde{\gamma}_+]$ and $[\tilde{\sigma}_+]$ is given in Section 3.7.

Theorem 3.3.1. *We have*

$$\mathrm{Lk}([\sigma], [\gamma]) = -\mathrm{Int}(\sigma, \gamma),$$

and the linking number is always even. Furthermore, if σ or γ is reciprocal, then the linking number is a multiple of 4.

Proof. Following [DIT17], let $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ and let $\Gamma_{\sigma} = \{g \in \Gamma : g\sigma g^{-1} = \sigma\} = \pm\sigma^{\mathbb{Z}}$. For $z_1, z_2 \in \overline{\mathbb{H}}$, define

$$I_{[\sigma]}(z_1, z_2) := \{\alpha \in \Gamma \backslash \Gamma_{\sigma} : \alpha \ell_{\sigma} \text{ intersects } \dot{\ell}_{z_1, z_2}\},$$

and note that its size does not depend on the choice of $\sigma \in [\sigma]$. Theorem 6.4 of [DIT17] shows that taking $z_0 = M_\gamma i \in \ell_\gamma$ gives

$$\mathrm{Lk}([\sigma], [\gamma]) = -|I_{[\sigma]}(z_0, \gamma z_0)|.$$

For $\alpha \in I_{[\sigma]}(z_0, \gamma z_0)$, the root geodesic $\alpha \ell_\sigma = \ell_{\alpha \sigma \alpha^{-1}}$ intersects $\dot{\ell}_{z_0, \gamma z_0}$, and $\alpha \sigma \alpha^{-1}$ is well defined and distinct α 's give distinct conjugates (since $\alpha \in \Gamma \setminus \Gamma_\sigma$).

Proposition 2.4.1 showed that

$$\mathrm{Int}(\sigma, \gamma) = \sum_{\substack{\beta \in \Gamma \text{ conjugate to } \sigma \\ |\ell_\beta \cap \dot{\ell}_{z, \gamma z}| = 1}} 1,$$

for $z \in \ell_\gamma$ not a fixed point of γ . The first result follows by taking $z = z_0$. The rest will follow from Corollary 3.4.8. \square

3.4 Conway's topograph

The Conway topograph is a device used to understand the equivalence class of a binary quadratic form. For an alternate presentation of the Conway topograph (as well as another interpretation of the river of an indefinite form), see [SV18].

3.4.1 The action of $\mathrm{PSL}(2, \mathbb{Z})$ on an infinite 3-regular graph

Let G be the infinite 3-regular connected graph drawn in the plane. The Conway topograph will consist of G and some additional data; we first study G . Let $E(G)_{\mathrm{or}}$ be the set of pairs (E, V) where E is an edge of G , and V is one of the two vertices on E (i.e. an oriented edge). We will define an action of $\mathrm{PSL}(2, \mathbb{Z})$ on $E(G)_{\mathrm{or}}$.

Recall that $\mathrm{PSL}(2, \mathbb{Z})$ is generated by the matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which gives the group presentation

$$\mathrm{PSL}(2, \mathbb{Z}) = \langle S, T \mid S^2 = (ST)^3 = 1 \rangle.$$

If E has vertices V_1, V_2 , define the action of S on (E, V_1) to be $S \circ (E, V_1) = (E, V_2)$, or equivalently you swap the edge orientation. To act via T , move along E to V_1 , and take

the left branch with the same orientation (i.e. the vertex that is not V_1). With reference to Figure 3.1, the action of T is

$$T \circ (E, V_1) = (F, V_3), \quad T \circ (F, V_1) = (G, V_4), \quad T \circ (G, V_1) = (E, V_2).$$

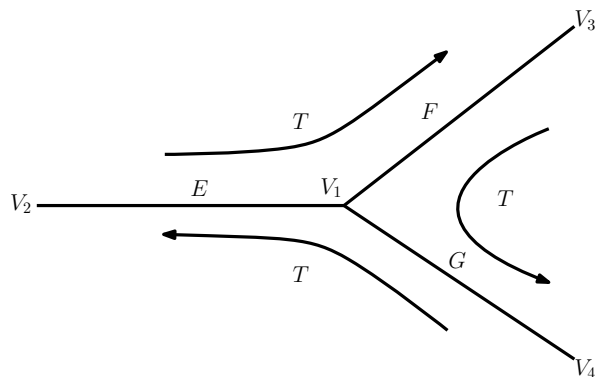


Figure 3.1: Action of T .

From this it is easy to see that the relations $S^2 = (ST)^3 = 1$ are satisfied, i.e. our action does descend down to an action of $\text{PSL}(2, \mathbb{Z})$. Furthermore, it is clear that the action is transitive, and the stabilizer of (E, V) is trivial. Thus we can form a (non-canonical) bijection between $E(G)_{\text{or}}$ and $\text{PSL}(2, \mathbb{Z})$, by picking a base element of $E(G)_{\text{or}}$.

Note that an alternate interpretation of $E(G)_{\text{or}}$ is as the set of ordered triples (R_1, E, R_2) , where R_1, R_2 are distinct regions of the plane formed by G that are separated by the edge E .

3.4.2 Definition of the topograph

A completed topograph will consist of the graph G , with numbers in all the regions formed by G , numbers on all of the edges, and arrows on certain edges. To read off a BQF, pick any region R_1 and edge E bordering the region, and let R_2 be the region on the other side of E . Orient so that E is horizontal, with R_1 above E and R_2 below it. If r_i and e represent the numbers on the regions and edge, then we form the BQF $[r_1, e, r_2]$ if the arrow on E is pointing right, and $[r_1, -e, r_2]$ if the arrow is pointing left. There will be no arrow if and only if $e = 0$, and then you form $[r_1, 0, r_2]$. The BQFs read off in this fashion will form an entire equivalence class of BQFs. Figure 3.2 is an example of how to read off BQFs.

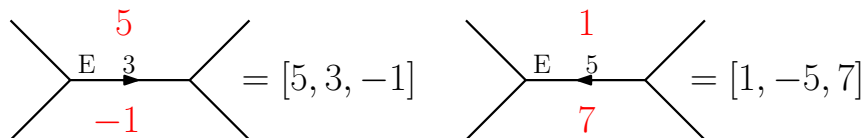


Figure 3.2: Reading BQFs from the topograph.

To create the topograph, start with a BQF $q = [A, B, C]$, and pick any pair $(E, V) \in E(G)_{\text{or}}$. For $M \in \mathrm{PSL}(2, \mathbb{Z})$, let $M \circ (E, V) = (E', V')$. When E' is horizontal with V' on the right, let R_1 be the region above E' and R_2 be the region below E' . If $M \circ [A, B, C] = [A', B', C']$, we write the number A' in R_1 , and $|B'|$ on E' . If $B' > 0$, draw the arrow so that when E' is horizontal with R_1 above it, then the arrow points right. If $B' < 0$ draw the opposite arrow, and if $B' = 0$ draw no arrow.

First, we claim that this is well defined. Consider the equations

$$T \circ [A, B, C] = [A, B + 2A, A + B + C], \quad S \circ [A, B, C] = [C, -B, A]. \quad (3.4.1)$$

If M, M' correspond to the same region R_1 , then we necessarily have $M' = MT^k$ for some integer k , and Equation 3.4.1 implies that they define the same number. If M, M' correspond to the same edge, we either have $M' = M$ or $M' = MS$, and Equation 3.4.1 again implies that the definition of $|B|$ and the arrow was consistent. Also, note that C' is necessarily assigned to the region R_2 .

For an alternate interpretation of the arrow, note that each edge E touches four regions, two along the length of the edge, and two its vertices. The arrow on E points from the region touching a vertex with a smaller number to the region touching a vertex with a larger number. These regions have the same number if and only if the number on the edge is 0, i.e. no arrow was drawn.

As examples, Figures 3.3 and 3.4 are parts of the topographs for the forms $[1, 0, -2]$ and $[1, 2, -2]$. The numbers in the regions are coloured red, and the numbers on the edges are black.

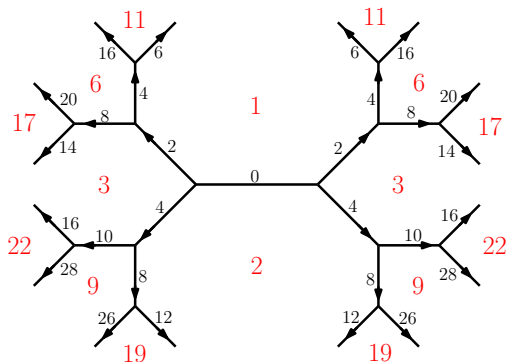


Figure 3.3: $[1, 0, 2]$ topograph.

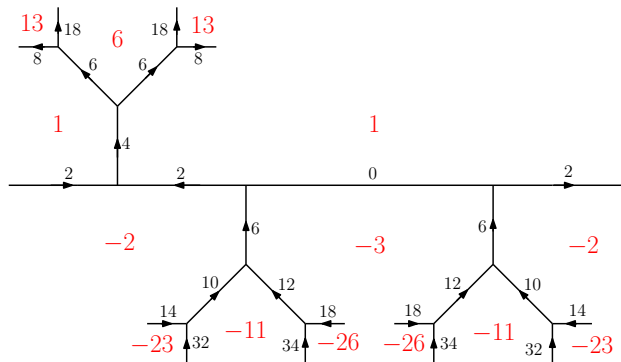


Figure 3.4: $[1, 2, -2]$ topograph.

3.4.3 Key properties of the topograph

From the construction, it is immediate that the BQFs read off from the topograph created from $[A, B, C]$ form the equivalence class of forms similar to $[A, B, C]$. Furthermore, any two forms in this equivalence class produce isomorphic topographs. However, one must be careful, as a form $[A, B, C]$ does not necessarily correspond to a *unique* pair (E, V) on its topograph. Indeed, it appears uniquely if and only if $[A, B, C]$ has trivial automorph. Assuming the form is primitive, this happens if and only if $D < -4$.

The numbers which appear in regions are precisely the numbers which can be represented properly by the BQFs in the equivalence class. This fact, coupled with the following lemma, allows us to determine if a number is properly represented by a given BQF.

Lemma 3.4.1 (Climbing Lemma). *Let $q = [A, B, C]$ be a BQF with $A, B, C > 0$. In the topograph with q present, numbers beyond q (in the direction of the arrow on the edge corresponding to q) are strictly increasing.*

Proof. In the region beyond we fill in $A + B + C$, and on the two adjacent edges we fill in $B + 2A, B + 2C$, so the numbers in the regions and the edges grow (and they remain positive, so the same applies again). □

Given two forms on a topograph q_1, q_2 , we can easily find the transition matrix to go between them. Indeed, let $M = \text{Id}$, let

$$L = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad (3.4.2)$$

and start at the oriented edge corresponding to q_1 . Take the path to the oriented edge corresponding to q_2 , where going forward and left corresponds to multiplying M by L on the right, forward and right corresponds to multiplying M by R on the right, and reversing direction corresponds to multiplying M by S on the right.

For example, from the $[1, 0, 2]$ topograph found in Figure 3.3, take $q_1 = [2, 4, 3]$ and $q_2 = [17, 14, 3]$, and we find that

$$M = SRLRR = \begin{pmatrix} 5 & 2 \\ -3 & -1 \end{pmatrix}.$$

It can be checked that indeed, $M \circ q_1 = q_2$.

3.4.4 The topograph of indefinite forms

When a binary quadratic form is indefinite, it will properly represent both positive and negative numbers. How is this fact reflected in the topograph? First, note that there are finitely many forms $[A, B, C]$ of fixed discriminant $D > 0$ which satisfy $AC < 0$, since the equation $D = B^2 - 4AC > B^2$ must be satisfied. On the topograph, it can be shown that such forms form a single path called the “river,” which separates the regions with positive numbers from the regions with negative numbers. Since there are finitely many forms possible, it is in fact a periodic sequence.

When drawing the topograph of an indefinite form, it is best to “flatten” the river and draw it horizontally, with trees branching off above (the positive direction) and below (the negative direction). Start at a vertex V on the river, and travel to the right along it, keeping track at each vertex whether we go left (L) or right (R). By stopping after the going along the smallest period of the river, we get a sequence of L 's and R 's. By taking a sequence to be equivalent to cyclic shifts, we assign a sequence to each topograph.

Definition 3.4.2. For a topograph T or form f in T , define $\mathrm{Riv}(T) = \mathrm{Riv}(f)$ to be this sequence, called the “river sequence”. It can either be thought of as an infinite (in both directions) periodic sequence of L 's and R 's, or as a finite sequence by only taking the least period of the topograph river, and declaring two sequences to be the same if they differ by

a cyclic shift (for example $LLR \sim LRL \sim RLL$). Furthermore, the river is said to “flow” from left to right when the positive regions are above the river.

The topograph of $[1, 2, -2]$ as displayed in Figure 3.4 has river sequence RLL , and Figure 3.5 gives part of the topograph of $[10, 14, -5]$, which has discriminant 396 and river sequence $RRLLRL$.

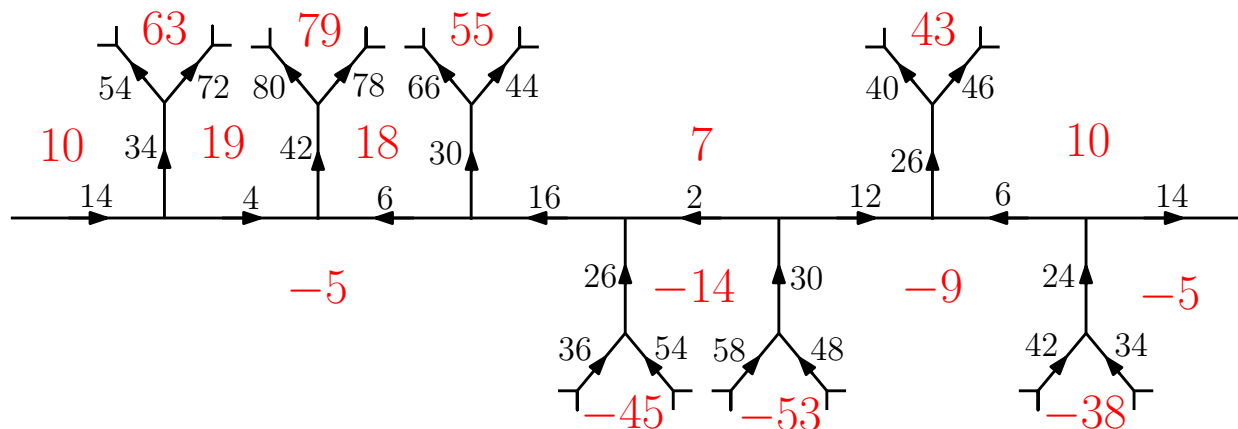


Figure 3.5: $[10, 14, -5]$ topograph.

Some key questions are:

- Can we recover a topograph from a river sequence?
- What is the connection to a topograph where the river “flows backwards”?
- What river sequences are possible?
- For q in the topograph, does γ_q flow with or against the river?

The answer to the first question is yes. Take the smallest period of the river sequence, and using R, L as in Equation 3.4.2, we get the invariant automorph of a form on the river, which thus determines the form and hence the entire topograph. It is important that we constructed this automorph by going *right* in the sequence, i.e. in the direction of the flow of the river. If we had gone to the left (against the flow), we would have also picked up a generator of the automorphism group of q , but it would be the inverse of what we define in Definition 3.1.1. In fact, this shows that this river sequence (i.e. going left) gives us the

river sequence of $-q$, the reciprocal of q . Formally put, to get $\mathrm{Riv}(-q)$, take $\mathrm{Riv}(q)$, replace the L 's by R 's and R 's by L 's, and reverse the sequence. Thus it is easy to detect if an equivalence class is reciprocal directly from the river sequence. For example, $RRRL$ is not reciprocal, but RRL is.

In terms of possible sequences, note that there must be at least one L and one R , as indefinite forms represent both positive and negative numbers. From the above commentary, we see that any periodic sequence with at least one L and one R is the river of some topograph (noting that the constructed automorph is in fact hyperbolic, so it does correspond to a PIBQF).

The final answer is γ_q flows with the river, no matter what q is. To see this, first assume $q = [A, B, C]$ is on the river with $A > 0$. Then the entries of γ_q are all positive, and two of the entries of γ_q^{-1} are negative. The invariant automorph obtained by going along the flow of the river will be a product of L 's and R 's, and will thus have positive entries, which gives the result in this case. The general result follows from Equation 3.1.1.

Remark 3.4.3. When studying indefinite quadratic forms, one normally introduces the notion of a reduced form, defines right and left neighbours of reduced forms, and shows that this forms a unique cycle. Taking the common choice of $[A, B, C]$ is reduced if $B > |A + C|$, when going along the river, these reduced forms correspond to the forms between the branches switching from the negative to the positive sides of the river (and vice versa). Taking the right/left neighbour just corresponds to going to the next/previous reduced form along the river.

Remark 3.4.4. Let $q = [A, B, C]$ be a PIBQF; we can think of the river of the topograph of q as its root geodesic. We have $A = q(1, 0)$, and the number appearing in the corresponding place after applying γ_q^n will be $A = q(x, y)$, where

$$\begin{pmatrix} x \\ y \end{pmatrix} = \gamma_q^n \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

whence $\frac{x}{y} = \gamma_q^n(\infty)$. As $n \rightarrow \infty$, $\gamma_q^n(\infty) \rightarrow q_f$, and as $n \rightarrow -\infty$, $\gamma_q^n(\infty) \rightarrow q_s$. Since γ_q moves along the river in the direction it is flowing, we can think of the river as flowing from the second root of q to the first root of q .

3.4.5 Intersection numbers in terms of the topograph

Consider two topographs T_i , with chosen pairs (E_i, V_i) of an edge E_i in the graph of T_i and a vertex V_i on E_i ($i = 1, 2$). Since the underlying graphs are the same, we can superimpose one graph on the other by identifying V_1 with V_2 and E_1 with E_2 . When we do this, one can consider the interaction of the superimposed rivers R_1, R_2 .

Proposition 3.4.5. *Let the PIBQFs q_i correspond to topographs T_i ($i = 1, 2$).*

- (i) *The root geodesics of q_1, q_2 intersect transversely in the upper half plane if and only if when you superimpose T_1, T_2 at q_1, q_2 (as above), the superimposed rivers R_1, R_2 meet and cross. Furthermore, the root geodesics completely overlap if and only if the rivers R_1, R_2 completely overlap.*
- (ii) *If the root geodesics of q_1, q_2 intersect transversely in the upper half plane, consider the flow of the the rivers. Going along the river R_1 in the direction it is flowing, if R_2 joins the river from the right hand side then the sign of the intersection is 1, and if it joins from the left the sign is -1 .*

Proof. Consider the set

$$\{(\mathrm{sign}(q_1(x, 1)), \mathrm{sign}(q_2(x, 1)))\},$$

as x ranges over \mathbb{R} . Of the 4 possible non-zero pairs of signs $(\pm 1, \pm 1)$, we note that

- All 4 pairs appear if the root geodesics intersect in the upper half plane;
- 3 pairs appear if the root geodesics do not intersect in the upper half plane and do not overlap;
- 2 pairs appear if the root geodesics overlap.

This also remains true if we instead consider

$$\{(\mathrm{sign}(q_1(x, y)), \mathrm{sign}(q_2(x, y)))\},$$

where (x, y) range over pairs of coprime integers.

When we superimpose the topographs, the numbers in the regions correspond to the values that q_1, q_2 take on coprime integers. Since we impose q_1 on top of q_2 , the value of $q_1(x, y)$ is imposed onto the value of $q_2(x, y)$. However, the rivers R_1, R_2 determine the boundary between the signs of the numbers in the regions, so that we get 4 sign combinations if and only if the rivers meet and cross, 3 if they either never meet or meet and do not cross, and 2 if they overlap.

Figure 3.6 demonstrates the four possible flow configurations, and the claimed corresponding sign.

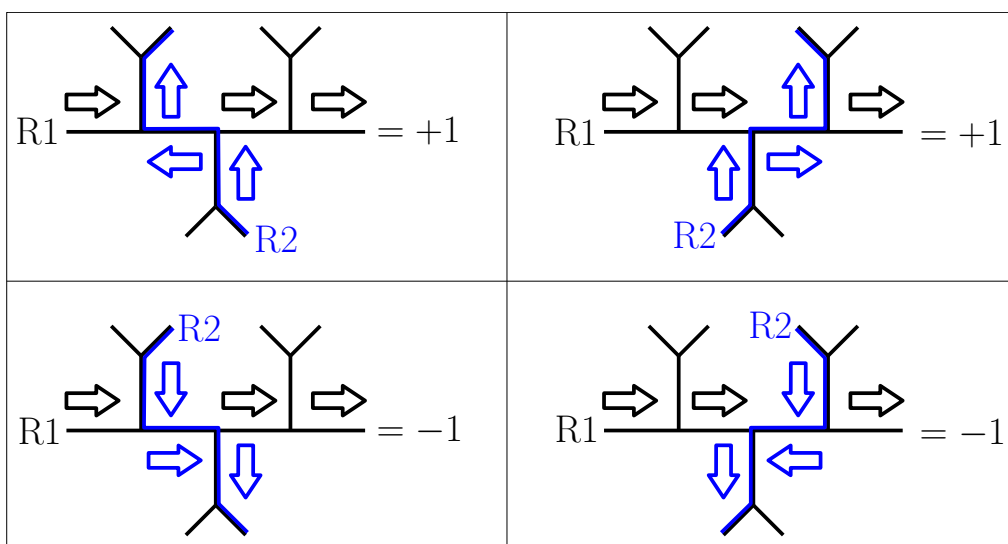


Figure 3.6: Possible flow configurations.

Recall Remark 3.4.4, where we interpreted the river as flowing between the two roots. Combining this with the interpretation of the sign found in Proposition 3.4.5 gives the above picture, as the second river originates at the second root and flows towards the first root. \square

Corollary 3.4.6. *Let q_1, q_2 be a pair of PIBQFs. Then the unweighted intersection number $\mathrm{Int}(q_1, q_2)$ is equal to the number of ways to superimpose the topographs corresponding to q_1, q_2 on top of each other so that the rivers R_1, R_2 meet and cross, modulo the periods of the rivers. The weighted intersection number $\mathrm{Int}^\pm(q_1, q_2)$ is the same, except we add 1 when R_2 joins R_1 from the right, and -1 when R_2 joins R_1 from the left.*

Proof. This follows from Proposition 2.4.2 and Proposition 3.4.5. \square

Let's examine the consequences of Corollary 3.4.6 a bit more closely. If we have an intersection, we can follow the flow of the river R_2 until it meets R_1 to find a unique pair of vertices (V_1, V_2) satisfying

- V_i is on R_i for $i = 1, 2$;
- V_1 is superimposed on V_2 ;
- the vertex preceding V_2 (in the sense of the flow of R_2) is not superimposed on the river R_1 .

Furthermore, given a pair (V_1, V_2) of vertices on the rivers R_1, R_2 respectively, there is a unique way to superimpose the topographs so the above is satisfied (though there is no guarantee that the rivers end up crossing). Since the rivers can either be flowing right or left at V_i , we have four different behaviours, and display them in Figure 3.7.

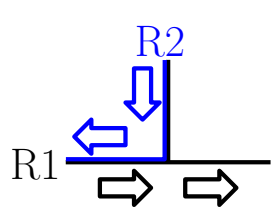
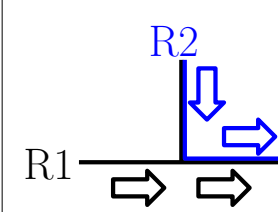
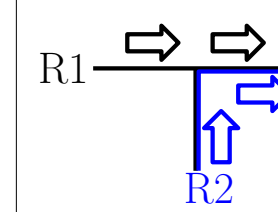
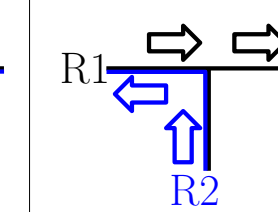
| | | | |
|---|---|--|---|
| Pair: (R,R) | (R,L) | (L,R) | (L,L) |
| Sign: -1 | -1 | +1 | +1 |
|  |  |  |  |

Figure 3.7: Sign of the intersection.

Put another way, the second river can join from the left (L) or right (R), and flow in the same (S) or opposite (O) direction. The above picture demonstrates the behaviours LO, LS, RS, RO in order from left to right. For each $x \in \{LO, LS, RS, RO\}$, define Int^x to be the intersection number where we only count intersections of the behaviour x . In particular, we get that

$$\text{Int} = \text{Int}^{\text{RS}} + \text{Int}^{\text{RO}} + \text{Int}^{\text{LS}} + \text{Int}^{\text{LO}} \quad \text{and} \quad \text{Int}^\pm = \text{Int}^{\text{RS}} + \text{Int}^{\text{RO}} - \text{Int}^{\text{LS}} - \text{Int}^{\text{LO}}. \quad (3.4.3)$$

Since the river of a reciprocal form is the same except with opposite flow, we can deduce that

$$\text{Int}^{\text{RS}}(q_1, q_2) = \text{Int}^{\text{LO}}(q_1, -q_2), \text{ and } \text{Int}^{\text{RO}}(q_1, q_2) = \text{Int}^{\text{LS}}(q_1, -q_2). \quad (3.4.4)$$

When we switch the order of q_1, q_2 , we get

$$\text{Int}^{\text{RS}}(q_1, q_2) = \text{Int}^{\text{LS}}(q_2, q_1), \text{ and } \text{Int}^{\text{RO}}(q_1, q_2) = \text{Int}^{\text{LO}}(q_2, q_1).$$

For a non-trivial identity, we have the following proposition.

Proposition 3.4.7. *The following equalities hold*

$$\text{Int}^{\text{RS}}(q_1, q_2) = \text{Int}^{\text{LS}}(q_1, q_2), \text{ and } \text{Int}^{\text{RO}}(q_1, q_2) = \text{Int}^{\text{LO}}(q_1, q_2).$$

Proof. Let the river corresponding to q_1 be $R_1 = (x_1, x_2, \dots, x_m)$ and the river corresponding to q_2 be $R_2 = (y_1, y_2, \dots, y_n)$, where L is represented by 0 and R by 1. For now, assume that $\text{gcd}(m, n) = 1$. Let $A = (a_1, a_2, \dots, a_{mn})$ be the sequence R_1 repeated n times, and let $B = (b_1, b_2, \dots, b_{mn})$ be the sequence R_2 repeated m times (take indices of A, B modulo mn). As $\text{gcd}(m, n) = 1$, pairs (x_i, y_j) with $1 \leq i \leq m$ and $1 \leq j \leq n$ biject with the pairs (a_k, b_k) for $1 \leq k \leq mn$. Intersecting the rivers flowing in the same direction at (a_k, b_k) first requires $a_k \neq b_k$. The rivers will then take the same path until we get to the smallest $r \geq 1$ such that $a_{k+r} \neq b_{k+r}$. We will have an intersection if $a_k \neq a_{k+r}$!

In particular, consider the sequence $C = A + B \pmod{2} = (c_1, c_2, \dots, c_{mn})$. Potential intersections will correspond to consecutive pairs of 1's in C , so let $I = \{1 \leq i \leq mn : c_i = 1\} = \{i_1, \dots, i_r\}$ with $i_1 < i_2 < \dots < i_r$. Form the sequence $D = (a_{i_1}, a_{i_2}, \dots, a_{i_r})$, seen cyclically. In the sequence D , we have

- going from 0 to 0 corresponds to R_2 coming in from the right and leaving to the right;
- going from 0 to 1 corresponds to R_2 coming in from the right and leaving to the left;
- going from 1 to 0 corresponds to R_2 coming in from the left and leaving to the right;
- going from 1 to 1 corresponds to R_2 coming in from the left and leaving to the left.

In particular, $\mathrm{Int}^{\mathrm{RS}}(q_1, q_2)$ counts the number of times we change from 0 to 1 in D , and $\mathrm{Int}^{\mathrm{LS}}(q_1, q_2)$ counts how many times we change from 1 to 0 in D . As D is periodic, these are equal, hence the result follows in this case.

When $\mathrm{gcd}(m, n) = d > 1$, we instead form sequences of length $\frac{mn}{d} = \mathrm{lcm}(m, n)$, and apply the above. Repeat by shifting the B sequence by $1, 2, \dots, d - 1$ to the right, and this covers all intersections.

The second statement follows from replacing q_2 by $-q_2$ and using Equation 3.4.4. \square

Corollary 3.4.8. *We have*

$$\mathrm{Int}(q_1, q_2) = 2(\mathrm{Int}^{\mathrm{RS}}(q_1, q_2) + \mathrm{Int}^{\mathrm{RO}}(q_1, q_2)), \text{ and } \mathrm{Int}^{\pm}(q_1, q_2) = 0.$$

Furthermore, if either q_1 or q_2 is reciprocal, then

$$\mathrm{Int}(q_1, q_2) = 4\mathrm{Int}^{\mathrm{RS}}(q_1, q_2).$$

Proof. This follows immediately from Equations 3.4.3, 3.4.4, and Proposition 3.4.7. Note that $\mathrm{Int}^{\pm}(q_1, q_2) = 0$ also follows from $\mathrm{PSL}(2, \mathbb{Z}) \backslash \mathbb{H}$ having genus 0, as the signed intersection number is well defined in homology. \square

Corollary 3.4.9. *Let q_1, q_2 be a pair of PIBQFs with river periods p_1, p_2 . Then*

$$4 \leq \mathrm{Int}(q_1, q_2) \leq p_1 p_2.$$

Proof. Each possible intersection came from a pair of vertices on the river modulo the periods, which gives the upper bound. For the lower bound, it suffices to prove that $\mathrm{Int}^{\mathrm{RS}}(q_1, q_2) \geq 1$. Since the river sequences contain at least one 0 and one 1, we can find the subsequence 01 in the first river, and 10 in the second. This will correspond to an intersection of type RS , completing the proof. \square

3.5 Continued fractions and explicit computation of the intersection number

The proof of Proposition 3.4.7 gives us a nice and fast algorithm to calculate intersection numbers. We first describe how to calculate the river sequences, and then present the algorithm.

Algorithm 3.5.1. Given a PIBQF q of discriminant D , this algorithm calculates the river sequence of q .

1. Find a reduced form q' equivalent to q (see any book on quadratic forms, for example Chapter VII of [Dic29]).
2. If the leading coefficient of q' is negative, replace q' by $S \circ q'$.
3. Input (\cdot, q') into the following process (\cdot is the empty string):
 - (a) Given (V, f) , write $f = [A, B, C]$ and let $k = \left\lfloor \frac{-B + \sqrt{D}}{2A} \right\rfloor$.
 - (b) If $k > 0$, append k copies of L to the right of V to form V' , and let $f' = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \circ f = L^k \circ f$. If $f' = q'$, then terminate the process and return V' ; otherwise, repeat with (V', f') .
 - (c) If $k \leq 0$, let $k' = \left\lfloor \frac{-B - \sqrt{D}}{2C} \right\rfloor$. Append k' copies of R to the right of V to form V' , and let $f' = \begin{pmatrix} 1 & 0 \\ k' & 1 \end{pmatrix} \circ f = R^{k'} \circ f$. If $f' = q'$, then terminate the process and return V' ; otherwise, repeat with (V', f') .

Proof. The algorithm works by finding the consecutive blocks of R 's and L 's found on the river. Reduced forms always appear between branches on opposite sides of the river, so we start in a valid location. The maximum number of L 's we can go along the river corresponds to the maximum value of k for which applying $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ to f gives a third coefficient that is negative, and the maximum number of R 's corresponds to the maximum value of k for which applying $\begin{pmatrix} 1 & 0 \\ k' & 1 \end{pmatrix}$ to f gives a first coefficient that is positive. By applying this process repeatedly, we will follow the river and eventually come back to our original form after completing the period of the river. Note that in the actual process, after finding a block of L 's we know that we will get a block of R 's (and vice versa), so we only have to calculate both k and k' the first time. \square

By calculating maximal blocks of L 's and R 's at once, the algorithm more efficient than calculating each L and R on the river step by step.

Remark 3.5.2. Let the continued fraction of q_f be

$$[a_0, a_1, \dots] = [a_0, a_1, \dots, a_s, \overline{a_{s+1}, \dots, a_{s+p}}],$$

where s is the smallest integer such that the continued fraction is periodic after index s , and p is the smallest *even* integer such that the sequence has period p .

Define $\text{Riv}'(q)$ to be the sequence of 0's and 1's formed by:

- $s + 1 \pmod{2}$ repeated a_{s+1} times;
- $s + 2 \pmod{2}$ repeated a_{s+2} times;
- ...
- $s + p \pmod{2}$ repeated a_{s+p} times.

Then $\text{Riv}'(q)$ and $\text{Riv}(q)$ are equal! For example, if $q = [10, 14, -5]$, then the continued fraction of q_f is

$$[0, \overline{3, 2, 1, 1}],$$

and

$$\text{Riv}'(q) = (1, 1, 1, 0, 0, 1, 0),$$

which agrees with Figure 3.5, where L corresponds to 0 and R corresponds to 1.

By using the continued fraction definition of river sequence, we can remove the need for the Conway topograph in the presentation of results (though its understanding is crucial to the proofs).

Algorithm 3.5.3. Given a pair of PIBQFs q_1, q_2 , this algorithm calculates $\text{Int}^{RS}(q_1, q_2)$.

1. Use Algorithm 3.5.1 to calculate the river sequences for q_1, q_2 , denoted $r_1 = (x_1, x_2, \dots, x_m)$ and $r_2 = (y_1, y_2, \dots, y_n)$, where L 's are denoted by 0's and R 's by 1's.
2. Let $g = \gcd(m, n)$, let $N = \text{lcm}(m, n)$, and let $I = 0$. Form the sequence $B = (b_1, b_2, \dots, b_N)$ by repeating the sequence $r_2 \frac{N}{n}$ times starting at $b_1 = y_1$. For each $1 \leq i \leq g$,
 - (a) Form the sequence $A = (a_1, a_2, \dots, a_N)$ by repeating the sequence $r_1 \frac{N}{m}$ times, starting at $a_1 = x_i$.
 - (b) Form the sequence $C = A + B \pmod{2} = (c_1, c_2, \dots, c_N)$.

- (c) Let $j_1 < j_2 < \dots < j_r$ be the indices j for which $c_j = 1$, and let $j_{r+1} = j_1$.
- (d) For each index $1 \leq k \leq r$ with $a_{j_k} = 0$ and $a_{j_{k+1}} = 1$, add 1 to I .

3. Return I .

By applying the above algorithm to the pair $(-q_2, q_1)$, we calculate $\mathrm{Int}^{RO}(q_1, q_2)$, and hence get $\mathrm{Int}(q_1, q_2)$ by Corollary 3.4.8.

3.6 Examples

As illustration, we provide two examples of intersection numbers.

Example 3.6.1. Let $q_1 = [1, 3, -3]$ and $q_2 = [7, 6, -10]$, hence $D_1 = 21$ and $D_2 = 316$. We compute the river sequences to be

$$\mathrm{Riv}(q_1) = a = (1, 0, 0, 0), \quad \mathrm{Riv}(q_2) = b = (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0).$$

To compute $\mathrm{Int}^{RS}(q_1, q_2)$, it requires to count the triples (i, j, k) for which $(a_{i+1}, a_{i+2}, \dots, a_{i+k-1}) = (b_{j+1}, b_{j+2}, \dots, b_{j+k-1}) = s$, $(a_i, a_{i+k}) = (0, 1)$, and $(b_j, b_{j+k}) = (1, 0)$. The triples, s , a pair (f_1, f_2) with $f_i \sim q_i$ of the corresponding simultaneous equivalence class, and $B_\Delta(f_1, f_2)$ are given in Table 3.1.

Table 3.1: Intersections of $[1, 3, -3]$ and $[7, 6, -10]$ of type RS .

| (i, j, k) | s | f_1 | f_2 | $B_\Delta(f_1, f_2)$ |
|-------------|-----------------|-------------|---------------|----------------------|
| (2, 1, 3) | (0, 0) | [1, -1, -5] | [3, -14, -10] | 64 |
| (3, 1, 2) | (0) | [1, 1, -5] | [3, -14, -10] | 36 |
| (3, 9, 2) | (0) | [1, 1, -5] | [6, -14, -6] | 56 |
| (3, 12, 6) | (0, 1, 0, 0, 0) | [1, 1, -5] | [7, -8, -9] | 80 |
| (4, 1, 1) | () | [1, 3, -3] | [3, -14, -10] | -4 |
| (4, 9, 1) | () | [1, 3, -3] | [6, -14, -5] | 4 |
| (4, 12, 1) | () | [1, 3, -3] | [7, -8, -9] | 36 |

Note that in all examples, $B_\Delta(f_1, f_2) \leq 81 < \sqrt{21 \cdot 316}$, as is predicted by Theorem 3.2.1. We can compute $\mathrm{Int}^{RO}([1, 3, -3], [7, 6, -10])$ in similar fashion, by finding the triples (i, j, k)

for which $(a_{i+1}, a_{i+2}, \dots, a_{i+k-1}) = (1 - b_{j+k-1}, 1 - b_{j+k-2}, \dots, 1 - b_{j+1}) = s$, $(a_i, a_{i+k}) = (1, 0)$, and $(b_j, b_{j+k}) = (0, 1)$. The triples, s , a pair (f_1, f_2) with $f_i \sim q_i$ of the corresponding simultaneous equivalence class, and $B_\Delta(f_1, f_2)$ are given in Table 3.2.

Table 3.2: Intersections of $[1, 3, -3]$ and $[7, 6, -10]$ of type RO .

| (i, j, k) | s | f_1 | f_2 | $B_\Delta(f_1, f_2)$ |
|--------------|----------|---------------|----------------|----------------------|
| $(1, 6, 1)$ | $()$ | $[1, -3, -3]$ | $[-5, -16, 3]$ | 12 |
| $(1, 6, 2)$ | (0) | $[1, -1, -5]$ | $[-5, -16, 3]$ | -40 |
| $(1, 6, 3)$ | $(0, 0)$ | $[1, 1, -5]$ | $[-5, -16, 3]$ | -72 |
| $(1, 11, 1)$ | $()$ | $[1, -3, -3]$ | $[-9, -10, 6]$ | -36 |
| $(1, 13, 1)$ | $()$ | $[1, -3, -3]$ | $[-10, -6, 7]$ | -56 |

Therefore we have an example where $\text{Int}^{RS}(q_1, q_2) \neq \text{Int}^{RO}(q_1, q_2)$.

Example 3.6.2. If $q_1 = [1, 1, -1]$ and $q_2 = [1, n, -1]$ for $n \geq 2$, we claim that $\text{Int}(q_1, q_2) = 8$.

The automorphs of q_1, q_2 can be shown to be

$$\gamma_{q_1} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = RL, \quad \gamma_{q_2} = \begin{pmatrix} 1 & n \\ n & n^2 + 1 \end{pmatrix} = R^n L^n.$$

The corresponding river sequences are $(1, 0)$, and n 1's followed by n 0's respectively. Since q_1 is reciprocal, by Corollary 3.4.8, $\text{Int}(q_1, q_2) = 4 \text{Int}^{RS}(q_1, q_2)$. Following Algorithm 3.5.3, if n is even we generate Table 3.3.

Table 3.3: Intersections of $[1, 1, -1]$ and $[1, n, -1]$ for $n \geq 2$.

| | |
|--|---|
| $A = (1, 0, \dots, 1, 0, 1, 0, \dots, 1, 0)$ | $A = (0, 1, \dots, 0, 1, 0, 1, \dots, 0, 1);$ |
| $B = (1, 1, \dots, 1, 1, 0, 0, \dots, 0, 0)$ | $B = (1, 1, \dots, 1, 1, 0, 0, \dots, 0, 0);$ |
| $C = (0, 1, \dots, 0, 1, 1, 0, \dots, 1, 0)$ | $C = (1, 0, \dots, 1, 0, 0, 1, \dots, 0, 1).$ |

In the left hand case, the only time sequence A goes from a 0 to a 1 between consecutive 1's in C is from index n to $n + 1$. Similarly, in the right hand case, it is only from indices $n - 1$ to $n + 2$. Therefore, $\text{Int}^{RS}(q_1, q_2) = 2$, as claimed. When n is odd, the analogous result follows.

3.7 Filling in the trefoil knot

As commented on in Section 3.3, the linking number of $[\tilde{\sigma}_+]$ and $[\tilde{\gamma}_+]$ is unknown. This linking pair exhibits a very similar formal behaviour to $\mathrm{Int}^{\mathrm{RS}}$ and $\mathrm{Int}^{\mathrm{RO}}$: they sum to half of the full intersection number, they are equal when either input is a reciprocal matrix/quadratic form, and they are not necessarily equal when both inputs are not reciprocal.

Conjecture 3.7.1. *Let q_1, q_2 be a strongly inequivalent pair of PIBQFs. Then the linking number of $\tilde{\gamma}_{q_1,+}$ and $\tilde{\gamma}_{q_2,+}$ in $\mathrm{SL}(2, \mathbb{Z}) \setminus \mathrm{SL}(2, \mathbb{R})$ with the trefoil filled in is equal to either $-\mathrm{Int}^{\mathrm{RS}}(q_1, q_2)$ or $-\mathrm{Int}^{\mathrm{RO}}(q_1, q_2)$.*

To approach this conjecture, one would need to understand how to compute the linking number when the trefoil knot is filled in. Since this has not been done, we do not have any numerical evidence towards the conjecture.

Chapter 4

Quaternionic background

From now on, we shift our focus to quaternion algebras. The goal of this section is to recall quaternion algebras and Eichler orders, describe some of their key properties, and then give a full study of optimal embeddings of quadratic orders into Eichler orders. This will set us up to study intersection numbers on Shimura curves in Sections 5 and beyond. For a full exposition on quaternion algebras, see [Voi21].

4.1 Local and global quaternion algebras

Let F be a field of characteristic 0, and $a, b \in F^\times$. We take $B = \left(\frac{a,b}{F}\right)$ to be the quaternion algebra associated to a, b, F . As an additive vector space, this is of dimension 4 over F , with basis $1, i, j, k$, and general element of the form

$$x = e + fi + gj + hk, \text{ where } e, f, g, h \in F.$$

The multiplicative structure is determined by the standard equations

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji,$$

which imply that $k^2 = -ab$. Alternatively, a quaternion algebra over F is a central simple algebra of dimension 4. The standard involution on B is denoted by an overline, and explicitly defined by

$$\bar{x} := e - fi - gj - hk.$$

The quaternion algebra also comes equipped with the reduced trace $\text{trd} : B \rightarrow F$ and the reduced norm $\text{nrd} : B \rightarrow F$, defined by

$$\begin{aligned}\text{nrd}(x) &:= x\bar{x} = e^2 - af^2 - bg^2 + abh^2; \\ \text{trd}(x) &:= x + \bar{x} = 2e.\end{aligned}$$

When $F = \mathbb{R}$, there are exactly two quaternion algebras up to isomorphism: $\text{Mat}(2, \mathbb{R})$, and the Hamilton quaternions $\text{QA}_\infty^{\text{div}} = \left(\frac{-1, -1}{\mathbb{R}}\right)$ (which is a division algebra). Similarly, over \mathbb{Q}_p , there are two quaternion algebras up to isomorphism: $\text{Mat}(2, \mathbb{Q}_p)$, and a division algebra which we denote by QA_p^{div} . From Theorem 13.3.10 of [Voi21], it follows that we can write

$$\text{QA}_p^{\text{div}} = \left(\frac{p, e}{\mathbb{Q}_p}\right),$$

where e is any integer such that $\left(\frac{e}{p}\right) = -1$, and $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

Let $B = \left(\frac{a, b}{\mathbb{Q}}\right)$ be a quaternion algebra over \mathbb{Q} . Crucial to understanding B is understanding its local behaviour, i.e. studying $B_v = B \otimes \mathbb{Q}_v = \left(\frac{a, b}{\mathbb{Q}_v}\right)$, where v is a place of \mathbb{Q} and $\mathbb{Q}_\infty = \mathbb{R}$. Call v ramified in B if $B_v \simeq \text{QA}_v^{\text{div}}$, and call v split otherwise. Define the Hilbert symbol $(a, b)_v$ to be 1 if p is split in B , and -1 if B is ramified. Then the set of ramified places is both finite and of even size, and we say that B has discriminant \mathfrak{D} , which is the product of all ramifying places.

The quaternion algebra B over \mathbb{Q} is uniquely determined (up to isomorphism) by the set of ramifying places, and furthermore, any finite even sized set of places corresponds to a quaternion algebra over \mathbb{Q} . We call B indefinite if ∞ is split, and so B is ramified at an even number of finite primes. In this thesis, we will primarily be working with indefinite quaternion algebras, though some results can be adapted to the definite case.

An order O of B is a lattice that is also a subring. A maximal order is an order which is not properly contained within another order. An example of a maximal order of $\text{Mat}(2, \mathbb{Q}_p)$ is $\text{Mat}(2, \mathbb{Z}_p)$, and in fact all maximal orders of $\text{Mat}(2, \mathbb{Q}_p)$ are conjugate. Over QA_p^{div} , there is a unique maximal order, which consists of all integral elements.

Let I be a lattice in B , and define the left order of I to be

$$O_L(I) := \{\alpha \in B : \alpha I \subseteq I\}.$$

Note that $O_L(I)$ is always an order of B , even if I is not. Given an order O , a left fractional ideal of O is a lattice I for which $O \subseteq O_L(I)$, i.e. I admits multiplication on the left by O . The notion of right order and right fractional ideal can be similarly defined.

If $F = \mathbb{Q}$ or \mathbb{Q}_p , then an order O is always a dimension four $\mathcal{O}_F = \mathbb{Z}, \mathbb{Z}_p$ -module respectively. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be a basis of O , and define the discriminant of O to be

$$\text{disc}(O) = -d(\alpha_1, \alpha_2, \alpha_3, \alpha_4) := -\det(\text{trd}(\alpha_i \alpha_j)_{i,j}).$$

It turns out that this is always a square, so we define the reduced discriminant of O by

$$\text{discrd}(O)^2 = \text{disc}(O).$$

The reduced discriminant is only defined up to \mathcal{O}_F^\times , so over \mathbb{Q} we typically take the convention that it is positive, and over \mathbb{Q}_p we take it to be of the form p^e with $e \geq 0$. With these conventions, it follows that if $F = \mathbb{Q}$, then

$$\text{discrd}(O) = \prod_p \text{discrd}(O_p),$$

where the product is taken over all primes p and $O_p = O \otimes \mathbb{Z}_p$ is the corresponding local order in B_p . This product is well defined as $\text{discrd}(O_p) = 1$ for all but finitely many p .

Over $F = \mathbb{Q}$, an order is maximal if and only if the reduced discriminant is equal to the finite part of \mathfrak{D} , the discriminant of the quaternion algebra. A general order O will have $\text{discrd}(O) = \mathfrak{D}\mathfrak{M}$, where \mathfrak{M} is necessarily coprime to \mathfrak{D} , and is called the level of the order.

Working locally will be essential, so we will state the local-global correspondence for lattices, (in [Voi21] it is given in terms of localizations and not completions, but they are equivalent).

Theorem 4.1.1 (Theorem 9.5.1 of [Voi21]). *Let V be a finite dimensional \mathbb{Q} -vector space, and let $M \subset V$ be a \mathbb{Z} -lattice. Then the map $N \rightarrow (N_p)_p$ gives a bijection between \mathbb{Z} -lattices $N \subset V$ and collections of lattices $(N_p)_p$ indexed by the primes which satisfies $M_p = N_p$ for all but finitely many primes p .*

Since orders are lattices, we derive the following corollary.

Corollary 4.1.2. *Let M, N be orders in B . Then*

$$M = N \Leftrightarrow M_p = N_p \text{ for all primes } p.$$

An Eichler order O of B is an order that is the intersection of two (uniquely determined) maximal orders. Over $F = \mathbb{Q}_p$, if B is division there is exactly one maximal order, hence this is the only Eichler order. Otherwise, $B = \text{Mat}(2, \mathbb{Q}_p)$, and there exist Eichler orders of levels p^e for all $e \geq 0$. They are all conjugate, and we define the standard Eichler order of level p^e to be

$$\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}.$$

Following the local-global principle of orders, when $F = \mathbb{Q}$, an order O is Eichler if and only if O_p is Eichler for all primes p .

Over $F = \mathbb{Q}$, if B is indefinite, a consequence of strong approximation is that all Eichler orders of level \mathfrak{M} are conjugate over B^\times . Furthermore, all left fractional ideals I are principal, i.e. there exists a $c \in B$ for which $I = Oc$.

4.2 Normalizer of an Eichler order

Starting with an Eichler order O , we can produce more Eichler orders by conjugation. In this section we determine when this action is trivial. Assume that $F = \mathbb{Q}$ or $F = \mathbb{Q}_p$, and that B is a quaternion algebra over F .

Proposition 4.2.1. *Let $x \in B - F$. Then the set $C_B(x) := \{v \in B : vx = xv\}$ is an F -algebra and a two dimensional F -vector space spanned by $1, x$. We call it the centralizing algebra of x .*

Proof. This follows immediately from Proposition 7.7.8 of [Voi21]. □

Corollary 4.2.2. *Let $x_1, x_2 \in B^\times - F^\times$ have the same minimal separable polynomial. Then the set $C_B(x_1, x_2) := \{v \in B : vx_1 = x_2v\}$ is a two dimensional F -vector space.*

Proof. By Corollary 7.7.3 of [Voi21], the equality of the minimal polynomials of x_1, x_2 implies that there exists a $w \in B^\times$ with $wx_1w^{-1} = x_2$. Thus

$$v \in C_B(x_1, x_2) \Leftrightarrow vw^{-1}x_2 = x_2vw^{-1},$$

so the corollary follows from Proposition 4.2.1. \square

Definition 4.2.3. Let O be an order in B , and define the subgroup of $x \in B^\times$ for which $xOx^{-1} = O$ to be $N_{B^\times}(O)$, the normalizer group of the order O .

Definition 4.2.4. For $f \in \mathcal{O}_F$ and an order O in B , let $O_{N=f} := \{x \in O : \text{nrd}(x) = f\}$ be the set of elements of O of reduced norm f . Let O^{\min} be the set of $x \in O$ satisfying $x/f \notin O$ for all $f \in \mathcal{O}_F - \mathcal{O}_F^\times$. For $f \in \mathcal{O}_F$, let $O_{N=f}^{\min} := O^{\min} \cap O_{N=f}$.

Now, let's specialize to indefinite quaternion algebras over \mathbb{Q} .

Proposition 4.2.5. *Let B be an indefinite quaternion algebra over \mathbb{Q} and O an Eichler order of level \mathfrak{M} . Then the sets $O_{N=n}$ are non-empty for all non-zero integers n .*

Proof. By Eichler's theorem on norms (Theorem 28.5.1 of [Voi21]), there exists an integral $\alpha \in B^\times$ for which $\text{nrd}(\alpha) = n$. The proof of this (whose main ingredient is strong approximation for Eichler orders in an indefinite quaternion algebra) can be modified exactly like Corollary 28.5.4 of [Voi21] to produce an α in an Eichler order of level \mathfrak{M} . All such orders are conjugate, so an appropriate conjugate of α lies in $O_{N=n}$, as desired. \square

Proposition 4.2.6. *Let B be an indefinite quaternion algebra over \mathbb{Q} and let O be an Eichler order. For any $\alpha \in O$ with $\text{nrd}(\alpha) > 0$, factorize $\text{nrd}(\alpha) = p_1 p_2 \cdots p_r$ as a product of (not necessarily distinct) primes. Then there exists $\pi_1, \pi_2, \dots, \pi_r \in O$ with $\text{nrd}(\pi_i) = p_i$ for all i and $\alpha = \pi_1 \pi_2 \cdots \pi_r$.*

Proof. Theorem 11.4.8 of [Voi21] proves this over a maximal order in the Hamilton quaternions. The proof essentially works for all orders of class number 1: the only possible issue is we are only guaranteed that $\text{nrd}(\pi_i) = \pm p_i$ (which was not an issue over the Hamilton quaternions). Pick any $u \in O_{N=-1}$, and if i is the smallest index for which $\text{nrd}(\pi_i) = -p_i$, replace π_i by $\pi_i u$ and π_{i+1} by $u^{-1} \pi_{i+1}$. We repeat until $\text{nrd}(\pi_i) > 0$ for all $i < r$; since $0 < \text{nrd}(\alpha) = \prod_{i=1}^r \text{nrd}(\pi_i)$, it follows that $\text{nrd}(\pi_r) > 0$ as well, and the proposition follows. \square

Next, we describe the normalizer groups of Eichler orders over \mathbb{Q} and \mathbb{Q}_p .

Proposition 4.2.7. *Let B be a quaternion algebra over \mathbb{Q}_p with Eichler order O . If $B = \mathbb{Q}A_p^{\text{div}}$, we have*

$$N_{B^\times}(O) = B^\times.$$

Otherwise, write $B = \text{Mat}(2, \mathbb{Q}_p)$ and take $O = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$, the standard Eichler order of level p^e . Let $\omega := \begin{pmatrix} 0 & 1 \\ -p^e & 0 \end{pmatrix}$, and then we have

$$N_{B^\times}(O) = \mathbb{Q}_p^\times O^\times \langle \omega \rangle.$$

Proof. If B is division, then there is a unique maximal order, which must be O . Since conjugating it keeps the order maximal, it is stabilized under conjugation by all of B^\times . The proof for B not being division is Proposition 23.4.14 of [Voi21] (we have adjusted the definition of ω so that it has positive norm). \square

Note that if B is not division and O is maximal, then $N_{B^\times}(O) = \mathbb{Q}_p^\times O^\times$. Translating the above proposition into the global case yields the following proposition.

Proposition 4.2.8. *Let B be an indefinite quaternion algebra over \mathbb{Q} with discriminant \mathfrak{D} , and let O be an Eichler order of B of level \mathfrak{M} . Then there exists a collection of elements $\{\omega_p : p \mid \mathfrak{D}\mathfrak{M}\infty\}$ with $\text{nrd}(\omega_p) = p^{v_p(\mathfrak{D}\mathfrak{M})}$ for $p < \infty$ and $\text{nrd}(\omega_\infty) = -1$ for which*

$$\frac{N_{B^\times}(O)}{\mathbb{Q}^\times O_{N=1}^\times} = \langle \omega_p \rangle_{p \mid \mathfrak{D}\mathfrak{M}\infty} \simeq \prod_{p \mid \mathfrak{D}\mathfrak{M}\infty} \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

In particular, if O is maximal, then $x \in O^{\text{min}} \cap N_{B^\times}(O)$ if and only if all prime divisors of $\text{nrd}(x)$ are ramified in B .

Proof. By combining Proposition 18.5.3 and Equation 23.4.20 of [Voi21] with the fact that O has class number one, we get the isomorphism

$$\frac{N_{B^\times}(O)}{\mathbb{Q}^\times O^\times} \simeq \prod_{p \mid \mathfrak{D}\mathfrak{M}} \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

By taking a set of generators and looking locally, we can use Proposition 4.2.7 to show that we can find an equivalent set of generators $\{\omega_p\}_{p \mid \mathfrak{D}\mathfrak{M}}$ which satisfy $\text{nrd}(\omega_p) = p^{v_p(\mathfrak{D}\mathfrak{M})}$ for $p < \infty$. Finally, we can pull out the ∞ by using $O^\times = O_{N=1} \cup O_{N=-1}$ and $O_{N=-1} = \omega_\infty O_{N=1}$ for any $\omega_\infty \in O_{N=-1}$. \square

4.3 Towers of Eichler orders

Let $F = \mathbb{Q}_p$ and $B = \text{Mat}(2, \mathbb{Q}_p)$. The Bruhat-Tits tree provides a combinatorial aspect to the theory of maximal/Eichler orders of B . Vertices of the graph are maximal orders in B , and there exists an edge between O and O' if and only if $O \cap O'$ is an Eichler order of level p . A summary of the main facts of the graph (see Section 23.5 of [Voi21]) are:

- The graph is connected and has no cycles, hence it is a tree (as the name implies);
- Every vertex has degree $p + 1$;
- Let O_1, O_2 be maximal orders, and let $O = O_1 \cap O_2$ be the corresponding Eichler order of level p^e . Then O corresponds to the unique path between O_1 and O_2 . This path has length $e + 1$, and the vertices on the path are precisely the $e + 1$ maximal orders which contain O .

Focusing on one Eichler order O of level p^e , we can define the “inverted triangle” of superorders of O as follows:

- It is a graph consisting of all (necessarily Eichler) superorders $O' \supset O$ as vertices;
- The vertices are arranged into $e + 1$ rows, where the i^{th} row from the top (starting with row 0) consists of the Eichler orders of level p^i containing O .
- There is an edge between orders O_1, O_2 if and only if one order contains the other and they are in adjacent rows.

It follows directly from the Bruhat-Tits tree that there are $e + 1 - i$ vertices in the i^{th} row, and the graph can be drawn in the plane so that each vertex (besides those in row 0) is connected to the two closest vertices in the row above it. An Eichler order is the intersection of the two orders it is connected to in the above row. As an example, the inverted triangle for an Eichler order of level p^5 looks like Figure 4.1.

The inverted triangle of O allows one to easily count superorders of O of a specified level which do not contain certain given superorders (this will become necessary in Section 6).

Remark 4.3.1. The inverted triangle of O is essentially the same concept of branches of orders, as found in [AC13] and [AAC18].

4.4 Optimal embeddings

Let B be a quaternion algebra over $F = \mathbb{Q}, \mathbb{Q}_p$, and let O be an order in B . Let D be a discriminant (i.e. a non-square integer equivalent to 0 or 1 modulo 4), and let \mathcal{O}_D be the unique quadratic order of discriminant D , lying in $\mathbb{Q}(\sqrt{D})$.

Definition 4.4.1. An *embedding* of \mathcal{O}_D into O is a ring homomorphism $\phi : \mathcal{O}_D \rightarrow O$. Call the embedding *optimal* if

- $F = \mathbb{Q}$ and the embedding does not extend to an embedding of a larger order into O . If D is a fundamental discriminant, then all embeddings of \mathcal{O}_D into O are optimal.
- $F = \mathbb{Q}_p$, and the embedding does not extend to an embedding of \mathcal{O}_{D/p^2} . If D/p^2 is not a discriminant, then all embeddings of \mathcal{O}_D into O are optimal.

In particular, if $F = \mathbb{Q}$, an embedding ϕ into O is optimal if and only if the corresponding embeddings ϕ_p into O_p are optimal for all primes p .

Any optimal embedding $\phi_1 : \mathcal{O}_D \rightarrow O$ extends to a unique ring homomorphism $\phi : \mathbb{Q}(\sqrt{D}) \rightarrow B$, and any ring homomorphism $\phi : \mathbb{Q}(\sqrt{D}) \rightarrow B$ will descend to an embedding of any order inside $\phi^{-1}(O)$ to O . In particular, it corresponds to an optimal embedding of a unique order, $\phi^{-1}(O)$.

Definition 4.4.2. If K is a quadratic extension of \mathbb{Q} and $\phi : K \rightarrow B$ is a ring homomorphism, let D_O^ϕ denote the discriminant of $\phi^{-1}(O)$. Let $\phi_O := \phi|_{\phi^{-1}(O)}$ denote the optimal embedding associated to ϕ and O .

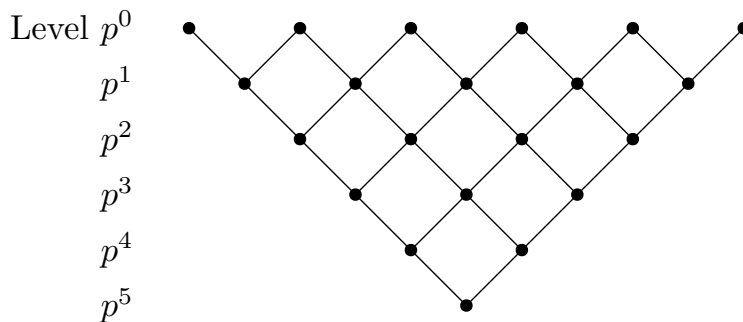


Figure 4.1: Inverted triangle of level p^5 .

For any $x \in B^\times$, let $\phi^x := x\phi x^{-1}$. If ϕ was an optimal embedding from \mathcal{O}_D to O , then ϕ^x remains so for $x \in O_{N=1}$. In general, the image of ϕ^x will not necessarily land inside O , and even if it does it may no longer be optimal. As such, we will often use ϕ_O^x for the optimal embedding associated to ϕ^x and O .

Definition 4.4.3. If ϕ_1, ϕ_2 are optimal embeddings of \mathcal{O}_D into O , we call them equivalent if there exists $r \in O_{N=1}$ for which $r\phi_1 r^{-1} = \phi_2$. The equivalence class of ϕ_1 is denoted $[\phi_1]$. Define the set of equivalence classes of optimal embeddings of \mathcal{O}_D into O to be $\text{Emb}(O, D)$.

As with tuples of hyperbolic matrices, we can extend the definition of equivalence to n -tuples of optimal embeddings as follows:

$$(\phi_1, \phi_2, \dots, \phi_n) \sim_n (\phi'_1, \phi'_2, \dots, \phi'_n)$$

if there exists an $r \in O_{N=1}$ such that $r\phi_i r^{-1} = \phi'_i$ for all $1 \leq i \leq n$.

As we shall see, if there exists an optimal embedding, then there are $h^+(D)$ classes of optimal embeddings, up to the notion of orientation. Studying this will be the focus of the next few sections.

Definition 4.4.4. For D an integer, define $p_D \in \{0, 1\}$ to be the parity of D . For D a discriminant, let the discriminant of $\mathbb{Q}(\sqrt{D})$ be D^{fund} .

Since $\mathcal{O}_D = \mathbb{Z} \left[\frac{p_D + \sqrt{D}}{2} \right]$, an embedding of \mathcal{O}_D into O is equivalent to picking an element $x = \phi \left(\frac{p_D + \sqrt{D}}{2} \right) \in O$ which has the same characteristic polynomial as $\frac{p_D + \sqrt{D}}{2}$, i.e. an element x satisfying $x^2 - p_D x + \frac{p_D - D}{4} = 0$.

We would like to determine when there exists an optimal embedding of a quadratic order into a quaternion order. The main result is the following theorem.

Theorem 4.4.5. *Let B be an indefinite quaternion algebra over \mathbb{Q} with discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} in B , and let D be a discriminant. Then there exists an embedding of \mathcal{O}_D into O if and only if the following holds:*

- for all $p \mid \mathfrak{D}$, we have $\left(\frac{D^{\text{fund}}}{p} \right) \neq 1$
- for all $p^e \parallel \mathfrak{M}$, at least one of the following holds:

- $\left(\frac{D^{\text{fund}}}{p}\right) = 1$;
- $e \leq v_p\left(\frac{D}{4}\right)$;
- $p = 2$ and $e = v_2\left(\frac{D}{4}\right) + 1$ and $v_2(D)$ is even;
- $p = 2$ and $e = v_2\left(\frac{D}{4}\right) + 2$ and D^{fund} is odd.

Furthermore, there exists an optimal embedding if and only if the condition $p \nmid \frac{D}{D^{\text{fund}}}$ for all $p \mid \mathfrak{D}$ is also satisfied.

Remark 4.4.6. When O is maximal, Theorem 4.4.5 takes a simpler form: all primes p ramifying in B must be ramified or split in \mathcal{O}_D , and they cannot divide $\frac{D}{D^{\text{fund}}}$ (for optimality).

Theorem 4.4.5 will be proved by studying the question locally, and using this to deduce the global answer.

4.4.1 Existence of optimal embeddings

We start by considering optimal embeddings into the division and non-division quaternion algebras over \mathbb{Q}_p .

Proposition 4.4.7. *Let $B = \text{QA}_p^{\text{div}}$, let D be a discriminant, and let O be the maximal order. Then there exists an embedding of \mathcal{O}_D into O if and only if we have $\left(\frac{D^{\text{fund}}}{p}\right) \neq 1$. Furthermore, any embedding of \mathcal{O}_D extends to an embedding of $\mathcal{O}_{D^{\text{fund}}}$.*

Proof. The first half of the proposition follows immediately from Proposition 30.5.3 of [Voi21]. For the final part, let ϕ give an embedding of \mathcal{O}_D . Since all elements of $\mathcal{O}_{D^{\text{fund}}}$ are integral, the same is true for $\phi(\mathcal{O}_{D^{\text{fund}}})$. As O is the set of integral elements, the result follows. \square

Proposition 4.4.8. *Let D be a discriminant, let $B = \text{Mat}(2, \mathbb{Q}_p)$, and let O be an Eichler order of level p^e in B . Then there exists an embedding of \mathcal{O}_D into O if and only if any of the following are satisfied:*

- $\left(\frac{D^{\text{fund}}}{p}\right) = 1$;
- $e \leq v_p\left(\frac{D}{4}\right)$;

- $p = 2$ and $e = v_2\left(\frac{D}{4}\right) + 1$ and $v_2(D)$ is even;
- $p = 2$ and $e = v_2\left(\frac{D}{4}\right) + 2$ and D^{fund} is odd.

Furthermore, if there exists an embedding, then there exists an optimal embedding.

Proof. Without loss of generality, we can take $O = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^e \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$, the standard Eichler order of level p^e .

If $e = 0$, then we can take ϕ defined by $\phi\left(\frac{pD + \sqrt{D}}{2}\right) = \begin{pmatrix} pD & \frac{D - pD}{4} \\ 1 & 0 \end{pmatrix}$, which clearly gives an optimal embedding.

Now assume that $e > 0$ and p is odd. An embedding is given by $\phi\left(\sqrt{D}\right) = \begin{pmatrix} a & b \\ p^e c & -a \end{pmatrix}$ for any $a, b, c \in \mathbb{Z}_p$ which satisfy $a^2 + bcp^e = D$. The embedding is optimal if and only if $p \nmid \gcd(a, b, c)$, and we see that if (a, b, c) give an embedding, then $(a, bc, 1)$ give an optimal embedding, which is the last statement. Such a triple (a, b, c) will exist if and only if there exists an $a \in \mathbb{Z}_p$ for which

$$p^e \mid D - a^2.$$

If $v_p(D) = v_p(D/4) \geq e$, this is true for $a = 0$. Otherwise, assume $v_p(D) < e$. Write $D = D^{\text{fund}} g^2 p^{2k}$ for some positive integer g coprime to p and non-negative integer k , with $2k < e$. Then we necessarily have $p^k \mid a$ in any solution, so we reduce to solving $p^{e-2k} \mid g^2 D^{\text{fund}} - a'^2$. If $p \mid D^{\text{fund}}$, then $e \geq v_p(D) + 1 = 2k + 2$, and we have no solution as $v_p(g^2 D^{\text{fund}} - a'^2) \leq 1$. Otherwise, this has a solution if and only if D^{fund} is a square modulo p , which completes the claim for p odd.

For $p = 2$, see Proposition A.2.1 □

To compile these local propositions into a global one, we need a version of the local-global principle.

Lemma 4.4.9. *Let B be a quaternion algebra over \mathbb{Q} , let O be an Eichler order of level \mathfrak{M} , and let D be a discriminant. Then there exists an (optimal) embedding of \mathcal{O}_D into O if and only if there exists (optimal) embeddings of \mathcal{O}_D into O_p for all finite primes p and an embedding of \mathcal{O}_D into B_∞ .*

Proof. The necessity of the conditions are immediate, so we need to check that they are sufficient. For each place v , let ϕ_v be a corresponding (optimal) embedding into O_v (where

$O_\infty = B_\infty$). By the local-global principle for embeddings of quadratic fields ([Voi21], Proposition 14.6.7), there exists an embedding $\varphi : \mathcal{O}_D \rightarrow B$.

Since $\varphi(\mathcal{O}_D)$ is integral, pick any maximal order R containing it. For all finite primes p , we define orders T_p of B_p as follows:

- If $p \nmid \mathfrak{M}$, define $T_p = R_p$
- If $p \mid \mathfrak{M}$, then as all embeddings are conjugate over B_p^\times , there exists an $x_p \in B_p^\times$ for which $x_p \phi_p x_p^{-1} = \varphi_p$. Then φ_p gives an (optimal) embedding into $T_p = x_p O_p x_p^{-1}$.

By Theorem 4.1.1, there exists an order T of B that completes to the T_p at all primes p . In particular, we see that φ gives an (optimal) embedding into T , and that T is also an Eichler order of level \mathfrak{M} . All such orders are conjugate, so there exists a $y \in B^\times$ which satisfies $yTy^{-1} = O$. Then $\phi = \varphi^y$ is an (optimal) embedding of \mathcal{O}_D into O . □

Theorem 4.4.5 is now an easy corollary of the above results.

Proof of Theorem 4.4.5. By Lemma 4.4.9, it suffices to do local calculations. There will be an embedding into B_∞ as B is indefinite, and Propositions 4.4.7 and 4.4.8 cover the completions at finite primes. □

In certain proofs, it will be useful to assume that an optimal embedding takes a certain form. The following lemma allows us to do this.

Lemma 4.4.10 (Exercise 2.5 of [Voi21]). *Let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over a field F of characteristic not equal to 2, and assume $x \in B^\times$ is an element with trace 0 and reduced norm $n \in F^\times$. Then there exists an $m \in F^\times$ and an isomorphism $\theta : B \rightarrow \left(\frac{-n,m}{F}\right)$ satisfying $\theta(x) = i$.*

Proof. Consider the inner product defined as $\langle u, v \rangle = \frac{1}{2} \text{trd}(u\bar{v})$. Pick any y such that $B = F(x, y)$, and by applying the Gram-Schmidt orthogonalization process, we can assume that $0 = \langle 1, y \rangle = \langle x, y \rangle$. This implies that $y^2 = m \in F^\times$ and $xy = -yx$, whence we have the result. □

Corollary 4.4.11. *Let $\phi : \mathcal{O}_D \rightarrow O$ be an (optimal) embedding into an order of the quaternion algebra B . Then there exists a quaternion algebra B' with order O' and an isomorphism $\theta : B \rightarrow B'$ taking O to O' such that $\theta \circ \phi : \mathcal{O}_D \rightarrow O'$ is an (optimal) embedding with $\theta \circ \phi(\sqrt{D}) = i_{B'}$. In particular, given an (optimal) embedding, we can choose coordinates so that the image of \sqrt{D} is i .*

Proof. Take $x = \phi(\sqrt{D})$ in Lemma 4.4.10, and consider the corresponding map θ . Let $O' = \theta(O)$, and then O' is an isomorphic order for which $\theta \circ \phi$ is an (optimal) embedding into. \square

4.4.2 Orientations of optimal embeddings

Fix B to be an indefinite quaternion algebra over \mathbb{Q} with discriminant \mathfrak{D} and Eichler order O of level \mathfrak{M} . Let D be a discriminant and $\phi_i : \mathcal{O}_D \rightarrow O$ optimal embeddings of the order of discriminant D for $i = 1, 2$. For every place v of \mathbb{Q} , let $\phi_{i,v}$ be the composition of ϕ_i with completing at v . If $\phi_1 \sim \phi_2$, then clearly $\phi_{1,v} \sim \phi_{2,v}$ for all places v , though the opposite notion need not be true (in fact, it will be true if and only if $h^+(D) = 1$).

Definition 4.4.12. Let $o_v(\phi)$ denote the (local) equivalence class of ϕ_v . The orientation of an optimal embedding $\phi : \mathcal{O}_D \rightarrow O$ is $o(\phi) = (o_v(\phi))_v$, the set of equivalence classes of the corresponding local embeddings (v runs over all places).

Definition 4.4.13. For each possible orientation o of an optimal embedding of \mathcal{O}_D into O , we denote by $\text{Emb}_o(O, D)$ the equivalence classes of optimal embeddings with orientation o .

Thus the orientation of an optimal embedding measures the local information coming from the embedding. The behaviour of the local orientations is summarized in the next proposition.

Proposition 4.4.14. *Assume that $\text{Emb}(O, D)$ is non-empty. Then,*

1. *If $B = O = \text{Mat}(2, \mathbb{R})$,*
 - *if $D > 0$, then $|\text{Emb}(O, D)| = 1$.*
 - *if $D < 0$, then $|\text{Emb}(O, D)| = 2$.*

2. If $B = \mathbb{Q}A_p^{\text{div}}$ with maximal order O ,
 - if $p \mid D$, then $|\text{Emb}(O, D)| = 1$.
 - if $p \nmid D$, then $|\text{Emb}(O, D)| = 2$.
3. If $B = \text{Mat}(2, \mathbb{Q}_p)$ and O is an Eichler order of level p^e ,
 - if $e = 0$, then $|\text{Emb}(O, D)| = 1$.
 - if $e > 0$ and $p \nmid D$, then $|\text{Emb}(O, D)| = 2$.

Proof. See sections 30.5 and 30.6 of [Voi21]. □

The above proposition is missing the case of $B = \text{Mat}(2, \mathbb{Q}_p)$, O is an Eichler order of level p^e with $e > 0$ and $p \mid D$. In this case, there are various cases corresponding to the valuations of D, \mathfrak{M} at p , and it becomes much more complicated. For simplicity of exposition, we will omit this case. If desired, see Lemma 30.6.17 of [Voi21] for the details.

Now consider an optimal embedding $\phi : \mathcal{O}_D \rightarrow O$, where we are working globally. If $v \nmid \mathfrak{DM}\infty$, then $\text{Emb}(O_v, D)$ is trivial. Thus when we consider the orientation of ϕ , it suffices to consider it only at places $v \mid \mathfrak{DM}\infty$. Furthermore, as long as $\gcd(D, \mathfrak{M}) = 1$, there are only one or two orientations at each local place, so we can represent a local orientation as either ± 1 if there are two, or as 0 if there is one. Note that the choice of ± 1 is *not canonical*. If $v < \infty$, then fixing the local orientation of one optimal embedding of \mathcal{O}_D will fix it for all optimal embeddings of \mathcal{O}_{Dk^2} with $\text{ord}_v(k) = 0$ *only*. If $v = \infty$, then fixing the local orientation of one embedding of a negative quadratic order will fix it for *all* embeddings of negative quadratic orders.

While the description of an orientation as a collection of local data is nice, it will be useful to have more tangible interpretations. We start with $v = \infty$. Fix an inclusion map $\iota : B \rightarrow \text{Mat}(2, \mathbb{R})$, for example,

$$\iota : e + fi + gj + hk \rightarrow \begin{pmatrix} e + f\sqrt{a} & b(g + h\sqrt{a}) \\ g - h\sqrt{a} & e - f\sqrt{a} \end{pmatrix},$$

where we are assuming that $a > 0$.

We can assume that $D < 0$, and thus the equation $\iota(\phi(\sqrt{D}))x = x$ has two solutions that are complex conjugates of each other. Using the algebraic definition of first root as found in Section 2.1, we call ϕ *positive definite* if the first root of $\iota(\phi(\sqrt{D}))$ lies in the upper half plane, and *negative definite* otherwise.

Definition 4.4.15. The orientation of ϕ at $v = \infty$ is

$$o_\infty(\phi) := \begin{cases} 1 & \text{if } \phi \text{ is positive definite;} \\ -1 & \text{if } \phi \text{ is negative definite;} \\ 0 & \text{if } D > 0. \end{cases}$$

The following lemma shows that this definition agrees with the previous notion of orientation, and that conjugating by an element of $O_{N=-1}$ will swap orientation.

Lemma 4.4.16. *Let $u \in O_{N=\pm 1}$. Then*

$$o_\infty(\phi^u) = \text{nr}(u)o_\infty(\phi).$$

Proof. Conjugation in $\text{GL}(2, \mathbb{R})$ by an element of $\text{SL}(2, \mathbb{R})$ preserves the half plane of the first root. It is an easy calculation that conjugation by an element with determinant -1 swaps the half planes, and the result follows. \square

Next, if $p \mid \mathfrak{D}$ and $p \nmid D$, then by Proposition 4.4.7 p is inert with respect to \mathcal{O}_D . Pick reduction maps

$$\pi_1 : \mathcal{O}_D \rightarrow \mathbb{F}_{p^2}, \quad \pi_2 : \mathcal{O}_D \xrightarrow{\phi} \mathcal{O} \rightarrow \mathcal{O}_p \rightarrow \mathbb{F}_{p^2},$$

where for the first map we reduce modulo p , and for the second map we tensor \mathcal{O} by with \mathbb{Z}_p and reduce via the unique maximal ideal. By lifting from \mathbb{F}_{p^2} to \mathcal{O}_D via π_1^{-1} and composing with π_2 , we get an automorphism $\pi_2\pi_1^{-1} : \mathbb{F}_{p^2} \rightarrow \mathbb{F}_{p^2}$. There are two such automorphisms, namely the identity and conjugation.

Definition 4.4.17. The orientation of ϕ at p is

$$o_p(\phi) := \begin{cases} 1 & \text{if } \pi_2\pi_1^{-1} \text{ is the identity;} \\ -1 & \text{if } \pi_2\pi_1^{-1} \text{ is non-trivial;} \\ 0 & \text{if } p \mid D. \end{cases}$$

Lemma 4.4.18 shows that this definition agrees with the previous notion of orientation.

Lemma 4.4.18. *If $\phi : \mathcal{O}_D \rightarrow O_p$ is an optimal embedding and $x \in O_p$ is non-zero, then*

- $o_p(\phi^x) = o_p(\phi)$ if $v_p(\text{nrd}(x))$ is even;
- $o_p(\phi^x) = -o_p(\phi)$ if $v_p(\text{nrd}(x))$ is odd.

Proof. If $p \mid D$ the result is trivial, so assume otherwise. By dividing x by powers of p , we can assume that $v_p(\text{nrd}(x)) = 0, 1$.

If $\text{nrd}(x)$ is coprime to p , then in the construction of $\pi_2\pi_1^{-1}$ for ϕ^x , we apply ϕ , conjugate by x , and then reduce modulo the unique maximal ideal \mathfrak{p} . Since $\text{nrd}(x)$ is coprime to p , the reduction $x \pmod{\mathfrak{p}}$ is invertible, hence we can do the conjugation after reducing. But then we are working in \mathbb{F}_{p^2} , which is commutative, hence we have the same map, and the same orientation.

Now assume that $p \parallel \text{nrd}(x)$. Write $B_p = \begin{pmatrix} p & \varepsilon \\ \varepsilon & p \end{pmatrix}$ with $\begin{pmatrix} \varepsilon \\ p \end{pmatrix} = -1$; by writing $x = yi$ with $\text{nrd}(y)$ coprime to p , we see that it suffices to prove the statement for $x = i$. Letting $\phi\left(\frac{pD+\sqrt{D}}{2}\right) = \frac{pD+fi+gj+hk}{2}$, we calculate that $\phi^i\left(\frac{pD+\sqrt{D}}{2}\right) = \frac{pD+fi-gj-hk}{2}$, whence

$$\phi\left(\frac{pD+\sqrt{D}}{2}\right) - \phi^i\left(\frac{pD+\sqrt{D}}{2}\right) = gj + hk \equiv gj \not\equiv 0 \pmod{\mathfrak{p}},$$

as if $p \mid g$ we would have $p \mid D$, contradiction. Therefore the image of $\frac{pD+\sqrt{D}}{2}$ under ϕ and ϕ^i reduce to different things modulo \mathfrak{p} , and so they have opposite orientation. \square

If $p \mid \mathfrak{M}$ and $p \nmid D$, let $\phi_p(\sqrt{D}) = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, where we are assuming that we map to the standard Eichler order of level \mathfrak{M} . Therefore $a^2 + bc = D$, and thus $a^2 \equiv D \pmod{p}$.

Definition 4.4.19. Pick a_1 such that $a_1^2 \equiv D \pmod{2p}$. The orientation of ϕ at p is

$$o_p(\phi) := \begin{cases} 1 & \text{if } a \equiv a_1 \pmod{2p}; \\ -1 & \text{otherwise.} \end{cases}$$

If $p > 2$ we note that the orientation corresponds to $a \pmod{p}$, and at $p = 2$ it corresponds to $a \pmod{4}$. Alternatively, it corresponds to $(\phi_p(\frac{pD+\sqrt{D}}{2}))_{1,1} \pmod{p}$ for all p . Lemma 4.4.20 shows that this definition agrees with the previous notion of orientation.

Lemma 4.4.20. *Let $\phi : \mathcal{O}_D \rightarrow O_p$ be an optimal embedding into the standard Eichler order of level p^e , where $e > 0$ and $p \nmid D$. If $x \in O_p$, then*

- $o_p(\phi^x) = o_p(\phi)$ if $\text{nrd}(x)$ is coprime to p ;
- $o_p(\phi^x) = -o_p(\phi)$ if $x = \omega = \begin{pmatrix} 0 & 1 \\ -p^e & 0 \end{pmatrix}$;
- if $o_p(\phi^x) = -o_p(\phi)$, then $\omega^{-1}x \in O_p$.

Proof. Let $\phi\left(\frac{p_D + \sqrt{D}}{2}\right) = \begin{pmatrix} a & b \\ c & p_D - a \end{pmatrix}$, let $x = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, and first assume that $p \nmid \text{nrd}(x) = eh - gf$.

We calculate that

$$\begin{aligned} \left(\phi^x \left(\frac{p_D + \sqrt{D}}{2} \right) \right)_{1,1} &\equiv \frac{1}{eh} \left(\begin{pmatrix} e & f \\ 0 & h \end{pmatrix} \begin{pmatrix} a & b \\ 0 & p_D - a \end{pmatrix} \begin{pmatrix} h & -f \\ 0 & e \end{pmatrix} \right)_{1,1} \pmod{p} \\ &\equiv a \pmod{p}, \end{aligned}$$

which implies that ϕ and ϕ^x have the same orientation.

If $x = \omega$, we calculate that

$$\phi^x \left(\frac{p_D + \sqrt{D}}{2} \right) = \begin{pmatrix} p_D - a & -c/p^e \\ -bp^e & a \end{pmatrix}.$$

Thus $\phi(\sqrt{D})_{1,1} = 2a - p_D = -(p_D - 2a) = -\phi^x(\sqrt{D})$, which implies the second result.

For the last point, we have $o_p(\phi^x) = -o_p(\phi) = o_p(\phi^\omega)$, hence ϕ^x and ϕ^ω are equivalent optimal embeddings (if they were not, then $|\text{Emb}(O_p, D)| \geq 3$, which is a contradiction).

Therefore there exists a $z \in O_p$ with $\text{nrd}(z) = 1$ for which

$$\omega^{-1}zx\phi(\omega^{-1}zx)^{-1} = \phi,$$

and by Proposition 4.2.1, we can write $zx = A\omega + B\omega\phi\left(\frac{p_D + \sqrt{D}}{2}\right)$ for some $A, B \in \mathbb{Q}_p$.

Explicitly,

$$zx = \begin{pmatrix} cB & A + (p_D - a)B \\ p^e(-A - aB) & -p^e bB \end{pmatrix} \in O_p,$$

whence $A + (p_D - a)B, A + aB \in \mathbb{Z}_p$. Subtracting yields $(2a - p_D)B \in \mathbb{Z}_p$, and we note that

$$(2a - p_D)^2 = (\phi(\sqrt{D})_{1,1})^2 \equiv D \pmod{p}.$$

Therefore $2a - p_D$ is coprime to p , so $B \in \mathbb{Z}_p$, and $A \in \mathbb{Z}_p$ follows as well. This implies that $x \in z^{-1}\omega O_p = \omega O_p$, as required. \square

Computationally, given embeddings ϕ_1, ϕ_2 , we would like to be able to tell which primes they differ in orientation at. The following proposition does the trick.

Proposition 4.4.21. *Let $\phi_1, \phi_2 : \mathcal{O}_D \rightarrow O$ be optimal embeddings, and p a finite prime which divides \mathfrak{DM} but does not divide $\gcd(D, \mathfrak{M})$. Then ϕ_1, ϕ_2 have the same orientation at p if and only if*

$$p \mid \text{nrd} \left(\phi_1 \left(\frac{p_D + \sqrt{D}}{2} \right) - \phi_2 \left(\frac{p_D + \sqrt{D}}{2} \right) \right),$$

or, equivalently,

$$p^{1+2v_2(p)} \mid \text{nrd} \left(\phi_1(\sqrt{D}) - \phi_2(\sqrt{D}) \right).$$

They have opposite orientations if and only if $p \nmid D$ and

$$p^{1+2v_2(p)} \mid \text{nrd}(\phi_1(\sqrt{D}) + \phi_2(\sqrt{D})).$$

Proof. It suffices to prove this proposition locally. First, consider the case of $p \mid \mathfrak{D}$; let \mathfrak{p} be the unique maximal ideal of O_p . If $p \mid D$ the conclusion is clear, and otherwise by Definition 4.4.17, ϕ_1, ϕ_2 have the same orientation if and only if the images of $\frac{p_D + \sqrt{D}}{2}$ are the same modulo \mathfrak{p} . This completes the first claim in this case.

Next, assume that $p \mid \mathfrak{M}$; thus $p \nmid D$. Assume that $M_i := \phi_{i,p} \left(\frac{p_D + \sqrt{D}}{2} \right) = \begin{pmatrix} a_i & b_i \\ c_i & p_D - a_i \end{pmatrix}$ ($i = 1, 2$) inside the standard Eichler order of level \mathfrak{M} in $\text{Mat}(2, \mathbb{Q}_p)$. By Definition 4.4.19, the orientations of ϕ_1, ϕ_2 are the same if and only if $a_1 \equiv a_2 \pmod{p}$. Since $p \mid c_1 - c_2$, we also see that $p \mid \text{nrd}(M_1 - M_2)$ if and only if $p \mid a_1 - a_2$, which completes the first claim.

The second equation follows directly from the first. The final part of the proposition follows from similar arguments to above. \square

Now that we have a good understanding of orientation, we will examine how the standard involution and conjugation affect it.

Proposition 4.4.22. *Let $\phi : \mathcal{O}_D \rightarrow O$ be an optimal embedding. Then $\bar{\phi} : \mathcal{O}_D \rightarrow O$ defined by $\bar{\phi}(x) = \overline{\phi(x)}$ is an optimal embedding with orientation $-o(\phi)$.*

Proof. The embedding $\bar{\phi}$ is clearly optimal, so we just need to check the orientation. Note that $\bar{\phi}(\sqrt{D}) = -\phi(\sqrt{D})$, so by Proposition 4.4.21, the result follows for the finite primes. At ∞ , the result follows from Definition 4.4.15. \square

Proposition 4.4.23. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} with Eichler order O of level \mathfrak{M} , let $\phi : \mathcal{O}_D \rightarrow O$ be an optimal embedding, and take $\omega_p \in N_B^\times(O)$ for $p \mid \mathfrak{D}\mathfrak{M}\infty$ as in Proposition 4.2.8. Then we have*

- $o_v(\phi^{\omega_p}) = o_v(\phi)$ for all places $v \neq p$;
- $o_p(\phi^{\omega_p}) = -o_p(\phi)$ if $p \nmid \gcd(D, \mathfrak{M})$.

In other words, the optimal embedding ϕ^{ω_p} only swaps orientation at p .

Proof. This follows immediately from Lemmas 4.4.16, 4.4.18, 4.4.20. □

Remark 4.4.24. When $\gcd(D, \mathfrak{M}) = 1$, by successively conjugating an embedding by the elements ω_p for $p \mid \mathfrak{D}\mathfrak{M}\infty$, we can pass between all possible orientations.

4.5 Action of the narrow class group on optimal embeddings

Let B be a quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} with Eichler order O of level \mathfrak{M} , and let ϕ_1, ϕ_2 be optimal embeddings of \mathcal{O}_D into O . Let $e_i = \phi_i(\sqrt{D})$ for $i = 1, 2$, and Corollary 4.2.2 implies that the set

$$S_{\phi_1, \phi_2}^B := \{v \in B : v\phi_1 = \phi_2v\} = \{v \in B : ve_1 = e_2v\}$$

is a two dimensional \mathbb{Q} -vector space. When we restrict to O , we define

$$S_{\phi_1, \phi_2}^O := S_{\phi_1, \phi_2}^B \cap O,$$

which is a 2 dimensional \mathbb{Z} -module, say with basis v_1, v_2 . Define the (integral) quadratic form

$$Q_{\phi_1, \phi_2}(X, Y) := \text{nrd}(Xv_1 + Yv_2);$$

note that this depends on (v_1, v_2) , though we do not include this in the notation. Working with Q_{ϕ_1, ϕ_2} thus implicitly implies that we are working both with the embeddings and a chosen basis. Different choices of basis (v_1, v_2) will translate Q_{ϕ_1, ϕ_2} by an element of $\text{GL}(2, \mathbb{Z})$.

We wish to orient the basis of S_{ϕ_1, ϕ_2}^O so that Q_{ϕ_1, ϕ_2} is well defined up to $\mathrm{SL}(2, \mathbb{Z})$, and thus $[Q_{\phi_1, \phi_2}]$ only depends on ϕ_1, ϕ_2 and not on the basis.

The discriminant of Q_{ϕ_1, ϕ_2} is $(v_2\bar{v}_1 - v_1\bar{v}_2)^2$, which motivates considering the quantity $v_2\bar{v}_1 - v_1\bar{v}_2$. Indeed, this quantity is invariant under $\mathrm{SL}(2, \mathbb{Z})$, and negates itself under a $\mathrm{GL}(2, \mathbb{Z})$ transformation with determinant -1 . Using the identities $v_i e_1 = e_2 v_i$ and $e_1 \bar{v}_i = \bar{v}_i e_2$ for $i = 1, 2$ (the second follows from conjugating the first, and using that $\bar{e}_i = -e_i$), we calculate

$$e_2 v_2 \bar{v}_1 = v_2 e_1 \bar{v}_1 = v_2 \bar{v}_1 e_2.$$

Thus by Proposition 4.2.1, we must have $v_2 \bar{v}_1 = A_1 + A_2 e_2$ for some rational numbers A_1, A_2 . Since $v_2 \bar{v}_1 \in O$, it follows that $A_1 + A_2 e_2 \in \mathbb{Z} + \frac{pD+e_2}{2}\mathbb{Z}$, using the fact that e_2 descends to an optimal embedding into O . In particular, $2A_1, 2A_2 \in \mathbb{Z}$. We see that

$$v_1 \bar{v}_2 = \overline{v_2 \bar{v}_1} = A_1 - A_2 e_2,$$

whence $V = v_2 \bar{v}_1 - v_1 \bar{v}_2 = 2A_2 e_2 = A e_2$, where $A = 2A_2$ is a non-zero integer. Before going further, we can already describe the orientation of the basis.

Definition 4.5.1. With the notation as above, (v_1, v_2) is said to be an oriented \mathbb{Z} -module basis of S_{ϕ_1, ϕ_2}^O if $v_2 \bar{v}_1 - v_1 \bar{v}_2 = A \phi_2(\sqrt{D})$ where A is a *positive* integer. With this choice, the $\mathrm{SL}(2, \mathbb{Z})$ equivalence class of Q_{ϕ_1, ϕ_2} is well defined.

If $u_1, u_2 \in O_{N=1}$, then we have

$$S_{\phi_1^{u_1}, \phi_2^{u_2}}^O = u_2 S_{\phi_1, \phi_2}^O u_1^{-1},$$

whence $[Q_{\phi_1^{u_1}, \phi_2^{u_2}}] = [Q_{\phi_1, \phi_2}]$. That is, the quadratic form equivalence class is also well defined over equivalence classes of embeddings. The key results about Q_{ϕ_1, ϕ_2} are summarized in the following proposition, which will be proved in Section 4.5.1.

Proposition 4.5.2. *Let ϕ_1, ϕ_2 be optimal embeddings from \mathcal{O}_D to O . Then*

- (i) *if $o(\phi_1) = o(\phi_2)$, then Q_{ϕ_1, ϕ_2} is a primitive form of discriminant D , which is positive definite if $D < 0$.*
- (ii) *if ϕ_1, ϕ_2 differ in orientation at the finite primes q_1, \dots, q_s , where $q_i \nmid \gcd(D, \mathfrak{M})$ for all i , then Q_{ϕ_1, ϕ_2} is equal to a primitive form of discriminant D times $\prod_{i=1}^s q_i^{v_{q_i}(\mathfrak{M})}$.*

(iii) if ϕ_1, ϕ_2 differ in orientation at ∞ , then Q_{ϕ_1, ϕ_2} is negative definite.

(iv) If $\alpha \in N_{B^\times}(O)$ and ϕ_1, ϕ_2 have the same orientation, then we have

$$[Q_{\phi_1, \phi_2}] = [Q_{\phi_1^\alpha, \phi_2^\alpha}],$$

i.e. the group action commutes with conjugation by elements in $N_{B^\times}(O)$.

(v) If $\alpha \in O_{N=-1}$, then we have

$$[Q_{\phi_1^\alpha, \phi_2^\alpha}(X, Y)] = [-Q_{\phi_1, \phi_2}(X, -Y)].$$

Proposition 4.5.2 produces a quadratic form out of two optimal embeddings, but does not give a recipe to produce an optimal embedding given a quadratic form and an initial optimal embedding.

Definition 4.5.3. Let ϕ be an optimal embedding of \mathcal{O}_D into O representing the equivalence class $[\phi] \in \text{Emb}(O, D)$, and let $g \in \text{Cl}^+(D)$ be an element of the narrow class group.

- Take a proper fractional ideal I representing g in $\text{Cl}^+(D)$ such that $v_p(\text{Nm}(I)) = 0$ for all $p \mid \mathfrak{DM}$.
- Form the left ideal $I_O := O\phi(I)$ in O .
- As B is indefinite, all left ideals of a maximal order are principal, so write $I_O = Oc_I$ for a $c_I \in B$ of positive norm.
- Define the optimal embedding $\phi_I = c_I\phi c_I^{-1}$, and the action of g on $[\phi]$ to be $g \cdot [\phi] := [\phi_I]$.

In Section 4.5.2 we will prove that the above is well-defined, independent of all choices, and is a group action.

The main result about the action of the class group on optimal embeddings is the following theorem.

Theorem 4.5.4. *Let D be a discriminant for which $|\text{Emb}(O, D)|$ is non-empty, and let o be a fixed orientation. Then the action of $\text{Cl}^+(D)$ on $\text{Emb}_o(O, D)$ as described in Definition 4.5.3 is simply transitive. Furthermore, we have*

$$Q_{\phi_1, \phi_2} \cdot [\phi_1] = [\phi_2],$$

i.e. the action is consistent with the definition of Q_{ϕ_1, ϕ_2} .

Theorem 4.5.4 immediately implies the following corollary.

Corollary 4.5.5. *If $\gcd(D, \mathfrak{M}) = 1$, then the set $\text{Emb}(O, D)$ is a finite set of size*

$$h^+(D)(1 + \mathbf{1}_{D < 0}) \prod_{p|\mathfrak{D}} \left(1 - \left(\frac{D}{p}\right)\right) \prod_{p|\mathfrak{M}} \left(1 + \left(\frac{D}{p}\right)\right).$$

Furthermore, for any valid orientation o , the set $\text{Emb}_o(O, D)$ has size $h^+(D)$, and the narrow class group $\text{Cl}^+(D)$ acts simply transitively on it.

The results of Corollary 4.5.5 are not new, for example see Example 30.7.4 of [Voi21]. However, they are typically derived adelicly, whereas it is important for us to have very explicit interpretations.

Remark 4.5.6. The set $\text{Emb}_o(O, D)$ carries extra natural automorphisms, i.e. in addition to the ones coming from the narrow class group action. Indeed, conjugation by the element ω_p where $p \mid \mathfrak{D}$ (or ω_∞ when $D > 0$) will not change the orientation of an embedding, and will be an involution.

4.5.1 Determining the quadratic form

This section is devoted to proving Proposition 4.5.2 through a series of lemmas.

Lemma 4.5.7. *Let ϕ_1, ϕ_2 have the same orientation. Then the quadratic form Q_{ϕ_1, ϕ_2} is primitive, and is positive definite if $D < 0$.*

Proof. For the primitiveness, it suffices to show that for all finite primes p , there exists integers x, y such that $p \nmid Q_{\phi_1, \phi_2}(x, y) = \text{nr}_d(xv_1 + yv_2)$. Since we have

$$S_{\phi_1, \phi_2}^{O_p} = \{v \in O_p : v\phi_1 = \phi_2 v\} = S_{\phi_1, \phi_2}^O \otimes \mathbb{Z}_p = \mathbb{Z}_p v_1 \oplus \mathbb{Z}_p v_2,$$

it suffices to show that there exists an $\alpha \in S_{\phi_1, \phi_2}^{O_p}$ for which $p \nmid \text{nr}_d(\alpha)$. But ϕ_1, ϕ_2 have the same orientation at p , whence they are locally conjugate by an element of norm 1, and the result follows.

If $D < 0$, the definiteness follows from Lemma 4.4.16. □

Lemma 4.5.8. *If ϕ_1, ϕ_2 differ in orientation at the finite primes q_1, \dots, q_s , where $q_i \nmid \gcd(D, \mathfrak{M})$ for all i , then Q_{ϕ_1, ϕ_2} is equal to a primitive quadratic form multiplied by $\prod_{i=1}^s q_i^{v_{q_i}(\mathfrak{M})}$. If $D < 0$, then Q_{ϕ_1, ϕ_2} is negative definite if ϕ_1, ϕ_2 have opposite orientations at ∞ .*

Proof. Let $x = \prod_{i=1}^s \omega_{q_i}$, and then ϕ_1^x, ϕ_2 have the same orientation by Proposition 4.4.23. It is clear that

$$S_{\phi_1, \phi_2}^O \supseteq S_{\phi_1^x, \phi_2}^O x;$$

we would like to show equality (which would prove the claim for $D > 0$). If $z \in S_{\phi_1, \phi_2}^O$, then Lemmas 4.4.18 and 4.4.20 show that $x^{-1}z \in O$ necessarily. Since $x \in N_{B^\times}(O)$, we also have $zx^{-1} \in O$. If (v_1, v_2) is an oriented basis of $S_{\phi_1^x, \phi_2}^O$, then we can write $z = Av_1x + Bv_2x$ for some $A, B \in \mathbb{Q}$. Therefore $zx^{-1} = Av_1 + Bv_2 \in O$, whence $A, B \in \mathbb{Z}$, and therefore a basis of S_{ϕ_1, ϕ_2}^O is (v_1x, v_2x) . This is properly oriented since $x\bar{x} = \text{nr}(x) > 0$.

If ϕ_1, ϕ_2 have opposite orientations at ∞ , the definiteness follows from Lemma 4.4.16. \square

Recall that we took (v_1, v_2) to be an ordered basis of S_{ϕ_1, ϕ_2}^O , and wrote $v_2\bar{v}_1 = A_1 + A_2e_2 \in \mathbb{Z} + \frac{pD+e_2}{2}\mathbb{Z}$. In particular,

$$\begin{aligned} D \text{ even} &\Rightarrow A_1 \in \mathbb{Z}, A_2 \in \frac{1}{2}\mathbb{Z}; \\ D \text{ odd} &\Rightarrow A_1, A_2 \in \frac{1}{2}\mathbb{Z} \text{ and } 2A_1 \equiv 2A_2 \pmod{2}. \end{aligned}$$

Lemma 4.5.9. *If ϕ_1, ϕ_2 have the same orientation, then Q_{ϕ_1, ϕ_2} has discriminant D .*

Proof. The discriminant of Q_{ϕ_1, ϕ_2} is

$$(v_2\bar{v}_1 - v_1\bar{v}_2)^2 = (2A_2e_2)^2 = (2A_2)^2D,$$

whence it suffices to show that $A = 2A_2$ has no prime divisors. Assume that $p \mid 2A_2$ for some prime p . First, note that

$$Q_{\phi_1, \phi_2}(X, Y) = \text{nr}(v_1)X^2 + 2A_1XY + \text{nr}(v_2)Y^2,$$

so by Lemma 4.5.7, $p \nmid \gcd(\text{nr}(v_1), 2A_1, \text{nr}(v_2))$. We first claim that one of $\text{nr}(v_1), \text{nr}(v_2)$ is coprime to p . Indeed, assume that $p \mid \text{nr}(v_1), \text{nr}(v_2)$, and

- if $p = 2$, then $2 \mid 2A_2$, i.e. A_2 is an integer. By our above comments, A_1 is also an integer, and thus $2 \mid 2A_1$. But now $2 \mid \gcd(\text{nrd}(v_1), 2A_1, \text{nrd}(v_2))$, contradiction.
- if p is odd, then $p \mid \text{nrd}(v_2\bar{v}_1) = A_1^2 - DA_2^2$, whence $p \mid A_1$. Again, $p \mid \gcd(\text{nrd}(v_1), 2A_1, \text{nrd}(v_2))$, contradiction.

Without loss of generality, assume that $p \nmid \text{nrd}(v_1)$. As (v_1, v_2) was defined to be the ordered basis of a \mathbb{Z} -module, we can also replace v_2 by $v_2 + kv_1$ for any integer k : this changes $v_2\bar{v}_1$ by $k \text{nrd}(v_1)$, and hence $(A_1, A_2) \rightarrow (A_1 + k \text{nrd}(v_1), A_2)$. Since $\text{nrd}(v_1)$ is coprime to p , this allows us to assume that $A_1 \equiv A_2D \pmod{p}$ (which is equivalent to $0 \pmod{p}$ by assumption, except in the case where $p = 2$ and A_2, D are odd). Then

$$v_2\bar{v}_1 = p \frac{A_1 + A_2e_2}{p} \in pO.$$

Since v_1 has reduced norm coprime to p , this implies that $v_2 \in pO$. This contradicts (v_1, v_2) generating S_{ϕ_1, ϕ_2}^O , so we are done. \square

Lemma 4.5.10. *Let ϕ_1 and ϕ_2 have the same orientation, and let $\alpha \in N_{B^\times}(O)$. Then*

$$[Q_{\phi_1, \phi_2}] = [Q_{\phi_1^\alpha, \phi_2^\alpha}],$$

i.e. the group action commutes with conjugation by elements in $N_{B^\times}(O)$ with positive norm.

If $\alpha \in O_{N=-1}$, then we have

$$[Q_{\phi_1^\alpha, \phi_2^\alpha}(X, Y)] = [-Q_{\phi_1, \phi_2}(X, -Y)].$$

Proof. If (v_1, v_2) is an oriented basis of S_{ϕ_1, ϕ_2}^O , then $(\alpha v_1 \alpha^{-1}, \alpha v_2 \alpha^{-1})$ is a basis of $S_{\phi_1^\alpha, \phi_2^\alpha}^O$. We calculate

$$\alpha v_2 \alpha^{-1} \overline{\alpha v_1 \alpha^{-1}} = \alpha v_2 \bar{v}_1 \alpha^{-1},$$

which implies that the basis is properly oriented. Thus

$$Q_{\phi_1^\alpha, \phi_2^\alpha}(X, Y) = \text{nrd}(\alpha v_1 \alpha^{-1} X + \alpha v_2 \alpha^{-1} Y) = \text{nrd}(v_1 X + v_2 Y) = Q_{\phi_1, \phi_2}(X, Y),$$

as desired.

For the second statement, $(v_1 \alpha^{-1}, -v_2 \alpha^{-1})$ is a basis of S_{ϕ_1, ϕ_2}^O . We calculate

$$-v_2 \alpha^{-1} \overline{v_1 \alpha^{-1}} = v_2 \bar{v}_1,$$

which implies that this is properly oriented. Thus

$$Q_{\phi_1, \alpha, \phi_2}(X, Y) = \text{nrd}(Xv_1\alpha^{-1} - Yv_2\alpha^{-1}) = \text{nrd}(\alpha^{-1}) \text{nrd}(Xv_1 - Yv_2) = -Q_{\phi_1, \phi_2}(X, -Y),$$

as desired. \square

Lemmas 4.5.7, 4.5.8, 4.5.9, and 4.5.10 constitute a proof of Proposition 4.5.2. To close the section, we note a corollary of this result.

Corollary 4.5.11. *Let ϕ_1 and ϕ_2 differ in orientation at the primes q_1, \dots, q_s , where $q_i \nmid \gcd(D, \mathfrak{M})$ for all i . Let $S_{\phi_1, \phi_2}^O = \mathbb{Z}v_1 + \mathbb{Z}v_2$, where (v_1, v_2) is properly oriented. Then we have*

$$v_2\bar{v}_1 - v_1\bar{v}_2 = \prod_{i=1}^s q_i^{v_{q_i}(\mathfrak{D}\mathfrak{M})} \phi_2(\sqrt{D}).$$

4.5.2 Narrow class group action

Now that we have the required facts about Q_{ϕ_1, ϕ_2} , we turn to the claimed group action in Definition 4.5.3. First, we show that it is well-defined.

Lemma 4.5.12. *In Definition 4.5.3, the equivalence class $g \cdot [\phi]$ is independent of the choice of ϕ representing $[\phi]$, the choice of I representing g , and the choice of c_I in Definition 4.5.3. Furthermore, $g \cdot [\phi]$ has the same orientation as ϕ .*

Proof. First, we claim that all choices made are indeed possible. Since all equivalence classes of proper ideals contain infinitely many prime ideals, the choice of I is possible. For c_I , we choose an arbitrary c_I that works, and if it has negative norm, we can multiply it on the left by any element of $O_{N=-1}$ to get a valid choice.

Next, we need to show that ϕ_I gives an optimal embedding into O . Let

$$O_I = \text{Ord}_R(I_O) = \{b \in B : I_O b \subseteq I_O\} = c_I^{-1} O c_I;$$

whence O_I is another Eichler order of level \mathfrak{M} . It is clear that $\phi(\mathcal{O}_D) \subseteq O_I$, so ϕ gives an embedding into O_I . Let $K = \mathbb{Q}(\sqrt{D})$, and then ϕ extends uniquely to a homomorphism $\phi : K \rightarrow B$. If the embedding $\phi : \mathcal{O}_D \rightarrow O_I$ is not optimal, then it extends to $\phi : \mathcal{O}_{D'} \rightarrow O_I$, where D' is a discriminant properly dividing D . Since $\mathcal{O}_{D'}$ commutes with I , we get

$$O\phi(I) \supseteq O\phi(I)\phi(\mathcal{O}_{D'}) = O\phi(\mathcal{O}_{D'})\phi(I).$$

Let J be the proper fractional ideal with $IJ = \mathcal{O}_D$, and then multiplying by $\phi(J)$ on the right gives us

$$O = O\phi(\mathcal{O}_D) = O\phi(I)\phi(J) \supseteq O\phi(\mathcal{O}_{D'})\phi(I)\phi(J) = O\phi(\mathcal{O}_{D'})\phi(\mathcal{O}_D) = O\phi(\mathcal{O}_{D'}).$$

Therefore $\phi(\mathcal{O}_{D'}) \subseteq O$, which contradicts ϕ being an optimal embedding into O . Thus our assumption is wrong, and $\phi : \mathcal{O}_D \rightarrow O_I$ is indeed optimal. When we conjugate by c_I , we get that the embedding ϕ_I into $c_I O_I c_I^{-1} = O$ is optimal, so it represents a class in $\text{Emb}(O, D)$.

To prove that the action is independent of our choices, let $x \in O_{N=1}$, and let $\alpha \in K$ satisfy $\text{Nm}_{K/\mathbb{Q}}(\alpha) > 0$ and $v_p(\text{Nm}_{K/\mathbb{Q}}(\alpha)) = 0$ for all $p \mid \mathfrak{DM}$. Assume we start with ϕ^x and $I' = \alpha I$ as representatives instead. We have

$$O c_{I'} = O \phi_x(I') = O x \phi(\alpha I) x^{-1} = O \phi(I) \phi(\alpha) x^{-1} = O c_I \phi(\alpha) x^{-1},$$

where we used that $Ox = O$ and α commutes with I . In particular, $O = O c_I \phi(\alpha) x^{-1} c_I^{-1}$, which implies that $r = c_I \phi(\alpha) x^{-1} c_I^{-1}$ is a unit in O . Its reduced norm satisfies

$$\text{nrd}(c_I \phi(\alpha) x^{-1} c_I^{-1}) = \text{nrd}(c_I) \text{Nm}_{K/\mathbb{Q}}(\alpha) \text{nrd}(c_I)^{-1} > 0,$$

whence it must be in $O_{N=1}$. Then $c_{I'} = r^{-1} c_I \phi(\alpha) x^{-1}$, and we calculate

$$\begin{aligned} [c_{I'} \phi_x c_{I'}^{-1}] &= [r^{-1} c_I \phi(\alpha) x^{-1} (x \phi x^{-1}) x \phi(\alpha^{-1}) c_I^{-1} r] \\ &= [r^{-1} c_I \phi(\alpha) \phi \phi(\alpha^{-1}) c_I^{-1} r] \\ &= [r^{-1} c_I \phi c_I^{-1} r] \\ &= [c_I \phi c_I^{-1}], \end{aligned}$$

so the action is well defined.

For the orientation, we consider the norm ideal of I_O , i.e. $\text{nrd}(I_O) := \{\text{nrd}(\alpha) : \alpha \in I_O\}$, a fractional ideal of \mathbb{Z} . We get

$$\langle \text{nrd}(c_I) \rangle = \text{nrd}(O c_I) = \text{nrd}(I_O) = \text{nrd}(O \phi(I)) = \text{Nm}(I) \mathbb{Z},$$

whence $\text{nrd}(c_I) = \text{Nm}(I)$ as it is positive. By our assumption on I , we have $v_p(c_I) = 0$ for all $p \mid \mathfrak{DM}$, so by Lemmas 4.4.18 and 4.4.20, the orientation of ϕ_I is the same as the orientation of ϕ at all finite primes. Since $\text{nrd}(c_I) > 0$, by Lemma 4.4.16 the orientation at ∞ is also unchanged. \square

Next, we prove that we do have a group action.

Lemma 4.5.13. *If $g, h \in \text{Cl}^+(D)$ and $[\phi] \in \text{Emb}(O, D)$, then*

$$g \cdot (h \cdot [\phi]) = gh \cdot [\phi].$$

Proof. Pick proper fractional ideals I, J representing the class group elements g, h respectively for which $v_p(\text{Nm}(I)) = v_p(\text{Nm}(J)) = 0$ for all $p \mid \mathfrak{DM}$. Note that IJ is then a valid choice to represent gh , let $O\phi(J) = Oc_J$, and let $O\phi(IJ) = Oc_{IJ}$. We have $h \cdot [\phi] = [c_J\phi c_J^{-1}]$, and we calculate

$$O(c_J\phi c_J^{-1})(I) = Oc_J\phi(I)c_J^{-1} = O\phi(J)\phi(I)c_J^{-1} = O\phi(IJ)c_J^{-1} = Oc_{IJ}c_J^{-1}.$$

Therefore

$$g \cdot (h \cdot [\phi]) = [(c_{IJ}c_J^{-1})c_J\phi c_J^{-1}(c_{IJ}c_J^{-1})^{-1}] = [c_{IJ}\phi c_{IJ}^{-1}] = gh \cdot [\phi],$$

as required. □

The final ingredient required is that the two interpretations of the group action are identical. Before doing so, we recall the equivalence between (positive definite/indefinite) binary quadratic forms of discriminant D and proper fractional ideals of \mathcal{O}_D .

If the proper ideal $I = \langle \alpha_1, \alpha_2 \rangle_{\mathbb{Z}}$ satisfies $\frac{\alpha_2\bar{\alpha}_1 - \alpha_1\bar{\alpha}_2}{\sqrt{D}} > 0$, then we send it to the quadratic form

$$\frac{\text{Nm}(X\alpha_1 - Y\alpha_2)}{\text{Nm}(I)}.$$

Given the quadratic form $f = [A, B, C]$, we send it to the proper ideal

$$\left\langle A, \frac{-B + \sqrt{D}}{2} \right\rangle_{\mathbb{Z}}.$$

Lemma 4.5.14. *Let f be a binary quadratic form representing an element of $\text{Cl}^+(D)$ (where f is positive definite if $D < 0$), and let $[\phi] \in \text{Emb}(O, D)$. Then $Q_{\phi, f \cdot \phi}$ and f are equivalent binary quadratic forms.*

Proof. Working with ideals, there are infinitely many split prime proper ideals in the class of $[f]$ in $\text{Cl}^+(D)$. Take I to be a sufficiently large one, and without loss of generality write

$$I = p\mathbb{Z} + \frac{-m + \sqrt{D}}{2}\mathbb{Z},$$

which has norm p , an odd prime for which $p \nmid D\mathfrak{D}\mathfrak{M}$. The quadratic form associated to I is $f = \left[p, m, \frac{m^2 - D}{4p} \right]$.

Take c_I as in Definition 4.5.3, let $c_I \phi c_I^{-1} = \phi'$, and consider $S = S_{\phi, \phi'}^O$. We know that $c_I \in S$, and since $\text{nrd}(c_I) = p$ is prime, it is not a non-trivial integer multiple of any element in S . In particular, we can take a oriented \mathbb{Z} -module basis of S to be (c_I, v) for some $v \in S$. From Corollary 4.5.11 we know that v must satisfy $v\bar{c}_I - c_I\bar{v} = c_I\phi(\sqrt{D})c_I^{-1}$. Let $n = \text{trd}(v\bar{c}_I) = v\bar{c}_I + c_I\bar{v}$, and combining these two equations gives us

$$v = \frac{n + c_I\phi(\sqrt{D})c_I^{-1}}{2p}c_I = c_I \frac{n + \phi(\sqrt{D})}{2p}.$$

It follows that the quadratic form associated to this basis is $Q_{\phi, \phi'} = \left[p, n, \frac{n^2 - D}{4p} \right]$, and it will suffice to prove that $n \equiv m \pmod{2p}$. Since m, n have the same parity as D , it suffices to show that $m \equiv n \pmod{p}$ only. Furthermore, as our quadratic forms are integral, we have $m^2 \equiv n^2 \equiv D \pmod{p}$, so it follows that $m \equiv \pm n \pmod{p}$; we must only eliminate the possibility of $m \equiv -n \pmod{p}$.

Define the two candidate v 's to be

$$v_1 = c_I \frac{m + \phi(\sqrt{D})}{2p}, \quad v_2 = c_I \frac{-m + \phi(\sqrt{D})}{2p}.$$

Since $O\phi(I) = Oc_I$, we see that $Op + O\frac{-m + \phi(\sqrt{D})}{2} = Oc_I$. In particular, there exist $r_1, r_2 \in O$ such that $c_I = r_1p + r_2\frac{-m + \phi(\sqrt{D})}{2}$. Multiply on the right by $\frac{m + \phi(\sqrt{D})}{2}$, and we derive

$$c_I \frac{m + \phi(\sqrt{D})}{2} = p \left(r_1 \frac{m + \phi(\sqrt{D})}{2} + r_2 \frac{m^2 - D}{4p} \right) \in pO,$$

whence $v_1 \in O$. Next,

$$v_1 + v_2 = c_I \frac{\phi(\sqrt{D})}{p} \notin O$$

since it has norm $\frac{-D}{p} \notin \mathbb{Z}$. In particular, it follows that $v_2 \notin O$, and therefore $v_2 \notin S$. Thus we must have $v \equiv v_1 \pmod{c_I}$, i.e. $m \equiv n \pmod{p}$, and so we are done. \square

All the ingredients are now prepared!

Proof of Theorem 4.5.4. Lemmas 4.5.12 and 4.5.13 show that Definition 4.5.3 gives a group action of $\text{Cl}^+(D)$ on $\text{Emb}_o(O, D)$. For the transitivity, let $[\phi_1], [\phi_2] \in \text{Emb}_o(O, D)$, and consider $Q_{\phi_1, \phi_2} \in \text{Cl}^+(D)$. Lemma 4.5.14 implies that $Q_{\phi_1, \phi_2} \cdot [\phi_1] = [\phi_2]$, as desired. For the

faithfulness, let $[\phi] \in \text{Emb}_o(O, D)$ and $f \in \text{Cl}^+(D)$. If $f \cdot [\phi] = [\phi]$, then by Lemma 4.5.14 we have $f \sim Q_{\phi, \phi}$. An oriented basis of $S_{\phi, \phi}^O$ is $(1, \phi(\frac{p_D + \sqrt{D}}{2}))$, whence

$$f \sim Q_{\phi, \phi} = X^2 + p_D XY + \frac{p_D - D}{4} Y^2,$$

which is the identity element. Therefore the action is faithful. \square

Remark 4.5.15. It is also possible to prove the group action using Q_{ϕ_1, ϕ_2} by showing that if ϕ_1, ϕ_2, ϕ_3 all have the same orientation, then

$$Q_{\phi_1, \phi_2} \circ Q_{\phi_2, \phi_3} = Q_{\phi_1, \phi_3},$$

where \circ is Gauss composition of quadratic forms.

Chapter 5

Intersection numbers for Shimura curves

The goal of this section is to begin the study of intersection numbers on Shimura curves by setting up the language and translating the results of Section 2.

In this chapter, let B be an indefinite quaternion algebra over \mathbb{Q} with Eichler order O of level \mathfrak{M} , and fix an embedding $\iota : B \rightarrow \text{Mat}(2, \mathbb{R})$. Let

$$\Gamma_O = \Gamma := \iota(O_{N=1}^\times) / \{\pm 1\}$$

be the image of $O_{N=1}$ in $\text{PSL}(2, \mathbb{R})$, a discrete subgroup. The quotient $\Gamma_O \backslash \mathbb{H}$ is referred to as a Shimura curve. We will be considering intersection numbers with respect to Γ_O .

5.1 Basic facts on intersections

Let ϕ be an optimal embedding of discriminant D into O . Let $\epsilon_D = \frac{T+U\sqrt{D}}{2}$ be the fundamental unit in \mathcal{O}_D , where (T, U) is the smallest positive integer solution to $T^2 - DU^2 = 4$. Then $\phi(\epsilon_D) \in O_{N=1}$ and $\text{trd}(\phi(\epsilon_D)) = T > 2$, hence $\iota(\phi(\epsilon_D))$ is a primitive hyperbolic element of Γ_O (the primitiveness comes from the optimality of ϕ), and thus corresponds to a closed geodesic on $\Gamma_O \backslash \mathbb{H}$ (and all closed geodesics arise in this fashion). Abbreviate $\ell_{\iota(\phi(\epsilon_D))}$ as ℓ_ϕ .

Definition 5.1.1. Let ϕ_1, ϕ_2 be optimal embeddings of positive discriminants D_1, D_2 , and let f be any function on transversal intersections. Then the f -weighted intersection number

of ϕ_1, ϕ_2 is defined to be the f -weighted intersection number of $\tilde{\ell}_{\phi_1}, \tilde{\ell}_{\phi_2}$. Explicitly, we write

$$\text{Int}_O^f(\phi_1, \phi_2) := \text{Int}_{\Gamma_O}^f(\iota(\phi_1(\epsilon_{D_1})), \iota(\phi_2(\epsilon_{D_2}))).$$

As before, we translate Proposition 2.4.3 to the language of optimal embeddings.

Proposition 5.1.2. *Every transverse intersection point of $\tilde{\ell}_{\phi_1}$ and $\tilde{\ell}_{\phi_2}$ can be lifted to \mathbb{H} to the intersection of $\ell_{\phi'_1}, \ell_{\phi'_2}$, where $\phi_1 \sim \phi'_1$ and $\phi_2 \sim \phi'_2$. This lifting is unique up to the action of simultaneous conjugation of (ϕ'_1, ϕ'_2) by $O_{N=1}$, i.e. \sim_2 .*

In particular, it suffices to count pairs (ϕ'_1, ϕ'_2) of intersecting root geodesics individually similar to (ϕ_1, ϕ_2) , taken up to simultaneous conjugation. Note that intersection numbers are defined on pairs of equivalence classes of optimal embeddings, since they correspond to conjugacy classes in Γ_O .

The next task is to translate Theorem 2.5.2 into the new setting. When we do so, a natural definition pops out.

Definition 5.1.3. Let x be any integer such that $x^2 \neq D_1 D_2$ and $x \equiv D_1 D_2 \pmod{2}$. The pair (ϕ_1, ϕ_2) of embeddings of discriminants D_1, D_2 is called x -linked if

$$x = \frac{1}{2} \text{trd} \left(\phi_1(\sqrt{D_1}) \phi_2(\sqrt{D_2}) \right).$$

In particular, if (ϕ_1, ϕ_2) is x -linked, then every pair in the equivalence class (of simultaneous equivalence) $[(\phi_1, \phi_2)]$ is x -linked.

The reason that x -linking is important is that it determines if root geodesics intersect or not.

Theorem 5.1.4. *The root geodesics $\ell_{\phi_1}, \ell_{\phi_2}$ intersect transversely if and only if (ϕ_1, ϕ_2) are x -linked for an x with*

$$x^2 < D_1 D_2.$$

If the root geodesics intersect, then

- (i) *The intersection point is the upper half plane root of $\iota(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}))$, and so it corresponds to an (not necessarily optimal) embedding of the negative quadratic order $\mathcal{O}_{x^2 - D_1 D_2}$.*

(ii) The sign of intersection is 1 if and only if $\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})$ corresponds to a positive definite embedding.

(iii) The angle of intersection θ satisfies

$$\tan(\theta) = \frac{\sqrt{D_1 D_2 - x^2}}{x}.$$

Proof. Adopt the notation of Theorem 2.5.2. Let $M_i = \iota(\phi_i(\epsilon_{D_i}))$ for $i = 1, 2$, where $\epsilon_{D_i} = \frac{T_i + U_i \sqrt{D_i}}{2}$, with (T_i, U_i) being the smallest positive integer solution to $T^2 - D_i U^2 = 4$. We calculate

$$Z_i = \iota(\phi_i(\epsilon_{D_i})) - \frac{T_i}{2} = \frac{U_i}{2} \iota(\phi_i(\sqrt{D_i})),$$

hence

$$\det(Z_i) = \frac{-U_i^2 D_i}{4}, \quad \text{Tr}(Z_1 Z_2) = \frac{U_1 U_2 x}{2}.$$

Therefore

$$\det(Z_1 Z_2 - Z_2 Z_1) = 4 \det(Z_1 Z_2) - (\text{Tr}(Z_1 Z_2))^2 = \frac{U_1^2 U_2^2}{4} (D_1 D_2 - x^2),$$

and so the root geodesics intersect if and only if $x^2 < D_1 D_2$.

Assume the root geodesics intersect, and let $T = \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})$; the intersection point is the upper half plane fixed point of $\iota(T)$. Since T satisfies $T^2 - 2xT + D_1 D_2 = 0$, T acts as $x + \sqrt{x^2 - D_1 D_2}$. But $T \in (2O + p_{D_1})(2O + p_{D_2}) \subset 2O + p_{D_1 D_2}$, hence T corresponds to an embedding of $\mathcal{O}_{x^2 - D_1 D_2}$ into O . This also implies that $x \equiv D_1 D_2 \pmod{2}$.

Note that $\overline{\phi_i(\sqrt{D_i})} = -\phi_i(\sqrt{D_i})$, whence $\overline{T} = \phi_2(\sqrt{D_2})\phi_1(\sqrt{D_1})$. Thus the sign of the intersection is 1 if and only if

$$0 < \iota(T - \overline{T})_{21} = 2\iota(T)_{2,1}.$$

The first root of $\iota(T)$ lies in the upper half plane if and only if $\iota(T)_{2,1} > 0$, hence the sign of intersection is as claimed.

Finally, the angle of intersection satisfies

$$\tan(\theta) = \frac{\sqrt{U_1^2 U_2^2 (D_1 D_2 - x^2)/4}}{U_1 U_2 x/2} = \frac{\sqrt{D_1 D_2 - x^2}}{x}.$$

□

Remark 5.1.5. Similarly to Remark 3.2.2, it can be shown that if (ϕ_1, ϕ_2) are x -linked, the first and second roots of $\iota(\phi_i(\epsilon_{D_i}))$ are $\phi_{i,f}, \phi_{i,s}$ respectively, then the cross-ratio between the roots satisfies

$$(\phi_{1,f}, \phi_{1,s}; \phi_{2,f}, \phi_{2,s}) = \frac{x - \sqrt{D_1 D_2}}{x + \sqrt{D_1 D_2}}.$$

Note that this is independent of the form in the simultaneous equivalence class (ϕ_1, ϕ_2) and the embedding ι into $\text{Mat}(2, \mathbb{R})$.

Now that the concept of intersecting root geodesics has been replaced by x -linking, deriving results becomes a lot more manageable. While intersections only come from the case of $x^2 < D_1 D_2$, a lot of properties of x -linking hold true for all x except for $x^2 = D_1 D_2$ (which is why this is included as a hypothesis). This case is a degenerate case, where the root geodesics completely overlap.

The definition of x -linking does not assume that the embeddings land inside the same order; they can just be arbitrary embeddings into B . In Lemma 6.2.1, we will show that $x \equiv D_1 D_2 \pmod{2}$ is all that is required for such an order to exist.

Define

$$\text{Emb}(O, \phi_1, \phi_2, x) := \{(\sigma_1, \sigma_2) : \sigma_1 \sim \phi_1, \sigma_2 \sim \phi_2, (\sigma_1, \sigma_2) \text{ are } x\text{-linked}\} / \sim_2,$$

the equivalence classes of x -linked pairs of embeddings similar to ϕ_1, ϕ_2 . Going further, write

$$\begin{aligned} \text{Emb}(O, D_1, D_2, x) &:= \{(\sigma_1, \sigma_2) : [\sigma_i] \in \text{Emb}(O, D_i), (\sigma_1, \sigma_2) \text{ are } x\text{-linked}\} / \sim_2 \\ &= \bigcup_{[\phi_i] \in \text{Emb}(O, D_i)} \text{Emb}(O, \phi_1, \phi_2, x), \end{aligned}$$

so that $\text{Emb}(O, D_1, D_2, x)$ captures all possible x -linking between optimal embeddings of discriminants D_1, D_2 . While we will eventually characterize and count $\text{Emb}(O, D_1, D_2, x)$ (see Theorems 6.4.2 and 7.1.2), we can already prove a strong necessary condition for this set to be non-empty.

Lemma 5.1.6. *Let $v_1, v_2 \in O$. Then*

$$\mathfrak{DM} \mid \text{nrd}(v_1 v_2 - v_2 v_1).$$

Proof. Let $p \mid \mathfrak{DM}$, and consider completing the quaternion algebra at p . We can assume that the completion O_p is either the unique maximal order if B_p is division, or the standard Eichler order of level p^e otherwise. In the first case, let the unique maximal ideal of O_p be \mathfrak{p} , and then $\frac{O_p}{\mathfrak{p}} \simeq \mathbb{F}_{p^2}$ is a field. Thus

$$v_1v_2 \equiv v_2v_1 \pmod{\mathfrak{p}},$$

which implies that $v_1v_2 - v_2v_1 \in \mathfrak{p}$, and so $p \mid \text{nrd}(v_1v_2 - v_2v_1)$.

The second case follows from the fact that looking modulo p^e , we have upper triangular matrices. The diagonal of their product is unchanged when we swap the order of multiplication, and the result follows. \square

Corollary 5.1.7. *If (ϕ_1, ϕ_2) are x -linked, then*

$$\mathfrak{DM} \mid \frac{D_1D_2 - x^2}{4}.$$

In particular, for a fixed pair of discriminants D_1, D_2 , there is a finite set of non-isomorphic pairs (B, O) of an indefinite quaternion algebra B over \mathbb{Q} with Eichler order O for which there exists optimal embeddings of D_1, D_2 into O giving a non-zero unweighted intersection number.

Proof. Let $x_i = \frac{pD_i + \sqrt{D_i}}{2}$, and from Lemma 5.1.6 and the calculations in Theorem 5.1.4, we have

$$\begin{aligned} \mathfrak{DM} \mid \text{nrd}(\phi_1(x_1)\phi_2(x_2) - \phi_2(x_2)\phi_1(x_1)) \\ = \frac{\text{nrd}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) - \phi_2(\sqrt{D_2})\phi_1(\sqrt{D_1}))}{16} = \frac{D_1D_2 - x^2}{4}. \end{aligned}$$

Intersections come from the finite set of x for which $x^2 < D_1D_2$, and this calculation shows that for each such x there are finitely many pairs $(\mathfrak{D}, \mathfrak{M})$ that satisfy the divisibility condition (in Theorem 6.4.2 we will show that \mathfrak{D} is in fact uniquely determined from D_1, D_2, x). Therefore, there are finitely many Eichler orders for which there exist intersections of optimal embeddings of discriminants D_1, D_2 . \square

5.2 Intersection weights

To bring more arithmetic into the setup, we would like to vary the weight function.

Definition 5.2.1. Let ϕ_1, ϕ_2 be x -linked optimal embeddings of \mathcal{O}_{D_1} and \mathcal{O}_{D_2} into O , and define $\phi_1 \times \phi_2$ to be the optimal embedding into O for which

$$\phi_1 \times \phi_2(x + \sqrt{x^2 - D_1 D_2}) = \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}).$$

Note that in the equivalence class $[(\phi_1, \phi_2)]$ of simultaneous conjugation, the equivalence class of $[\phi_1 \times \phi_2]$ is constant.

Definition 5.2.2. The *sign* of the intersection (ϕ_1, ϕ_2) , denoted $\text{sg}(\phi_1, \phi_2)$, is 1 if $\phi_1 \times \phi_2$ is positive definite, -1 if $\phi_1 \times \phi_2$ negative definite, and 0 otherwise. The level of the intersection, denoted $\ell(\phi_1, \phi_2) = \ell \in \mathbb{Z}^+$, is defined by $\phi \times \phi_2$ being an optimal embedding of discriminant $\frac{x^2 - D_1 D_2}{\ell^2}$.

By Theorem 5.1.4, the sign of the intersection corresponds to the physical sign of intersection as defined in Section 2.

Using the notion of sign and level, we can describe three different intersection functions f that will be studied in this paper:

1. $f(\phi_1, \phi_2) = 1$ is called the unweighted intersection number, and is denoted Int_O .
2. $f(\phi_1, \phi_2) = \text{sg}(\phi_1, \phi_2)$ is called the signed intersection number, and is denoted Int_O^\pm .
3. For a prime q , $f(\phi_1, \phi_2) = \text{sg}(\phi_1, \phi_2)(1 + v_q(\ell(\phi_1, \phi_2)))$ is called the q -weighted intersection number, and is denoted Int_O^q .

We now present an alternate description of the q -weighted intersection for $q \mid \mathfrak{D}$. For any $n \in \mathbb{Z}^{\geq 0}$ we get maps

$$\mathcal{O}_{D_i} \rightarrow O \rightarrow \frac{O}{q^n O}.$$

Let N be the largest nonnegative integer such that the images of \mathcal{O}_{D_i} in $\frac{O}{q^N O}$ are equal.

Proposition 5.2.3. *Assume that $q \nmid \gcd(D_1, D_2)$ and $q \mid \mathfrak{D}$. With notation as above, we have $v_q(\ell(\phi_1, \phi_2)) = N$.*

Proof. We can work in the completion, since $\frac{O}{q^n O} = \frac{O_q}{q^n O_q}$. The images of $\phi_i(\mathcal{O}_{D_i})$ in $\frac{O_q}{q^n O_q}$ are the same if and only if there exist integers a, b with b coprime to q for which

$$\frac{p_{D_1} + \phi_1(\sqrt{D_1})}{2} \equiv a + b \frac{p_{D_2} + \phi_2(\sqrt{D_2})}{2} \pmod{q^n O_q}.$$

For now, assume that $q > 2$. Multiplying by 2 and rearranging, this is equivalent to

$$\phi_1(\sqrt{D_1}) - b\phi_2(\sqrt{D_2}) \equiv 2a + bp_{D_2} - p_{D_1} \pmod{q^n O_q},$$

for some integers a, b with b coprime to q . Taking the trace of each side gives $0 \equiv 2(2a + bp_{D_2} - p_{D_1}) \pmod{q^n}$, hence

$$\phi_1(\sqrt{D_1}) - b\phi_2(\sqrt{D_2}) \equiv 0 \pmod{q^n O_q}.$$

If this is true for some b coprime to q , then taking $a \equiv \frac{p_{D_1} - bp_{D_2}}{2} \pmod{q^n}$ gives a valid pair (a, b) , hence this condition is equivalent.

If this is true, then multiplying on right by $\phi_2(\sqrt{D_2})$ implies that

$$\frac{T - bD_2}{q^n} \in O_q,$$

where $T = \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})$. This implies that $\phi_1 \times \phi_2$ descends to an embedding of discriminant $\frac{x^2 - D_1 D_2}{q^n}$. Therefore $v_q(\ell(\phi_1, \phi_2)) \geq N$.

For the other direction, we have $T - x \in q^n O_q$. If q is coprime to D_2 , multiplying by $\frac{\phi_2(\sqrt{D_2})}{D_2}$ on the right gives

$$\phi_1(\sqrt{D_1}) - \frac{x}{D_2} \phi_2(\sqrt{D_2}) \in q^n O_q.$$

If $q \nmid x$ we would be done, so assume otherwise. From Corollary 5.1.7,

$$q \mid \mathfrak{D} \mid D_1 D_2 - x^2,$$

whence $q \mid D_1$. Since ϕ_1 is an optimal embedding and $q \mid \mathfrak{D}$, Proposition 4.4.7 implies that $q \parallel D_1$. In particular, $v_q(x^2 - D_1 D_2) = 1$ necessarily, so $v_q(\ell(\phi_1, \phi_2)) = 0$, and the conclusion of $N \geq v_q(\ell(\phi_1, \phi_2))$ still follows. If $q \mid D_2$, then q is coprime to D_1 , and multiplying $T - x$ by $\frac{\phi_1(\sqrt{D_1})}{D_1}$ on the left and following the same argument gives the result.

For $q = 2$, see Proposition A.2.2. □

Remark 5.2.4. The proof of Proposition 5.2.3 also shows that $v_q(\ell(\phi_1, \phi_2)) \geq N$ for all primes q . Equality also holds if $q \nmid x$ or $q \nmid D_1 D_2$, but does not necessarily hold for all q .

Chapter 6

Existence of x -linking

In general, we would like to start with an indefinite quaternion algebra B over \mathbb{Q} with Eichler order O , and take optimal embeddings ϕ_1, ϕ_2 of discriminants D_1, D_2 into O and study their intersections. In the last section, we saw that this corresponds to studying the possible x -linkings of pairs (ϕ'_1, ϕ'_2) individually similar to (ϕ_1, ϕ_2) . Studying this directly is still difficult, so in this chapter we study the inverted setup. We will start with a pair of x -linked embeddings into B , and study the possible Eichler orders for which these embeddings land in, are optimal with respect to, and the resulting levels of intersection. In Chapter 7 we will take the ideas of this chapter, and translate them back to the setting where we start with a fixed Eichler order.

The first main result of this chapter is a refinement of Corollary 5.1.7, namely that there is exactly one quaternion algebra admitting x -linked embeddings of discriminants D_1, D_2 , as well as giving a precise description of it (Theorem 6.4.2). Assuming $\gcd\left(D_1, D_2, \frac{D_1 D_2 - x^2}{4}\right) = 1$, let (ϕ_1, ϕ_2) be such an x -linked pair. We then describe the possible Eichler orders that admit ϕ_1, ϕ_2 as embeddings, consider which admit them optimally, and finally describe the possible levels of such embedding pairs. The condition $\gcd\left(D_1, D_2, \frac{D_1 D_2 - x^2}{4}\right) = 1$ is included as a sort of “most general case possible while still producing comprehensible results”. Assuming that D_1, D_2 are coprime and fundamental will produce very nice statements, whereas when you allow $D_1, D_2, \frac{D_1 D_2 - x^2}{4}$ to have common factors, many results and proofs become more technical and full of casework. The methods found in this thesis adapt to those cases, so if one has a specific need for this, it can be done.

6.1 Simultaneous conjugation

The fact that we are only allowing conjugation by elements of $O_{N=1}^\times$ and not all of B^\times is crucial to x -linking.

Proposition 6.1.1. *Let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over a field F of characteristic not equal to 2, and let (x_1, y_1) and (x_2, y_2) be pairs of elements of B^\times for which:*

- *None of $x_n, y_n, x_n y_n$ lie in F for $n = 1, 2$;*
- *x_1 and x_2 have the same separable minimal polynomial over F ;*
- *y_1 and y_2 have the same separable minimal polynomial over F ;*
- *$x_1 y_1$ and $x_2 y_2$ have the same separable minimal polynomial over F .*

Then the pairs are simultaneously conjugate over B , i.e. there exists an $r \in B^\times$ for which $rx_1 r^{-1} = x_2$ and $ry_1 r^{-1} = y_2$.

Proof. The minimal polynomials of x_n, y_n are quadratic, and by simultaneously conjugating (x_1, y_1) and using Corollary 4.2.2 we can assume that $x_1 = x_2 = x$. By replacing $(x, y_1), (x, y_2)$ by $(x - \frac{\text{trd } x}{2}, y_1 - \frac{\text{trd } y_1}{2}), (x - \frac{\text{trd } x}{2}, y_2 - \frac{\text{trd } y_2}{2})$ no assumptions or conclusions change. Therefore we can assume that x, y_1, y_2 all have trace 0 and square to an element of F^\times . By Lemma 4.4.10, we can relabel our coordinates to assume that $x = i$.

Let y_n have reduced norm $-N$ and let $x y_n$ have reduced trace $2T$. Writing $y_n = f_n i + g_n j + h_n k$ for $n = 1, 2$, the reduced norm and trace conditions give us the equations

$$a f_n^2 + b g_n^2 - a b h_n^2 = N, \quad T = f_n a.$$

Thus $f_n = \frac{T}{a}$, and with this substitution, our first equation rearranges to

$$g_n^2 - a h_n^2 = \frac{aN - T^2}{ab}.$$

If we can produce an invertible element $c + di$ for which $(c + di)y_1(c + di)^{-1} = y_2$, then we will be done as $c + di$ stabilizes $x = i$ under conjugation. Consider the elements

$$\begin{aligned} c_1 + d_1 i &= -a(h_1 + h_2) + (g_1 - g_2)i; \\ c_2 + d_2 i &= -(g_1 + g_2) + (h_1 - h_2)i, \end{aligned}$$

and assume that $g_1 \neq g_2$ and $h_1 \neq h_2$. We calculate that

$$\begin{aligned} (c + di)y_1(c + di)^{-1} &= (c + di)(f_1i + g_1j + h_1k)(c + di)^{-1} \\ &= f_1i + \frac{(g_1c^2 + 2ah_1cd + ag_1d^2)j + (h_1c^2 + 2g_1cd + ah_1d^2)k}{c^2 - ad^2}. \end{aligned}$$

The i coefficients of this and y_2 are always equal as $f_1 = f_2 = \frac{T}{a}$. The j coefficient is equal to g_2 is equivalent to

$$(g_1 - g_2)c^2 + 2ah_1cd + (ag_1 + ag_2)d^2 = 0.$$

This has discriminant

$$4a^2h_1^2 - 4a(g_1 - g_2)(g_1 + g_2) = 4a(ah_1^2 - g_1^2 + g_2^2) = 4a(ah_2^2 - g_2^2 + g_2^2) = (2ah_2)^2,$$

and therefore it factorizes as

$$(g_1 - g_2) \left(c - \frac{a(-h_1 - h_2)}{g_1 - g_2} d \right) \left(c - \frac{a(-h_1 + h_2)}{g_1 - g_2} d \right),$$

which equals 0 for $(c, d) = (c_n, d_n)$ for $n = 1, 2$. The k coefficient is h_2 is equivalent to

$$(h_1 - h_2)c^2 + 2g_1cd + (ah_1 + ah_2)d^2 = 0.$$

This has discriminant

$$4g_1^2 - 4a(h_1 - h_2)(h_1 + h_2) = 4(g_1^2 - ah_1^2 + ah_2^2) = 4g_2^2 = (2g_2)^2,$$

whence the quadratic factorizes as

$$(h_1 - h_2) \left(c - \frac{-g_1 - g_2}{h_1 - h_2} d \right) \left(c - \frac{-g_1 + g_2}{h_1 - h_2} d \right),$$

which again equals 0 for $(c, d) = (c_n, d_n)$ for $n = 1, 2$. We just need to check that at least one of these elements is invertible, i.e. has non-zero norm. The minimal polynomial of xy_i is $X^2 - 2TX + aN$, and as it is separable it has non-zero discriminant. Thus $4T^2 - 4aN \neq 0$, and therefore $T^2 - aN \in F^\times$. If $\text{nr}(c_n + d_n i) = 0$ for $i = 1, 2$, then we have

$$0 = \text{nr}(c_1 + d_1 i) - a \text{nr}(c_2 + d_2 i) = 4 \frac{T^2 - aN}{b} \neq 0,$$

a contradiction. Therefore the proposition is proved in this case.

The remaining cases are when $g_1 = g_2$ or $h_1 = h_2$. If $g_1 = g_2$, then we get $h_1^2 = h_2^2$ so $h_1 = \pm h_2$. If $h_1 = h_2$ the proposition is trivial, and if $h_1 = -h_2 \neq 0$, then $c + di = -g_1 + h_1 i$ gives an element which works (noting that $\text{nrd}(c + di) = g_1^2 - ah_1^2 = \frac{aN-T^2}{ab} \neq 0$). The last case is $h_1 = h_2$ and $g_1 = -g_2$, and $c + di = -ah_1 + g_1 i$ works. \square

Applying Proposition 6.1.1 to optimal embeddings produces the following corollary.

Corollary 6.1.2. *Let B be a quaternion algebra over $F = \mathbb{Q}$ or \mathbb{Q}_p , and let $(\phi_1, \phi_2), (\phi'_1, \phi'_2)$ be pairs of x -linked embeddings from $\mathcal{O}_{D_1}, \mathcal{O}_{D_2}$ respectively into B . Then $V = \{v \in B : v\phi_n = \phi'_n v \text{ for } n = 1, 2\}$ is a 1-dimensional F -vector space, generated by an element of B with non-zero norm. In particular, the pairs of embeddings are simultaneously conjugate over B^\times .*

Proof. Let $V_n = \{v \in B : v\phi_n = \phi'_n v\}$ for $n = 1, 2$; by Corollary 4.2.2, this is a two dimensional F -vector space. Furthermore, we have $V_n = r_n(F + \phi_n(\sqrt{D_n})F)$ for $n = 1, 2$ for some $r_1, r_2 \in B^\times$. We claim that V_1 and V_2 are distinct: otherwise, right multiplication by $\phi_1(\sqrt{D_1})$ on V_1 remains in V_1 , hence it is true for V_2 as well. This implies that $\phi_1(\sqrt{D_1}) \in F + \phi_2(\sqrt{D_2})F$, and therefore $\phi_1(\sqrt{D_1})$ is a scalar multiple of $\phi_2(\sqrt{D_2})$ (by taking traces). Writing $\phi_1(\sqrt{D_1}) = f\phi_2(\sqrt{D_2})$ for $f \in F^\times$, squaring gives us $D_1 = f^2 D_2$ and $x = \frac{1}{2} \text{trd}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})) = fD_1$. Thus $x^2 = f^2 D_1^2 = D_1 D_2$, which is a contradiction by definition of x -linkage.

Since $V = V_1 \cap V_2$, V has dimension 0 or 1 as V_1, V_2 are distinct. We apply proposition 6.1.1 to the images of $\sqrt{D_1}, \sqrt{D_2}$ under (ϕ_1, ϕ_2) and (ϕ'_1, ϕ'_2) respectively. All the minimal polynomials in question are quadratic and separable as the discriminants are $D_1, D_2, 4x^2 - 4D_1 D_2$, which are all non-zero. Thus the proposition applies and implies that V has dimension 1 and contains an invertible element, as desired. \square

6.2 Orders containing pairs of optimal embeddings

Given a pair of embeddings ϕ_1, ϕ_2 , we study the set of orders for which they can (optimally) embed into.

Lemma 6.2.1. *Let $F = \mathbb{Q}$ or \mathbb{Q}_p , and let B be a quaternion algebra over F . Let $\phi_i : \mathcal{O}_{D_i} \rightarrow B$ be embeddings of the orders of discriminants D_1, D_2 into B , and define $v_i = \phi_i\left(\frac{p_{D_i} + \sqrt{D_i}}{2}\right)$ for $i = 1, 2$. Assume that $x := \frac{1}{2} \text{trd}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})) \in p_{D_1 D_2} + 2\mathcal{O}_F$ and $x^2 \neq D_1 D_2$. Then*

$$O_{\phi_1, \phi_2} := \langle 1, v_1, v_2, v_1 v_2 \rangle_{\mathcal{O}_F}$$

is an order of B , necessarily the smallest order of B for which ϕ_1, ϕ_2 embed into. Furthermore, up to multiplication by \mathcal{O}_F^\times we have

$$\text{discrd}(O_{\phi_1, \phi_2}) = \frac{D_1 D_2 - x^2}{4}.$$

Proof. For ease of notation write $O = O_{\phi_1, \phi_2}$. First,

$$\text{trd}(v_1 v_2) = \frac{p_{D_1} p_{D_2} + x}{2} = p_{D_1} p_{D_2} + \frac{x - p_{D_1} p_{D_2}}{2} \in \mathcal{O}_F,$$

and $\text{nr}(v_1 v_2) = \text{nr}(v_1) \text{nr}(v_2) \in \mathcal{O}_F$, whence $v_1 v_2$ is integral. We will demonstrate that $v_2 v_1 \in O$, and the rest of the equations to prove that O_{ϕ_1, ϕ_2} is closed under multiplication can be deduced from this and the minimal polynomials for v_1, v_2 . We compute

$$\begin{aligned} v_1 v_2 + v_2 v_1 &= \frac{p_{D_1 D_2} + p_{D_1} \phi_2(\sqrt{D_2}) + p_{D_2} \phi_1(\sqrt{D_1})}{2} + \frac{\phi_1(\sqrt{D_1}) \phi_2(\sqrt{D_2}) + \phi_2(\sqrt{D_2}) \phi_1(\sqrt{D_1})}{4} \\ &= p_{D_1} v_2 + p_{D_2} v_1 + \frac{x - p_{D_1} p_{D_2}}{2}, \end{aligned}$$

whence $v_2 v_1$ lies in O , as claimed.

The fact that O is an order will follow from computing its reduced discriminant, and seeing that it is non-zero. To ease our calculations, write

$$\begin{pmatrix} 1 \\ \phi_1(\sqrt{D_1}) \\ \phi_2(\sqrt{D_2}) \\ \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -p_{D_1} & 2 & 0 & 0 \\ -p_{D_2} & 0 & 2 & 0 \\ p_{D_1} p_{D_2} & -2p_{D_2} & -2p_{D_1} & 4 \end{pmatrix} \begin{pmatrix} 1 \\ v_1 \\ v_2 \\ v_1 v_2 \end{pmatrix},$$

and we have the equation

$$d(1, \phi_1(\sqrt{D_1}), \phi_2(\sqrt{D_2}), \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})) = \det(M)^2 d(1, v_1, v_2, v_1 v_2),$$

where M is the transition matrix above. We calculate that $\det(M) = 16$ and

$$\begin{aligned} d(1, \phi_1(\sqrt{D_1}), \phi_2(\sqrt{D_2}), \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})) &= \det \begin{pmatrix} 2 & 0 & 0 & 2x \\ 0 & 2D_1 & 2x & 0 \\ 0 & 2x & 2D_2 & 0 \\ 2x & 0 & 0 & 4x^2 - 2D_1D_2 \end{pmatrix} \\ &= -16(D_1D_2 - x^2)^2. \end{aligned}$$

Since the $\text{discrd}(O)^2 = -d(1, v_1, v_2, v_1v_2)$, the reduced discriminant is as claimed (and is non-zero by the assumption of $x^2 \neq D_1D_2$). See the proof of Theorem 2' in [Kan89] for a similar computation in a definite quaternion algebra.

It is immediate that O is the smallest order for which ϕ_1, ϕ_2 embed into, as such an order must contain $\{1, v_1, v_2\}$, and O is generated as an \mathcal{O}_F algebra by these elements. \square

Lemma 6.2.1 will be crucial to understanding and counting x -linking. First, we use it to show that things can be done locally.

Lemma 6.2.2. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} in B , let D_1, D_2 be positive discriminants, and let x be any integer such that $x \equiv D_1D_2 \pmod{2}$ and $x^2 \neq D_1D_2$. Then the set $\text{Emb}(O, D_1, D_2, x)$ is non-empty if and only if $\text{Emb}(O_p, D_1, D_2, x)$ is non-empty for all finite primes p .*

Proof. If such a pair $(\phi_1, \phi_2) \in \text{Emb}(O, D_1, D_2, x)$ exists, then the corresponding maps to the completions gives elements of $\text{Emb}(O_p, D_1, D_2, x)$ for all p .

To prove the opposite direction, assume that $(\alpha_p, \beta_p) \in \text{Emb}(O_p, D_1, D_2, x)$ for all p . By Lemma 4.4.9, there exists an embedding ϕ_1 of \mathcal{O}_{D_1} into B . By Corollary 4.4.11, we can assign coordinates so that $\phi_1(\sqrt{D_1}) = i$. In this case, we are considering the existence of a map ϕ_2 such that $\phi_2(\sqrt{D_2}) = fi + gj + hk$, where

$$\text{nrd}(fi + gj + hk) = -D_2 \quad \text{and} \quad 2x = \text{trd}(i(fi + gj + hk)) = 2fD_1.$$

With the substitution of $f = \frac{x}{D_1}$, the equation $\text{nrd}\left(\frac{x}{D_1}i + gj + hk\right) + D_2 = 0$ is a quadratic form in g, h . This will have a solution in \mathbb{R} since B is indefinite, and it will have a solution

in \mathbb{Q}_p for all p since $\text{Emb}(O_p, D_1, D_2, x)$ is non-empty. By Hasse's principle, it has a solution over \mathbb{Q} ; let the corresponding map be ϕ_2 .

Following Lemma 6.2.1, let $O' = O_{\phi_1, \phi_2}$ be the smallest order for which ϕ_1, ϕ_2 embed into. By Corollary 6.1.2, for all finite primes p there exists an $r_p \in B_p^\times$ for which $r_p(\alpha_p, \beta_p)r_p^{-1} = (\phi_{1,p}, \phi_{2,p})$. By the definition of O' , it follows that $O'_p \subset r_p O_p r_p^{-1}$. For all primes p ,

- let $s_p = r_p$ if $O'_p \neq O_p$ or $p \mid D_1 D_2$;
- let $s_p = 1$ otherwise.

Consider the sequence of local orders $\{s_p O_p s_p^{-1}\}_p$. Since $O'_p = O_p$ holds for all but finitely many primes, by Theorem 4.1.1 there exists an order O'' of B which localizes to $s_p O_p s_p^{-1}$ for all primes p . In particular, we note that O'' is an Eichler order of level \mathfrak{M} , and ϕ_1, ϕ_2 give embeddings into O'' . When $p \mid D_1 D_2$ the local embeddings are optimal since (α_p, β_p) were optimal, hence ϕ_1, ϕ_2 are optimal embeddings into O'' . Since all Eichler orders are conjugate, let $r O'' r^{-1} = O$, and then $[r(\phi_1, \phi_2)r^{-1}] \in \text{Emb}(O, D_1, D_2, x)$, as required. \square

In particular, the non-emptiness of $\text{Emb}(O, D_1, D_2, x)$ can be studied locally.

6.3 Local x-linking

While we were concerned with orders in Lemma 6.2.2, we will drop this for now and instead consider embeddings into the entire quaternion algebra.

Definition 6.3.1. Define $\text{Emb}(B, D_1, D_2, x)$ to be the set of all pairs (ϕ_1, ϕ_2) of x -linked embeddings of discriminants D_1, D_2 into B .

Note that the results of Lemma 6.2.2 also applies to the sets $\text{Emb}(B, D_1, D_2, x)$ and $\text{Emb}(B_p, D_1, D_2, x)$.

We start the local calculations by considering the division algebra case. Recall the Hilbert symbol $(a, b)_p$, which is 1 if $\left(\frac{a, b}{\mathbb{Q}_p}\right) \simeq \text{Mat}(2, \mathbb{Q}_p)$, and -1 otherwise. An alternate characterization is $(a, b)_p = 1$ if and only if $ax^2 + by^2 = 1$ has solutions with $x, y \in \mathbb{Q}_p$ (see Section 5.6 of [Voi21]).

Lemma 6.3.2. *Let D_1, D_2 be discriminants, let x be any integer such that $x \equiv D_1 D_2 \pmod{2}$ and $x^2 \neq D_1 D_2$, and let $B = \mathbb{Q}A_p^{\text{div}}$. Then $\text{Emb}(B, D_1, D_2, x)$ is non-empty if and only if*

$$(D_1, x^2 - D_1 D_2)_p = -1.$$

If $p \nmid D_1$, this is equivalent to

$$\left(\frac{D_1}{p}\right) = -1 \text{ and } v_p\left(\frac{D_1 D_2 - x^2}{4}\right) \text{ is odd.}$$

Proof. If there does not exist an embedding of \mathcal{O}_{D_1} into B , then by Proposition 4.4.7 we find that $(D_1, N)_p = 1$ for all $N \neq 0$, and the result follows. Otherwise, by Corollary 4.4.11, we can write $B = \left(\frac{D_1 e}{\mathbb{Q}_p}\right)$ for some $e \in \mathbb{Z}_p$, where $\phi_1(\sqrt{D_1}) = i$ and $(D_1, e)_p = -1$. Writing $\phi_2(\sqrt{D_2}) = fi + gj + hk$, it suffices to solve the equations

$$D_1 f^2 + eg^2 - D_1 eh^2 = D_2, \quad x = fD_1.$$

Therefore $f = \frac{x}{D_1}$, and the first equation rearranges to

$$g^2 - D_1 h^2 = \frac{D_1 D_2 - x^2}{eD_1}.$$

If this has a solution with $h = h_1$, then by Hensel's lemma there will be a solution with $h = h_1 + p^k$ for some k . In particular, they correspond to distinct g 's, so we can solve the equation with the assumption that $g \neq 0$. The equation then rearranges to

$$D_1 (h/g)^2 + \frac{D_1 D_2 - x^2}{eD_1} (1/g)^2 = 1,$$

which is in the format of the Hilbert symbol. The properties of the Hilbert symbol imply that

$$\left(D_1, \frac{D_1 D_2 - x^2}{eD_1}\right)_p = (D_1, (x^2 - D_1 D_2)e)_p = -(D_1, x^2 - D_1 D_2)_p,$$

from which the result follows.

If $p \nmid D_1$, there exists an embedding of \mathcal{O}_{D_1} if and only if $\left(\frac{D_1}{p}\right) = -1$. If this holds, then $v_p(e)$ is odd. Scaling by powers of p , it suffices to solve

$$g^2 - D_1 h^2 = \frac{D_1 D_2 - x^2}{eD_1} p^{2r}, \tag{6.3.1}$$

for $r \geq 0$ and $g, h \in \mathbb{Z}_p$. Proposition A.1.1 implies that Equation 6.3.1 has a solution if and only if $v_p\left(\frac{D_1 D_2 - x^2}{eD_1} p^{2r}\right)$ is even, which is equivalent to our condition. \square

Now we consider non-division algebras.

Lemma 6.3.3. *Let D_1, D_2 be discriminants, and let x be any integer such that $x \equiv D_1 D_2 \pmod{2}$ and $x^2 \neq D_1 D_2$. Then $\text{Emb}(\text{Mat}(2, \mathbb{Q}_p), D_1, D_2, x)$ is non-empty if and only if*

$$(D_1, x^2 - D_1 D_2)_p = 1.$$

If $p \nmid D_1$ this is equivalent to either

$$\left(\frac{D_1}{p}\right) = 1 \quad \text{or} \quad \left(\frac{D_1}{p}\right) = -1 \quad \text{and} \quad v_p\left(\frac{D_1 D_2 - x^2}{4}\right) \text{ is even.}$$

Proof. Via Corollary 6.1.2, we can fix the first embedding to be $\phi_1(\sqrt{D_1}) = \begin{pmatrix} 0 & D_1 \\ 1 & 0 \end{pmatrix}$, and we write $\phi_2(\sqrt{D_2}) = \begin{pmatrix} e & f \\ g & -e \end{pmatrix} \in \text{Mat}(2, \mathbb{Q}_p)$. We will have a solution if and only if

$$e^2 + fg = D_2, \quad D_1 g + f = 2x.$$

This implies that $f = 2x - D_1 g$, and plugging this into the first equation and rearranging gives

$$e^2 - D_1 \left(g - \frac{x}{D_1}\right)^2 = \frac{D_1 D_2 - x^2}{D_1}.$$

Let $X = e$ and $Y = g - \frac{x}{D_1}$, and then the equation is

$$X^2 - D_1 Y^2 = \frac{D_1 D_2 - x^2}{D_1}.$$

The rest of the proof is analogous to Lemma 6.3.2, where Proposition A.1.1 completes the characterization of the solubility when $p \nmid D_1$. □

Lemmas 6.3.2 and 6.3.3 immediately imply the following corollary

Corollary 6.3.4. *Let D_1, D_2 be discriminants, and let x be an integer such that $x \equiv D_1 D_2 \pmod{2}$ and $x^2 \neq D_1 D_2$. Then exactly one of QA_p^{div} and $\text{Mat}(2, \mathbb{Q}_p)$ admits x -linked embeddings of $\mathcal{O}_{D_1}, \mathcal{O}_{D_2}$, and which one is determined by if $(D_1, x^2 - D_1 D_2)_p$ is -1 or 1 , respectively.*

Remark 6.3.5. The first half of Lemmas 6.3.2, 6.3.3 and Corollary 6.3.4 still holds when $p = \infty$, where $\mathbb{Q}_\infty = \mathbb{R}$.

6.4 Global x-linking

Fix discriminants D_1, D_2 and x any integer such that $x \equiv D_1 D_2 \pmod{2}$ and $x^2 \neq D_1 D_2$. Corollary 6.3.4 combined with Lemma 6.2.2 implies that there is precisely one quaternion algebra B over \mathbb{Q} for which there exist embeddings ϕ_i of \mathcal{O}_{D_i} into B that are x -linked, and it is given by

$$\left(\frac{D_1, x^2 - D_1 D_2}{\mathbb{Q}} \right).$$

We can describe the ramification of this quaternion algebra by using a generalized definition of the ϵ function from [GZ85].

Definition 6.4.1. Let D_1, D_2 be discriminants, and p any prime (or -1) such that

$$p \nmid \gcd(D_1^{\text{fund}}, D_2^{\text{fund}}) \quad \text{and} \quad \left(\frac{D_1^{\text{fund}} D_2^{\text{fund}}}{p} \right) \neq -1.$$

Define

$$\epsilon(p) := \begin{cases} \left(\frac{D_1^{\text{fund}}}{p} \right) & \text{if } p \text{ and } D_1^{\text{fund}} \text{ are coprime;} \\ \left(\frac{D_2^{\text{fund}}}{p} \right) & \text{if } p \text{ and } D_2^{\text{fund}} \text{ are coprime.} \end{cases}$$

Theorem 6.4.2. Let D_1, D_2 be positive discriminants and x an integer with $x \equiv D_1 D_2 \pmod{2}$ and $x^2 \neq D_1 D_2$. Then the only quaternion algebra over \mathbb{Q} that admits x -linked embeddings from $\mathcal{O}_{D_1}, \mathcal{O}_{D_2}$ is

$$B = \left(\frac{D_1, x^2 - D_1 D_2}{\mathbb{Q}} \right).$$

Furthermore, let $N = \gcd(D_1^{\text{fund}}, D_2^{\text{fund}})$, and factorize

$$\frac{D_1 D_2 - x^2}{4} = \pm N' \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where N' is minimal so that $\frac{D_1 D_2 - x^2}{4N'}$ is coprime to N , p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$. Then B is ramified at

$$\{p_1, p_2, \dots, p_r\} \cup \{p : p \mid N', (D_1, x^2 - D_1 D_2)_p = -1\}.$$

Proof. It suffices to compute $(D_1, x^2 - D_1D_2)_p$ for $p \mid \frac{D_1D_2 - x^2}{4}$ satisfying $p \nmid N'$. If $p \nmid D_1$, Lemmas 6.3.2 and 6.3.3 imply that the Hilbert symbol is -1 if and only if $\epsilon(p) = -1$ and $v_p\left(\frac{D_1D_2 - x^2}{4}\right)$ is odd, i.e. $p = p_i$ for some i . Since

$$(D_1, x^2 - D_1D_2)_p = (D_2, x^2 - D_1D_2)_p,$$

the same holds for $p \nmid D_2$. As we assume that $p \nmid N'$, the final case is (without loss of generality) $p \nmid D_1^{\text{fund}}$ and $p \mid D_1, D_2$. By Lemma 6.5.5, we can replace (D_1, D_2, x) by $(D_1/p^2, D_2, x/p)$, and repeat. \square

Remark 6.4.3. To work with an explicit x -linked pair, take $B = \left(\frac{D_1, x^2 - D_1D_2}{\mathbb{Q}}\right)$, and define

$$\phi_1(\sqrt{D_1}) = i, \quad \phi_2(\sqrt{D_2}) = \frac{xi + k}{D_1}.$$

This pair is x -linked and corresponds to $\phi_1 \times \phi_2(\sqrt{x^2 - D_1D_2}) = j$.

6.5 Local Eichler orders containing x -linked pairs

In general, the order O_{ϕ_1, ϕ_2} will not be Eichler. As such, we need to describe and count the Eichler orders which contain it.

Definition 6.5.1. Given a triple (D_1, D_2, x) where D_1, D_2 are discriminants and x is an integer with $x \equiv D_1D_2 \pmod{2}$ and $x^2 \neq D_1D_2$, we call the triple *nice* if

$$\gcd\left(D_1, D_2, \frac{D_1D_2 - x^2}{4}\right) = 1.$$

More generally, call a prime p *nice* (with respect to (D_1, D_2, x)) if

$$p \nmid \gcd\left(D_1, D_2, \frac{D_1D_2 - x^2}{4}\right).$$

Restricting to nice triples/nice primes is a reasonable middle ground between a pleasant exhibition and full generality. When D_1, D_2 are coprime and fundamental the results take the simplest and nicest form, and working with not nice triples/primes yields results that are full of cases, and rather unwieldy.

In order to help prove that an order is Eichler, we consider the Eichler symbol (see Definition 24.3.2 of [Voi21] for a full exposition). Working in $B = \left(\frac{a,b}{\mathbb{Q}_p}\right)$, for $\alpha \in B$, define

$$\Delta(\alpha) = \text{trd}(\alpha)^2 - 4 \text{nrd}(\alpha) = 4(af^2 + bg^2 - abh^2),$$

where $\alpha = e + fi + gj + hk$. For an order O of B , define (O, p) to be the set of values that $\left(\frac{\Delta(\alpha)}{p}\right)$ takes as α ranges over O , where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

Lemma 6.5.2. *The set (O, p) determines the Eichlerness of O as follows:*

- *The order O is Eichler and non-maximal if and only if $(O, p) = \{0, 1\}$ (i.e. O is “residually split”).*
- *If $-1 \in (O, p)$, then O is contained in precisely one maximal order.*

Proof. The first point is a direct consequence of Lemma 24.3.6 of [Voi21]. For the second point, if O' is a superorder of O , then $(O, p) \subseteq (O', p)$. In particular, no superset has $(O, p) = \{0, 1\}$, whence O is not contained in a non-maximal Eichler order. If O were contained in two maximal orders, it would be contained in their intersection, a non-maximal Eichler order, contradiction. \square

Lemma 6.5.2 allows us to compute the Eichler orders containing O_{ϕ_1, ϕ_2} .

Lemma 6.5.3. *Let ϕ_1, ϕ_2 be x -linked embeddings of discriminants D_1, D_2 into B , a quaternion algebra over \mathbb{Q}_p , where p is nice. Let $O = O_{\phi_1, \phi_2}$, and then:*

- (i) *If $p \nmid \frac{D_1 D_2 - x^2}{4}$, then O is maximal;*
- (ii) *If $\epsilon(p) = -1$, then O is contained in a unique maximal order;*
- (iii) *If $\epsilon(p) = 1$, then O is Eichler.*

Proof. By Lemma 6.2.1, the reduced discriminant of O is $\frac{D_1 D_2 - x^2}{4}$. Thus if $p \nmid \frac{D_1 D_2 - x^2}{4}$, then O is maximal.

Now, assume that $p \mid \frac{D_1 D_2 - x^2}{4}$, which implies that $p^{1+2v_2(p)} \mid x^2 - D_1 D_2$. From the assumption, it follows that $p \nmid \gcd(D_1, D_2)$, so without loss of generality assume that $p \nmid D_1$.

Take B, ϕ_i as in Remark 6.4.3, and then by Lemma 6.2.1, a general element of O is of the form

$$\begin{aligned}\alpha &= A_0 + A \frac{p_{D_1} + i}{2} + B \frac{p_{D_2} + (xi + k)/D_1}{2} + C \frac{j}{2} \\ &= \left(A_0 + A \frac{p_{D_1}}{2} + B \frac{p_{D_2}}{2} \right) + \left(\frac{A}{2} + \frac{Bx}{2D_1} \right) i + \frac{C}{2} j + \frac{B}{2D_1} k,\end{aligned}$$

for $A_0, A, B, C \in \mathbb{Z}_p$. Therefore

$$\Delta(\alpha) = D_1 \left(A + \frac{Bx}{D_1} \right)^2 + (x^2 - D_1 D_2) C^2 - D_1 (x^2 - D_1 D_2) \frac{B^2}{D_1^2} \quad (6.5.1)$$

$$= D_1 A^2 + 2xAB + D_2 B^2 + (x^2 - D_1 D_2) C^2. \quad (6.5.2)$$

Considering Equation 6.5.1, we find

$$\Delta(\alpha) \equiv D_1 \left(A + \frac{Bx}{D_1} \right)^2 \pmod{p^{1+2v_2(p)}},$$

hence $(O, p) = \{0, \epsilon(p)\}$, which by Lemma 6.5.2 completes the second and third points. \square

Lemma 6.5.3 implies that locally, there is a minimal Eichler order containing $O_{\phi_1, \phi_2, p}$, which is either the order itself, or the unique maximal order it is contained within. Therefore the result is true globally, and we make this a definition.

Definition 6.5.4. Let ϕ_1, ϕ_2 be x -linked embeddings of discriminants D_1, D_2 into B , an indefinite quaternion algebra over \mathbb{Q} or \mathbb{Q}_p , where (D_1, D_2, x) is nice. Then there exists a minimal Eichler order containing O_{ϕ_1, ϕ_2} , denoted $O_{\phi_1, \phi_2}^{\text{Eich}}$.

Since we are concerned with the optimality of embeddings, we need to determine which orders containing $O_{\phi_1, \phi_2}^{\text{Eich}}$ admit ϕ_1, ϕ_2 as optimal embeddings.

Lemma 6.5.5. Let ϕ_1, ϕ_2 be x -linked embeddings of discriminants D_1, D_2 into B , an indefinite quaternion algebra over \mathbb{Q} . Let p be a prime for which $p \mid \frac{D_1}{D_1^{\text{fund}}}$, and let ϕ'_1 be the corresponding embedding of \mathcal{O}_{D_1/p^2} into B that agrees with ϕ_1 on \mathcal{O}_{D_1} . Then (ϕ'_1, ϕ_2) are $\frac{x}{p}$ -linked embeddings into B if and only if $p \mid \frac{D_1 D_2 - x^2}{4}$.

Proof. Since

$$\frac{1}{2} \text{trd} \left(\phi'_1(\sqrt{D_1/p^2}) \phi_2(\sqrt{D_2}) \right) = \frac{x}{p},$$

(ϕ'_1, ϕ_2) are $\frac{x}{p}$ -linked embeddings if and only if $\frac{x}{p}$ is an integer congruent to $\frac{D_1 D_2}{p^2}$ modulo 2.

If (ϕ'_1, ϕ_2) are $\frac{x}{p}$ -linked embeddings, then by Lemma 6.2.1 the reduced discriminant of $O_{\phi'_1, \phi_2}$ is $\frac{D_1 D_2 - x^2}{4p^2}$, which implies that $p \mid \frac{D_1 D_2 - x^2}{4}$, as required.

If $p \mid \frac{D_1 D_2 - x^2}{4}$, first assume that p is odd. Then $p \mid x^2$, whence $p \mid x$, and $\frac{x}{p}$ is an integer congruent to $\frac{D_1 D_2}{p^2}$, as required.

If $p = 2$, then $8 \mid D_1 D_2 - x^2$. If D_2 is even or $8 \mid D_1$, then $8 \mid D_1 D_2$, so $8 \mid x^2$, and hence $4 \mid x$. Therefore $\frac{x}{2} \equiv 0 \equiv \frac{D_1 D_2}{2^2} \pmod{2}$, as required. Otherwise, $4 \nmid D_1$ and D_2 is odd. As $D_1/4$ is a discriminant, it is equivalent to 1 (mod 4), and so $D_1 D_2 \equiv 4 \pmod{16}$. This implies that $x^2 \equiv 4 \pmod{8}$, and so $x \equiv 2 \pmod{4}$. Then $\frac{x}{2} \equiv 1 \equiv \frac{D_1 D_2}{2^2} \pmod{2}$, which completes the proof. \square

We are now able to study the optimality of embeddings in $O_{\phi_1, \phi_2}^{\text{Eich}}$, as well as the level of this order.

Definition 6.5.6. Let D_1, D_2 be discriminants. Define a prime to be *potentially bad* (with respect to D_1, D_2) if

$$p \mid \frac{D_1 D_2}{D_1^{\text{fund}} D_2^{\text{fund}}}.$$

Define $\text{PB}(D_1, D_2)$ to be the product of all potentially bad primes. In particular, D_1 and D_2 are both fundamental if and only if $\text{PB}(D_1, D_2) = 1$.

The embedding pair (ϕ_1, ϕ_2) can only fail to be optimal with respect to a potentially bad prime.

Proposition 6.5.7. Let ϕ_1, ϕ_2 be x -linked embeddings of discriminants D_1, D_2 into B , an indefinite quaternion algebra over \mathbb{Q} , where (D_1, D_2, x) is nice. Factorize

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$.

Then

- (i) The order $O_{\phi_1, \phi_2}^{\text{Eich}}$ is Eichler of level $\prod_{i=1}^t w_i^{g_i}$;

(ii) The embeddings ϕ_1, ϕ_2 are optimal embeddings into $O_{\phi_1, \phi_2}^{\text{Eich}}$ if and only if none of primes p_i and q_i are potentially bad.

Proof. Let $O = O_{\phi_1, \phi_2}$ and $O^{\text{Eich}} = O_{\phi_1, \phi_2}^{\text{Eich}}$. Lemma 6.2.1 computes the reduced discriminant of O to be $\frac{D_1 D_2 - x^2}{4}$, so it suffices to compute the change in reduced discriminant between O and O^{Eich} , which can be done locally. Lemma 6.5.3 implies that $O_p = O_p^{\text{Eich}}$ for $p = w_i$, hence those prime factors remain in the level. For $p = p_i, q_i$, O_p is contained in a unique maximal order, hence those prime factors disappear. This completes the first point.

For optimality, assume that ϕ_1 is not optimal with respect to O^{Eich} . Thus there exists a $p \mid \frac{D_1}{D_1^{\text{fund}}}$ for which $\phi(\mathcal{O}_{D_1/p^2})$ lands inside O^{Eich} . Let ϕ'_1 denote this embedding (which agrees with ϕ on \mathcal{O}_D), and then (ϕ'_1, ϕ_2) are $\frac{x}{p}$ -linked (things remain integral since their images land inside O^{Eich} , which is an order). By definition, we have

$$O \subseteq O_{\phi'_1, \phi_2} \subseteq O^{\text{Eich}},$$

and Lemma 6.2.1 says that the reduced discriminant of $O_{\phi'_1, \phi_2}$ is $\frac{D_1 D_2 - x^2}{4p^2}$. Therefore $p = p_i, q_i, w_i$, so assume that $p = w_i$. By Lemma 6.5.3, $O_p = O_p^{\text{Eich}}$, hence this is equal to $O_{\phi'_1, \phi_2, p}$ as well, which contradicts the fact that the level of $O_{\phi'_1, \phi_2}$ differs from the level of O by the factor p^2 . Therefore $p = p_i$ or $p = q_i$, as claimed.

To finish, it suffices to show that if $p \mid \frac{D_1}{D_1^{\text{fund}}}, \frac{D_1 D_2 - x^2}{4}$ satisfies $\epsilon(p) = -1$, then the embedding ϕ_1 is not optimal into O^{Eich} . As above, let ϕ'_1 denote the embedding of \mathcal{O}_{D_1/p^2} corresponding to ϕ . By Lemma 6.5.5, (ϕ'_1, ϕ_2) are $\frac{x}{p}$ -linked, so by Lemma 6.2.1, $O_{\phi'_1, \phi_2}$ is an order of reduced discriminant $\frac{D_1 D_2 - x^2}{4p^2}$. Since $O \subseteq O_{\phi'_1, \phi_2}$ and O_p is contained in a unique maximal order, this must be the same maximal order that contains $O_{\phi'_1, \phi_2, p}$. Therefore $O_p^{\text{Eich}} = O_{\phi'_1, \phi_2, p}^{\text{Eich}}$, and so ϕ'_1 embeds into O_p^{Eich} , hence it embeds into O^{Eich} , which proves that ϕ_1 is not optimal. \square

To finish off with optimality, we need to consider the optimality of ϕ_1, ϕ_2 into superorders O' of $O_{\phi_1, \phi_2}^{\text{Eich}}$. Assume that none of the p_i, q_i are potentially bad, so that ϕ_1, ϕ_2 are optimal in $O_{\phi_1, \phi_2}^{\text{Eich}}$. The only way that ϕ_1 would fail optimality in O' is if O' admitted the embedding ϕ'_1 of discriminant \mathcal{O}_{D_1/w_j^2} (some $1 \leq j \leq t$) that agrees with ϕ on \mathcal{O}_{D_1} . The pair (ϕ'_1, ϕ_2) is $\frac{x}{w_j}$ -linked by Lemma 6.5.5, and $O_{\phi'_1, \phi_2}^{\text{Eich}}$ is an Eichler order of level $\frac{1}{w_j^2} \prod_{i=1}^t w_i^{g_i}$ by Proposition 6.5.7i. Therefore O' admits ϕ_1 as an optimal embedding if and only if $O' \not\supseteq O_{\phi'_1, \phi_2}^{\text{Eich}}$.

Definition 6.5.8. With notation and assumption as above, let S_{ϕ_1, ϕ_2} be the (possibly empty) set of orders $O_{\phi_1, \phi_2}^{\text{Eich}}$ and $O_{\phi_1, \phi_2'}^{\text{Eich}}$, each of which corresponds to a $1 \leq j \leq t$ for which $w_j \mid \frac{D_1}{D_1^{\text{fund}}}$ or $w_j \mid \frac{D_2}{D_2^{\text{fund}}}$ respectively.

The above discussion is the proof of the following proposition.

Proposition 6.5.9. *Take the notation as in Proposition 6.5.7, and assume that none of p_i, q_i are potentially bad. Then a superorder O' of $O_{\phi_1, \phi_2}^{\text{Eich}}$ admits ϕ_1, ϕ_2 as optimal embeddings if and only if it does not contain any order in S_{ϕ_1, ϕ_2} .*

6.6 Local x-linking with level

Given D_1, D_2, x , Theorem 6.4.2 determines the unique quaternion algebra for which there exists x -linked optimal embeddings. Under the additional restriction of (D_1, D_2, x) being nice, Propositions 6.5.7 and 6.5.9 determine the possible Eichler orders that an x -linked pair of embeddings becomes optimal in. In this section, we study the possible levels of such embeddings.

Lemma 6.6.1. *Let B be a quaternion algebra over $F = \mathbb{Q}$ or \mathbb{Q}_p . Let $v_1, v_2, v_3 \in B$ be such that $\langle 1, v_i, v_j, v_i v_j \rangle_{\mathcal{O}_F}$ is an order for $(i, j) = (1, 2), (1, 3), (2, 3)$. Then*

$$O = \langle 1, v_1, v_2, v_3, v_1 v_2, v_1 v_3, v_2 v_3, v_1 v_2 v_3 \rangle_{\mathcal{O}_F}$$

is an order.

Proof. It suffices to show that any product $v = v_{i_1} \cdots v_{i_k}$ lands in O for any sequence i_1, \dots, i_k with $i_j \in \{1, 2, 3\}$ for all j . This is accomplished via induction: the base case of $k = 0$ is trivial. For the inductive step, assume it is true up to $k - 1 \geq 0$. If $i_j \neq 1$ for all j , then $v \in \langle 1, v_2, v_3, v_2 v_3 \rangle_{\mathcal{O}_F}$ (as this is an order), and we are done. Otherwise, take the last occurrence of 1, say i_m . If $i_{m-1} = 1$, then $v_{i_{m-1}} v_{i_m} = v_1^2 \in \langle 1, v_1 \rangle_{\mathcal{O}_F}$, and by replacing it we are done by induction. Otherwise, if $m > 1$, then $i_{m-1} \neq 1$, and if $i_{m-1} = j$ then $v_{i_{m-1}} v_{i_m} = v_j v_1 \in \langle 1, v_1, v_j, v_1 v_j \rangle_{\mathcal{O}_F}$. By writing $v_{i_{m-1}} v_{i_m}$ in this basis and using induction, we see that it suffices to prove the claim when we swap v_{i_m} and $v_{i_{m-1}}$. By successively repeating this process, we can assume that v starts with a v_1 and has no other terms v_1 . But

then $v_{i_2} \cdots v_{i_k}$ lies in $\langle 1, v_2, v_2, v_2 v_3 \rangle_{\mathcal{O}_F}$, and a left multiplication by v_1 still lands us in O , as desired. \square

The generalization of O_{ϕ_1, ϕ_2} , as found in Lemma 6.2.1, is the following.

Definition 6.6.2. Let ϕ_1, ϕ_2 be x -linked embeddings from $\mathcal{O}_{D_1}, \mathcal{O}_{D_2}$ to B . Let $\ell \in \mathbb{Z}^+$ be such that $\frac{x^2 - D_1 D_2}{\ell^2}$ is a discriminant, and define $O_{\phi_1, \phi_2}(\ell)$ to be the smallest order for which $\mathcal{O}_{D_1}, \mathcal{O}_{D_2}, \mathcal{O}_{(x^2 - D_1 D_2)/\ell^2}$ embed into via $\phi_1, \phi_2, \phi_1 \times \phi_2$ respectively, if it exists.

Lemma 6.6.3. Let $F = \mathbb{Q}$, and with the notation as above, $O_{\phi_1, \phi_2}(\ell)$ exists if and only if $\ell^2 \mid \frac{D_1 D_2 - x^2}{4}$. Furthermore, if (D_1, D_2, x) is nice, then $O_{\phi_1, \phi_2}(\ell)$ has reduced discriminant $\frac{D_1 D_2 - x^2}{4\ell^2}$ when it exists.

Proof. Let $D_3 = \frac{D_1 D_2 - x^2}{\ell^2}$, and let $\phi_3 : \mathcal{O}_{D_3} \rightarrow B$ be the embedding induced by $\phi_1 \times \phi_2$. Let $w_i = \phi_i(\sqrt{D_i})$ and $v_i = \phi_i\left(\frac{p_{D_i} + \sqrt{D_i}}{2}\right)$ for $i = 1, 2, 3$, and let $x = \frac{1}{2} \text{trd}(w_1 w_2) \in p_{D_1 D_2} + 2\mathbb{Z}$ by assumption. We have $w_3 = \frac{w_1 w_2 - x}{\ell}$, whence

$$\frac{1}{2} \text{trd}(w_1 w_3) = \frac{1}{2} \text{trd}\left(\frac{D_1 w_2 - x w_1}{\ell}\right) = 0.$$

Similarly, $\frac{1}{2} \text{trd}(w_2 w_3) = 0$. If D_3 is odd, then this is not in $2\mathbb{Z} + p_{D_3}$, and it will follow that $\langle 1, v_1, v_3, v_1 v_3 \rangle_{\mathbb{Z}}$ is not an order, whence no order exists. Since D_3 is a discriminant, if it is not odd it must be a multiple of 4. In particular, we have that $\ell^2 \mid \frac{D_1 D_2 - x^2}{4}$. In this case, $0 \in 2\mathbb{Z} + p_{D_3}$, and so by Lemma 6.2.1, $\langle 1, v_i, v_j, v_i v_j \rangle_{\mathbb{Z}}$ is an order for $(i, j) = (1, 2), (1, 3), (2, 3)$. Thus by Lemma 6.6.1, $O = \langle 1, v_1, v_2, v_3, v_1 v_2, v_1 v_3, v_2 v_3, v_1 v_2 v_3 \rangle_{\mathbb{Z}}$ is an order, and it is necessarily the smallest order for which ϕ_i embeds into for all $i = 1, 2, 3$.

Now, assume that (D_1, D_2, x) is nice. Let $p_i = p_{D_i}$, and we compute

$$\begin{pmatrix} 1 \\ v_1 \\ v_2 \\ v_3 \\ v_1 v_2 \\ v_1 v_3 \\ v_2 v_3 \\ v_1 v_2 v_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{p_1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{p_2}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{p_1 p_2 + x}{4} & \frac{p_2}{4} & \frac{p_1}{4} & \frac{\ell}{4} \\ 0 & \frac{-x}{4\ell} & \frac{D_1}{4\ell} & \frac{p_1}{4} \\ 0 & \frac{-D_2}{4\ell} & \frac{x}{4\ell} & \frac{p_2}{4} \\ \frac{x^2 - D_1 D_2}{8\ell} & \frac{-p_2 x - p_1 D_2}{8\ell} & \frac{p_1 x + p_2 D_1}{8\ell} & \frac{p_1 p_2 + x}{8} \end{pmatrix} \begin{pmatrix} 1 \\ w_1 \\ w_2 \\ w_3 \end{pmatrix}.$$

Let this transition matrix be M . From the calculation in Lemma 6.2.1, we can compute that $d(1, w_1, w_2, w_3) = \left(\frac{1}{\ell}\right)^2 d(1, w_1, w_2, w_1 w_2) = -\frac{16(D_1 D_2 - x^2)^2}{\ell^2}$. It suffices to show that the rows of M generate a \mathbb{Z} -lattice with determinant $\frac{1}{16\ell}$, as then we have the discriminant of O being $\frac{(D_1 D_2 - x^2)^2}{16\ell^4}$, whence the reduced discriminant is $\frac{D_1 D_2 - x^2}{4\ell^2}$, as desired. The calculation of the row space is done by hand in Appendix A.3. \square

Since $O_{\phi_1, \phi_2} \subseteq O_{\phi_1, \phi_2}(\ell)$, the inclusion holds when we complete at p . Considering Lemma 6.5.3, we find that

- If $p \nmid \frac{D_1 D_2 - x^2}{4}$, then $O_{\phi_1, \phi_2, p}(\ell)$ is maximal;
- If $\epsilon(p) = -1$, then $O_{\phi_1, \phi_2, p}(\ell)$ is contained in a unique maximal order, necessarily the same maximal order as the one containing $O_{\phi_1, \phi_2, p}$;
- If $\epsilon(p) = 1$, then $O_{\phi_1, \phi_2, p}(\ell)$ is Eichler.

In particular, this implies that there exists a minimal Eichler order containing $O_{\phi_1, \phi_2}(\ell)$, denoted $O_{\phi_1, \phi_2}^{\text{Eich}}(\ell)$. Factorize

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$.

The local conditions imply that

$$O_{\phi_1, \phi_2} = O_{\phi_1, \phi_2} \left(\prod_{i=1}^r p_i^{e_i} \prod_{i=1}^s q_i^{f_i} \right),$$

i.e. that the maximum possible level always occurs at the prime factors p of $\frac{D_1 D_2 - x^2}{4}$ for which $\epsilon(p) = -1$. The analogous assessment of the prime factors p for which $\epsilon(p) = 1$ leads to the following proposition.

Proposition 6.6.4. *Let $\ell = \prod_{i=1}^r p_i^{e'_i} \prod_{i=1}^s q_i^{f'_i} \prod_{i=1}^t w_i^{g'_i}$, where $e'_i \leq e_i$, $f'_i \leq f_i$, and $2g'_i \leq g_i$. Then the Eichler order $O_{\phi_1, \phi_2}^{\text{Eich}}(\ell)$ has level $\prod_{i=1}^t w_i^{g_i - 2g'_i}$. Furthermore, assume that all the p_i, q_i are not potentially bad. Let*

$$S = \{w_i : w_i \mid \text{PB}(D_1, D_2)\}$$

be the set of potentially bad primes among the w_i . Then a superorder O' of $O_{\phi_1, \phi_2}^{\text{Eich}}(\ell)$ admits ϕ_1, ϕ_2 as optimal embeddings if and only if O' does not contain $O_{\phi_1, \phi_2}^{\text{Eich}}(w_i)$ for all $w_i \in S$. This is equivalent to $g'_i = 0$ for all i such that $w_i \in S$.

Proof. The first half of the proposition has been proven in the above discussion. For the second half, the optimality of ϕ_1, ϕ_2 can only fail if we have a w_j for which ϕ_1 (without loss of generality) descends to an embedding of \mathcal{O}_{D_1/w_j^2} . Call this embedding ϕ'_1 , and as in Proposition 6.5.7 the order $O_{\phi'_1, \phi_2}^{\text{Eich}}$ has level $\frac{1}{w_j^2} \prod_{i=1}^t w_i^{g_i}$. It suffices to show that $O_{\phi'_1, \phi_2, w_j} = O_{\phi_1, \phi_2, w_j}(w_j)$, as this means that picking up a factor of w_j in the level is equivalent to killing optimality.

These Eichler orders have the same level, so it suffices to show inclusion only. However this is immediate, as the embedding $\phi'_1 \times \phi_2$ corresponds to an embedding of discriminant $\frac{x^2 - D_1 D_2}{p^2}$ induced from

$$\phi'_1(\sqrt{D_1/p^2})\phi_2(\sqrt{D_2}) = \frac{1}{p}\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}).$$

□

An embedding having level exactly ℓ in O' is equivalent to O' containing $O_{\phi_1, \phi_2}(\ell)$ but not containing $O_{\phi_1, \phi_2}(p\ell)$ for any prime p . At long last, we can describe the levels and counts of Eichler orders admitting ϕ_1, ϕ_2 as optimal embeddings.

Theorem 6.6.5. *Let ϕ_1, ϕ_2 be x -linked embeddings of discriminants D_1, D_2 into B , an indefinite quaternion algebra over \mathbb{Q} , let ℓ be a positive integer, and assume that (D_1, D_2, x) is nice. Factorize*

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$.

Then,

- (i) This setup is possible if and only if B is ramified at exactly p_1, p_2, \dots, p_r ;
- (ii) There exists an Eichler order of level \mathfrak{M} for which ϕ_1, ϕ_2 are optimal embeddings into B if and only if both of the following are satisfied:

- None of the p_i, q_i are potentially bad;
- $\mathfrak{M} = \prod_{i=1}^t w_i^{g'_i}$ with $g'_i \leq g_i$.

(iii) Let \mathfrak{M} satisfy the above. The number of Eichler orders of level \mathfrak{M} for which ϕ_1, ϕ_2 are optimal embeddings into is

$$\prod_{i=1}^t \begin{cases} g_i + 1 - g'_i & \text{if } w_i \nmid \text{PB}(D_1, D_2); \\ 2 & \text{if } w_i \mid \text{PB}(D_1, D_2) \text{ and } g'_i < g_i; \\ 1 & \text{if } w_i \mid \text{PB}(D_1, D_2) \text{ and } g'_i = g_i. \end{cases}$$

(iv) There exists an Eichler order of level \mathfrak{M} for which ϕ_1, ϕ_2 are optimal embeddings of into of level exactly ℓ if and only we have

$$\ell = \prod_{i=1}^r p_i^{e_i} \prod_{i=1}^s q_i^{f_i} \prod_{i=1}^t w_i^{g''_i},$$

where $2g''_i \leq g_i - g'_i$ and $g''_i = 0$ if $w_i \mid \text{PB}(D_1, D_2)$.

(v) Let \mathfrak{M}, ℓ satisfy the above. Let n be the number of indices i for which $2g''_i < g_i - g'_i$. Then the number of Eichler orders of level \mathfrak{M} for which ϕ_1, ϕ_2 are optimal embeddings into of level exactly ℓ is 2^n .

Proof. Part i is the content of Theorem 6.4.2, and the necessity of the conditions in part ii follow from Proposition 6.5.7. To complete part ii, it suffices to prove it locally, and Proposition 6.5.9 implies that there is an Eichler order of level $w_i^{g_i-2}$ whose containment must be avoided for each i such that $w_i \mid \text{PB}(D_1, D_2)$ (and no other orders need be avoided).

Recall the inverted triangle of local Eichler orders, as described in Section 4.3. The local Eichler orders containing $O_{\phi_1, \phi_2, w_i}^{\text{Eich}}$ form an inverted triangle with $g_i + 1$ rows. There are $g_i + 1 - n$ Eichler orders of level w_i^n in the n^{th} row of the triangle, starting at $n = 0$ and ending at $n = g_i$. Therefore if $w_i \nmid \text{PB}(D_1, D_2)$, there are $g_i + 1 - g'_i$ possible Eichler orders of level $w_i^{g'_i}$. If $w_i \mid \text{PB}(D_1, D_2)$, then there is one when $g'_i = g_i$, and on all rows above it there are two, as the order that we cannot contain has level $w_i^{g_i-2}$. In particular, this implies part ii as this is a non-zero number.

By the local-global principle for orders (Corollary 4.1.2), the total count for global orders is the product of the local counts. The count in part iii follows from this and the previous paragraph.

For parts iv, v, Proposition 6.6.4 and the discussion surrounding it imply that ℓ has the prime factorization as claimed. The necessity of $2g_i'' \leq g_i - g_i'$ comes from the level of $O_{\phi_1, \phi_2}^{\text{Eich}}(w_i^{g_i''})$ having valuation $g_i - 2g_i''$ at w_i . Proposition 6.6.4 also implies that if $w_i \mid \text{PB}(D_1, D_2)$, then the valuation of ℓ at w_i must be 0, i.e. $g_i'' = 0$.

To count this, we again work locally and use the local-global principle. The local count is unchanged at the primes w_i for which $w_i \mid \text{PB}(D_1, D_2)$. For primes w_i not satisfying this, we no longer have to worry about optimality. The Eichler order $O_{\phi_1, \phi_2, w_i}^{\text{Eich}}(w_i^n)$ has level $w_i^{g_i - 2n}$, and an intersection level is at least that if and only if the order contains $O_{\phi_1, \phi_2, w_i}^{\text{Eich}}(w_i^n)$. Drawing the inverted triangle as before, it follows by induction that

- In level $w_i^{g_i - 2n}$, there are $2n + 1$ orders, of which there are 2 of each embedding level $1, 2, \dots, n - 1$, and one of embedding level n ;
- In level $w_i^{g_i - 2n + 1}$, there are $2n$ orders, of which there are 2 of each embedding level $1, 2, \dots, n$.

In particular, there are 2 orders of embedding level g_i'' when $2g_i'' < g_i - g_i'$, and one when $2g_i'' = g_i - g_i'$. The condition coming from $w_i \mid \text{PB}(D_1, D_2)$ was there are two if $g_i' < g_i$, and one if we had equality. But since $g_i'' = 0$, if $g_i' < g_i$ then $2g_i'' < g_i - g_i'$, hence this condition is absorbed by $2g_i'' < g_i - g_i'$. This completes parts iv, v. □

Chapter 7

Counting intersection numbers

In this chapter, we shift the focus back to studying $\text{Emb}(O, D_1, D_2, x)$, which was the set of equivalence classes of x -linked pairs of optimal embeddings of discriminants D_1, D_2 into O . For a positive integer ℓ , denote $\text{Emb}(O, \phi_1, \phi_2, x, \ell)$ to be the set of pairs $[(\phi'_1, \phi'_2)]$ in $\text{Emb}(O, \phi_1, \phi_2, x)$ which have level ℓ . Define $\text{Emb}(O, D_1, D_2, x, \ell)$ in an analogous fashion. If o_1, o_2 are orientations of optimal embeddings, then attaching the subscript o_1, o_2 to any of the sets defined as $\text{Emb}(\dots)$ means we only take the pairs of optimal embeddings of the specified orientations.

7.1 Total x -linking count into a given Eichler order

As alluded to at the start of Chapter 6, we need to pass between Eichler orders containing a fixed pair of x -linked embeddings, and elements of $\text{Emb}(O, D_1, D_2, x)$. This is accomplished in the “inversion theorem”, which we now set up for.

Let F be \mathbb{Q} or \mathbb{Q}_p , and let B be a quaternion algebra over F of discriminant \mathfrak{D} , which is indefinite if $F = \mathbb{Q}$. Let O be an Eichler order of level \mathfrak{M} in B . Assume that D_1, D_2 are discriminants for which $\text{Emb}(B, D_1, D_2, x)$ is non-empty, fix $[(\phi_1, \phi_2)] \in \text{Emb}(B, D_1, D_2, x)$,

let $\ell^2 \mid \frac{D_1 D_2 - x^2}{4}$, and define

$$T_{\phi_1, \phi_2}(\mathfrak{M}) := \{\mathbb{E} : \mathbb{E} \text{ is an Eichler order of } B \text{ of level } \mathfrak{M}$$

for which ϕ_1, ϕ_2 give optimal embeddings into;\}

$$T_{\phi_1, \phi_2}(\mathfrak{M}, \ell) := \{\mathbb{E} \in T_{\phi_1, \phi_2}(\mathfrak{M}) \text{ such that } (\phi_1, \phi_2) \text{ has level } \ell \text{ in } \mathbb{E}.\}$$

Proposition 7.1.1. *We have*

$$|\text{Emb}(O, D_1, D_2, x, \ell)| = \left| \frac{N_{B^\times}(O)}{F^\times O_{N=1}^\times} \right| |T_{\phi_1, \phi_2}(\mathfrak{M}, \ell)|,$$

and the same result without the ℓ . If $F = \mathbb{Q}$, then

$$\left| \frac{N_{B^\times}(O)}{F^\times O_{N=1}^\times} \right| = 2^{\omega(\mathfrak{M})+1}.$$

Proof. By Corollary 6.1.2 and all Eichler orders of the same level being conjugate, we have that $T_{\phi_1, \phi_2}(\mathfrak{M})$ is non-empty if and only if $S = \text{Emb}(O, D_1, D_2, x)$ is non-empty. In particular, we can assume that (ϕ_1, ϕ_2) give a class in S , and we will use this pair to define a map $\theta : S \rightarrow T_{\phi_1, \phi_2}(\mathfrak{M})$. Given optimal embeddings (ϕ'_1, ϕ'_2) representing a class in S , by Corollary 6.1.2, there exists an $r \in B^\times$ for which $r\phi'_i r^{-1} = \phi_i$ for $i = 1, 2$. Define

$$\theta((\phi'_1, \phi'_2)) = rOr^{-1}.$$

It is clear that $rOr^{-1} \in T_{\phi_1, \phi_2}(\mathfrak{M})$, but we need to check that all choices were well defined. By Corollary 6.1.2, the element r is defined up to multiplication by F^\times , which does not change rOr^{-1} . If $(\phi'_1, \phi'_2) \sim (\phi''_1, \phi''_2)$ in S , then there exists an $s \in O_{N=1}^\times$ for which $\phi'_i = s\phi''_i s^{-1}$ for $i = 1, 2$. The corresponding element r can then be taken to be $r' = rs$, and then $r'Or'^{-1} = rsOs^{-1}r^{-1} = rOr^{-1}$, as desired. Therefore the map θ is well defined.

Next, it is clear that θ is surjective. Indeed, if $\mathbb{E} \in T_{\phi_1, \phi_2}(\mathfrak{M})$, then as all Eichler orders of a given level are conjugate, there exists a $b \in B^\times$ for which $b\mathbb{E}b^{-1} = O$. Then $(\phi^b_1, \phi^b_2) \in S$, and this pair also maps via θ to \mathbb{E} , as desired.

Therefore, it suffices to show that θ is a $\left| \frac{N_{B^\times}(O)}{F^\times O_{N=1}^\times} \right|$ -to-one map. Assume that $\theta((\phi'_1, \phi'_2)) = \theta((\phi''_1, \phi''_2))$, and that the pairs correspond to r, s respectively. Then $rOr^{-1} = sOs^{-1}$, hence $t = r^{-1}s \in N_{B^\times}(O)$. Writing $s = rt$, it follows that $t^{-1}\phi'_i t = \phi''_i$, so it suffices to determine how $t^{-1}(\phi'_1, \phi'_2)t$ varies as t ranges over $N_{B^\times}(O)$. For a fixed t , by Corollary 6.1.2, the set

of elements conjugating (ϕ'_1, ϕ'_2) to any form in the class of $t^{-1}(\phi'_1, \phi'_2)t$ is $O_{N=1}t^{-1}F^\times = t^{-1}F^\times O_{N=1}$. Thus, for distinct t_1, t_2 , they correspond to the same image if and only if

$$t_1^{-1}F^\times O_{N=1} = t_2^{-1}F^\times O_{N=1},$$

which is equivalent to $t_2 t_1^{-1} \in F^\times O_{N=1}$. This proves the first claim without the ℓ . It is clear that the level of intersection remains constant under θ , hence the statements remain true when we add in the level ℓ .

When $F = \mathbb{Q}$, Proposition 4.2.8 yields

$$\frac{N_{B^\times}(O)}{\mathbb{Q}^\times O_{N=1}^\times} \simeq \prod_{p|\mathfrak{D}\mathfrak{M}\infty} \frac{\mathbb{Z}}{2\mathbb{Z}},$$

which implies the final result. \square

Combining Proposition 7.1.1 with Theorem 6.6.5 produces the count of x -linking.

Theorem 7.1.2. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} , let (D_1, D_2, x) be nice, and let ℓ be a positive integer. Factorize*

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where the p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$. Then

(i) *The set $\text{Emb}(O, D_1, D_2, x)$ is non-empty if and only if all of the following hold:*

- $\mathfrak{D} = \prod_{i=1}^r p_i$;
- None of the p_i, q_i are potentially bad;
- $\mathfrak{M} = \prod_{i=1}^t w_i^{g'_i}$ with $g'_i \leq g_i$.

(ii) *Assume the above holds. Then*

$$|\text{Emb}(O, D_1, D_2, x)| = 2^{\omega(\mathfrak{D}\mathfrak{M})+1} \prod_{i=1}^t \begin{cases} g_i + 1 - g'_i & \text{if } w_i \nmid \text{PB}(D_1, D_2); \\ 2 & \text{if } w_i \mid \text{PB}(D_1, D_2) \text{ and } g'_i < g_i; \\ 1 & \text{if } w_i \mid \text{PB}(D_1, D_2) \text{ and } g'_i = g_i. \end{cases}$$

(iii) The set $\text{Emb}(O, D_1, D_2, x, \ell)$ is non-empty if and only if ℓ takes the form

$$\ell = \prod_{i=1}^r p_i^{e_i} \prod_{i=1}^s q_i^{f_i} \prod_{i=1}^t w_i^{g_i''},$$

where $2g_i'' \leq g_i - g_i'$ and $g_i'' = 0$ if $w_i \mid \text{PB}(D_1, D_2)$.

(iv) Assume the above holds. Let n be the number of indices i for which $2g_i'' < g_i - g_i'$. Then

$$|\text{Emb}(O, D_1, D_2, x, \ell)| = 2^{\omega(\mathfrak{D}\mathfrak{M})+n+1}.$$

When we restrict to the case of D_1, D_2 being coprime, fundamental, and O being maximal, Theorem 7.1.2 has a cleaner statement.

Corollary 7.1.3. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} with maximal order O , let D_1, D_2 be coprime fundamental discriminants, let x be an integer with $x^2 \neq D_1 D_2$ and $x \equiv D_1 D_2 \pmod{2}$, and let ℓ be a positive integer. Factorize*

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$.

Then

(i) $\text{Emb}(O, D_1, D_2, x)$ is non-empty if and only if $\mathfrak{D} = \prod_{i=1}^r p_i$;

(ii) Assume the above holds. Then

$$|\text{Emb}(O, D_1, D_2, x)| = 2^{\omega(\mathfrak{D})+1} \prod_{i=1}^t (g_i + 1).$$

(iii) $\text{Emb}(O, D_1, D_2, x, \ell)$ is non-empty if and only if

$$\ell = \prod_{i=1}^r p_i^{e_i} \prod_{i=1}^s q_i^{f_i} \prod_{i=1}^t w_i^{g_i''},$$

where $2g_i'' \leq g_i$.

(iv) Assume the above holds. Let n be the number of indices i for which $2g_i'' < g_i$. Then

$$|\text{Emb}(O, D_1, D_2, x, \ell)| = 2^{r+n+1}.$$

7.2 Orientations and sign of intersection

In this and the previous chapter, the orientations of optimal embeddings and the sign of intersection has been completely ignored; we now address this issue.

Lemma 7.2.1. *Let B be an indefinite quaternion algebra over \mathbb{Q} , let O be an Eichler order of level \mathfrak{M} , let (ϕ_1, ϕ_2) be x -linked optimal embeddings of positive discriminants D_1, D_2 respectively, where $x^2 < D_1 D_2$, let $v \mid \mathfrak{D}\mathfrak{M}\infty$, and let $\omega_v \in N_B^\times(O)$ be as in Proposition 4.4.23. Then $(\phi_1^{w_v}, \phi_2^{w_v})$ is an x -linked pair of optimal embeddings into O with the same level as (ϕ_1, ϕ_2) . Furthermore,*

- *If $v = \infty$ then the orientations are the same, but the sign of intersection is opposite.*
- *If $v < \infty$, then the orientations are negated at v only, and the sign of intersection is the same.*

Proof. It is clear that $(\phi_1^{w_v}, \phi_2^{w_v})$ remains x -linked, optimal, and the orientation follows from Proposition 4.4.23. Having opposite sign of intersection is equivalent to $\phi_1 \times \phi_2$ swapping orientation at ∞ when conjugating by w_v , and this also follows from Proposition 4.4.23. \square

In particular, any element of $O_{N=-1}$ acts as an involution on $\text{Emb}_{o_1, o_2}(O, D_1, D_2, x, \ell)$, dividing it into equal sized sets of intersection sign being 1 and -1 .

Definition 7.2.2. For any intersection set $\text{Emb}(\dots)$ or $\text{Emb}_{o_1, o_2}(\dots)$, use the superscript $+$ to denote the embeddings with positive sign of intersection, and use $-$ for negative sign of intersection. For example, $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)$ counts the equivalence classes of pairs $[(\phi_1, \phi_2)]$ of optimal embeddings of discriminants D_1, D_2 and orientations o_1, o_2 that are x -linked of level ℓ with positive sign.

Lemma 7.2.3. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} , let D_1, D_2 be positive discriminants, and let x be an integer such that $x^2 \neq D_1 D_2$ and $x \equiv D_1 D_2 \pmod{2}$. Assume that $\text{Emb}(O, D_1, D_2, x)$ is non-empty, let o_1 be a possible orientation of an optimal embedding of \mathcal{O}_{D_1} into O , and assume that $\gcd(D_1 D_2, \mathfrak{M}) = 1$. Then there exists a $[(\phi_1, \phi_2)] \in \text{Emb}(O, D_1, D_2, x)$ for which ϕ_1 has orientation o_1 . For each $p \mid \mathfrak{D}\mathfrak{M}$, we also have:*

- If $p \nmid D_1$, then $o_p(\phi_2)$ is uniquely determined;
- If $p \mid D_1$ but $p \nmid D_2$, then $o_p(\phi_1)$ can be both 1 and -1 .

Finally, the sets $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)$ all have the same size when they are non-empty.

Proof. Start with $[(\phi'_1, \phi'_2)] \in \text{Emb}(O, D_1, D_2, x)$, and from Lemma 7.2.1 we can conjugate the pair by ω_p for $p \mid \mathfrak{DM}$ to get (ϕ_1, ϕ_2) with ϕ_1 having orientation o_1 .

If $p \mid D_1$ but $p \nmid D_2$, the local orientation result follows from conjugating the embeddings by ω_p , as $o_p(\phi_1) = 0$.

Next, assume $p \nmid D_1$. It suffices to prove this lemma locally, so first assume we have $p \mid \mathfrak{D}$, i.e. $B_p = \text{QA}_p^{\text{div}}$. As in the proof of Lemma 6.3.2, write $B_p = \left(\frac{D_1, e}{\mathbb{Q}_p} \right)$, with $\phi_{1,p}(\sqrt{D_1}) = i$ and $(D_1, e)_p = -1$. Let $\phi_{2,p}(\sqrt{D_2}) = fi + gj + hk$ for $f, g, h \in \mathbb{Z}_p$ necessarily, and the trace condition gives that $f = \frac{x}{D_1}$. Let \mathfrak{p} be the maximal order in O_p , and then $\phi_{2,p}(\sqrt{D_2}) \equiv \frac{x}{D_1}i \pmod{\mathfrak{p}}$, which only depends on x, D_1 . Therefore the local orientation of ϕ_2 at p is fixed.

Otherwise, assume that $B_p = \text{Mat}(2, \mathbb{Q}_p)$, and O_p is the standard Eichler level of order p^e with $e > 0$. Let $e_1 = e + v_2(p)$, and then working modulo p^{e_1} we write

$$\phi_1(\sqrt{D_1}) \equiv \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix} \pmod{p^{e_1}}, \quad \phi_2(\sqrt{D_2}) \equiv \begin{pmatrix} c & d \\ 0 & -c \end{pmatrix} \pmod{p^{e_1}}.$$

Therefore $x \equiv ac \pmod{p^{e_1}}$, and since $p \nmid a$ (else $p \mid D_1$), we have $c \equiv \frac{x}{a} \pmod{p^{e_1}}$. But this is the definition of the orientation of ϕ_2 , namely the equivalence class of c modulo $p^{1+v_2(p)}$ is determined from x and the orientation of ϕ_1 (which is $a \pmod{p^{1+v_2(p)}}$). Therefore the local orientations statements follow.

Finally, the above shows that we can pass between all pairs (o_1, o_2) for which $\text{Emb}_{o_1, o_2}(O, D_1, D_2, x, \ell)$ is non-empty via conjugation by ω_p for $p \mid \mathfrak{DM}$, hence these sets all have the same size. Exactly half of the pairs in a given set have positive intersection sign, which completes the lemma. \square

We can say even more about how the possible x 's divide across a pair of orientations.

Proposition 7.2.4. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} , let D_1, D_2 be positive discriminants, and let o_1, o_2 be*

possible orientations of optimal embeddings of discriminants D_1, D_2 into O . Then there exists an integer x_{o_1, o_2} such that for all optimal embeddings $\phi_i \in \text{Emb}_{o_i}(O, D_i)$ ($i = 1, 2$), we have

$$x_{o_1, o_2} \equiv \frac{1}{2} \text{trd} \left(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) \right) \pmod{2\mathfrak{DM}}.$$

In particular, the possible x -linkings across an orientation pair are all equivalent modulo $2\mathfrak{DM}$.

Proof. Fix another pair $\phi'_i \in \text{Emb}_{o_i}(O, D_i)$, and say that ϕ_1, ϕ_2 are x -linked and ϕ'_1, ϕ'_2 are x' -linked. It suffices to show that $x \equiv x' \pmod{2\mathfrak{DM}}$. We can work locally, so start with $p \mid \mathfrak{D}$, and assume that ϕ_i, ϕ'_i now land in O_p . Let \mathfrak{p} be the unique maximal order of O_p , and as the embeddings have the same orientation, there exists $u_1, u_2 \in O_{p, N=1}$ for which $\phi'_i = \phi_i^{u_i}$ for $i = 1, 2$. Since $O_p/\mathfrak{p} \simeq \mathbb{F}_{p^2}$ is commutative, when working modulo \mathfrak{p} we can rearrange terms freely. Thus

$$\phi_1^{u_1} \left(\frac{p_{D_1} + \sqrt{D_1}}{2} \right) \phi_2^{u_2} \left(\frac{p_{D_2} + \sqrt{D_2}}{2} \right) \equiv \phi_1 \left(\frac{p_{D_1} + \sqrt{D_1}}{2} \right) \phi_2 \left(\frac{p_{D_2} + \sqrt{D_2}}{2} \right) \pmod{\mathfrak{p}}.$$

Taking reduced traces implies that

$$\frac{p_{D_1}p_{D_2} + x'}{2} \equiv \frac{p_{D_1}p_{D_2} + x}{2} \pmod{\mathfrak{p}}.$$

If $p \neq 2$, it follows that $x' \equiv x \pmod{\mathfrak{p}}$, whence $x' \equiv x \pmod{p}$ by subtracting and taking the norm. If $p = 2$, then $x' \equiv x \pmod{2\mathfrak{p}}$, and so subtracting and taking norms gives $8 \mid (x' - x)^2$, hence $x \equiv x' \pmod{4}$.

Next, assume that $p^e \parallel \mathfrak{M}$ with $e > 0$, and assume that O_p is the standard Eichler order of level p^e . As the embeddings have the same orientation, there exists $u_1, u_2 \in O_{p, N=1}$ for which $\phi'_i = \phi_i^{u_i}$ for $i = 1, 2$. Explicitly write

$$\phi_i \left(\frac{p_{D_i} + \sqrt{D_i}}{2} \right) = \begin{pmatrix} a_i & b_i \\ p^e c_i & p_{D_i} - a_i \end{pmatrix}, \quad u_i = \begin{pmatrix} f_i & g_i \\ p^e h_i & k_i \end{pmatrix}.$$

It follows that $f_i k_i \equiv 1 \pmod{p^e}$. Modulo p^e , we compute

$$\phi_i^{u_i} \left(\frac{p_{D_i} + \sqrt{D_i}}{2} \right) \equiv \begin{pmatrix} a_i & f_i(p_{D_i}g_i - 2g_ia_i + f_ib_i) \\ 0 & p_{D_i} - a_i \end{pmatrix} \pmod{p^e}.$$

By taking the explicit expressions for $\phi_i\left(\frac{p_{D_i} + \sqrt{D_i}}{2}\right)$, doubling and subtracting p_{D_i} , and multiplying together we find that

$$x \equiv (2a_1 - p_{D_1})(2a_2 - p_{D_2}) \equiv x' \pmod{p^{e+v_2(p)}},$$

as claimed.

Combining the above shows that $x \equiv x' \pmod{2\mathfrak{DM}}$ if $2 \mid \mathfrak{DM}$, and $x \equiv x' \pmod{\mathfrak{DM}}$ otherwise. In this case, $x \equiv p_{D_1}p_{D_2} \equiv x' \pmod{2}$, so the same conclusion follows. \square

If D_1 is coprime to \mathfrak{DM} , then Lemma 7.2.3 and Proposition 7.2.4 can be used to show that for o_1 fixed, the integers x_{o_1, o_2} are all distinct modulo $2\mathfrak{DM}$ across all orientations o_2 . If D_1 has factors in common with \mathfrak{DM} , this no longer needs to be true at those primes. Furthermore, not all x 's satisfying the congruence condition will necessarily appear as x -linkings, as this depends on the actual factorization of $\frac{D_1 D_2 - x^2}{4}$, and not just on congruences. For example, this number will always be divisible by \mathfrak{DM} , but prime factors of \mathfrak{D} could appear to even powers.

Lemma 7.2.3 allows us to count the sizes of $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)$, by dividing $|\text{Emb}^+(O, D_1, D_2, x, \ell)|$ across the total number of orientations. We record this in the next Corollary.

Corollary 7.2.5. *Let B be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} , let (D_1, D_2, x) be nice, and let ℓ be a positive integer.*

Factorize

$$\frac{D_1 D_2 - x^2}{4} = \pm \prod_{i=1}^r p_i^{2e_i+1} \prod_{i=1}^s q_i^{2f_i} \prod_{i=1}^t w_i^{g_i},$$

where the p_i are the primes for which $\epsilon(p_i) = -1$ that appear to an odd power, q_i are the primes for which $\epsilon(q_i) = -1$ that appear to an even power, and w_i are the primes for which $\epsilon(w_i) = 1$. Assume that

- $\mathfrak{D} = \prod_{i=1}^r p_i$;
- $\gcd(\mathfrak{M}, D_1 D_2) = 1$ and $\gcd(\mathfrak{D}, \text{PB}(D_1, D_2)) = 1$;
- $\mathfrak{M} = \prod_{i=1}^t w_i^{g'_i}$ with $g'_i \leq g_i$.
- $\ell = \prod_{i=1}^r p_i^{e_i} \prod_{i=1}^s q_i^{f_i} \prod_{i=1}^t w_i^{g''_i}$, where $2g''_i \leq g_i - g'_i$ and $g''_i = 0$ if $w_i \mid \text{PB}(D_1, D_2)$.

Let n be the number of indices i for which $2g_i'' < g_i - g_i'$. Then for every pair of orientations (o_1, o_2) , we have

$$|\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)| = 2^n \text{ or } 0.$$

Proof. By Theorem 7.1.2, the count without the orientations or $+$ is $2^{\omega(\mathfrak{DM})+n+1}$. If $p \mid \mathfrak{DM}$ but $p \nmid \gcd(D_1, D_2)$, then Lemma 7.2.3 implies that there are precisely 2 pairs $(o_p(\phi_1), o_p(\phi_2))$ which admit x -linking, hence we divide by 2 for all such p . But the assumption of (D_1, D_2, x) nice implies that this is all primes $p \mid \mathfrak{DM}$, so the factor $\omega(\mathfrak{DM})$ is eliminated. Finally, exactly half of the embeddings have positive sign, which implies the result. \square

7.3 Specializing to pairs of embeddings and summing over \mathbf{x}

We started with the question of finding intersections of $\tilde{\ell}_{\phi_1}, \tilde{\ell}_{\phi_2}$ where ϕ_1, ϕ_2 are optimal embeddings of discriminants D_1, D_2 , and instead answered the related problem of describing the sets $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)$. Accessing the original information boils down to:

- Identifying which values of x with $x^2 < D_1 D_2$ give x -linking with embeddings similar to ϕ_1, ϕ_2 . Proposition 7.2.4 identifies the residue class modulo $2\mathfrak{DM}$ that x must lie in, but not all such x are valid.
- For each of these x 's, identifying how many of the x -linked pairs drop into the equivalence classes of ϕ_1, ϕ_2 , out of the $h^+(D_1)h^+(D_2)$ possible class pairs.
- Identifying the corresponding signs and levels of the x -linked pairs equivalent to ϕ_1, ϕ_2 .

All of these steps are possible algorithmically, and we explore this in Section 10.3.2. Theoretically, this is much more difficult. For a fixed x , it is possible to partially describe how elements in $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x)$ distribute:

- Fix $[(\phi_1, \phi_2)] \in \text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x)$. Then the map θ found in Proposition 7.1.1 combined with the work on $T_{\phi_1, \phi_2}(\mathfrak{M})$ in Chapter 6 allows us to describe possible values of $\text{nrd}(r)$ for $r \in O$ such that $[(\phi_1^r, \phi_2^r)] \in \text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x)$ and $[(\phi_1^r, \phi_2^r)] \neq$

$[(\phi_1, \phi_2)]$; they are essentially products of powers of prime divisors p of $\frac{D_1 D_2 - x^2}{4}$ with $\epsilon(p) = 1$.

- Proposition 4.5.2 describes the element of the narrow class groups taking ϕ_i to ϕ_i^r in terms of the reduced norms of elements that conjugate ϕ_i to ϕ_i^r .
- In particular, the distribution of $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x)$ across the $h^+(D_1)h^+(D_2)$ pairs of equivalence classes relates to the representations of products of primes $p \mid \frac{D_1 D_2 - x^2}{4}$ with $\epsilon(p) = 1$ by binary quadratic forms of discriminants D_1, D_2 .

While it is possible to make this a bit more formal and explicit, this only works for a fixed x . It is not clear how classes from distinct x 's interact, and this is the main theoretical barrier to this approach.

7.4 Examples

We now present a few examples that illustrate the results of Theorem 7.1.2 and Corollary 7.2.5.

Example 7.4.1. Let $D_1 = 5$ and $D_2 = 381$, so that D_1, D_2 are coprime and fundamental. Since $43 < \sqrt{5 \cdot 381} < 44$, to compute which algebras admit non-trivial linking of D_1, D_2 , it suffices to compute $\frac{5 \cdot 381 - x^2}{4}$ for odd $|x| \leq 43$, and find $\epsilon(p)$ for all prime divisors. The values of $\epsilon(p)$ with $p \leq 100$ are in Table 7.1

Table 7.1: $\epsilon(p)$ for $D_1 = 5, D_2 = 381, p \leq 100$.

| | | | | | | | | | | | | | | | | |
|---------------|----|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|
| p | 2 | 3 | 5 | 7 | 17 | 19 | 29 | 31 | 43 | 47 | 59 | 61 | 67 | 79 | 89 | 97 |
| $\epsilon(p)$ | -1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | 1 | -1 |

Table 7.2 displays the possible ramifications of the quaternion algebras, along with the corresponding positive x 's (since x and $-x$ correspond to the same algebra).

Table 7.2: Quaternion algebras admitting non-trivial linking in a maximal order for discriminants 5 and 381.

| | | | | | | |
|------------------|---------------|------------------|----------------|-------|-------|-------|
| Ramifying primes | \emptyset | 2, 3 | 2, 7 | 2, 17 | 2, 43 | 2, 47 |
| Positive x 's | 7, 17, 25, 31 | 3, 9, 21, 27, 39 | 13, 29, 41, 43 | 35 | 23 | 5 |
| Ramifying primes | 2, 67 | 2, 193 | 2, 223 | 3, 7 | 3, 17 | 7, 17 |
| Positive x 's | 37 | 19 | 11 | 15 | 33 | 1 |

Let's focus on $Q = \left(\frac{3,-1}{\mathbb{Q}}\right)$, which is ramified at 2, 3. Let O be the maximal order spanned by $\{1, i, j, \frac{1+i+j+k}{2}\}$. Since $h^+(5) = 1$ and there are four orientations, there are 4 embedding classes of discriminant 5. Since $h^+(381) = 2$ and $3 \mid 381$, there are two orientations, and 4 total embedding classes of discriminant 381. Representative embeddings are given in Table 7.3.

Table 7.3: Optimal embedding classes for $D = 5, 381$.

| D | $o_2(\phi)$ | $o_3(\phi)$ | $\phi\left(\frac{p_D + \sqrt{D}}{2}\right)$ |
|-----|-------------|-------------|---|
| 5 | 1 | 1 | $\frac{1-i-j+k}{2}$ |
| 5 | -1 | 1 | $\frac{1-i-j-k}{2}$ |
| 5 | 1 | -1 | $\frac{1+i+j+k}{2}$ |
| 5 | -1 | -1 | $\frac{1+i+j-k}{2}$ |
| 381 | 1 | 0 | $\frac{1-11i-3j+3k}{2}$ |
| 381 | 1 | 0 | $\frac{1+9i-3j+7k}{2}$ |
| 381 | -1 | 0 | $\frac{1-11i-3j-3k}{2}$ |
| 381 | -1 | 0 | $\frac{1+9i-3j-7k}{2}$ |

The possible x 's are $|x| = \{3, 9, 21, 27, 39\}$. For each x , we factor $\frac{5 \cdot 381 - x^2}{4}$ in Table 7.4, and determine the possible levels.

Table 7.4: Factorization of $\frac{5 \cdot 381 - x^2}{4}$ for $|x| = \{3, 9, 21, 27, 39\}$.

| $ x $ | $\frac{5 \cdot 381 - x^2}{4}$ | $\prod p_i^{e_i}$ | $\prod q_i^{f_i}$ | $\prod w_i^{g_i}$ | Possible levels | n |
|-------|-------------------------------|-------------------|-------------------|-------------------|-----------------|-----|
| 3 | 474 | $2^1 3^1$ | | 79^1 | 1 | 1 |
| 9 | 456 | $2^3 3^1$ | | 19^1 | 2 | 1 |
| 21 | 366 | $2^1 3^1$ | | 61^1 | 1 | 1 |
| 27 | 294 | $2^1 3^1$ | 7^2 | | 7 | 0 |
| 39 | 96 | $2^5 3^1$ | | | 4 | 0 |

It turned out that each x corresponds to a unique level, but this will not be the case in general. This data says that $|\text{Emb}_{\sigma_1, \sigma_2}^+(O, 5, 381, x, \ell)|$ should be 0 or 2 for the first three entries and 0 or 1 for the last two entries. Let ϕ_1 be the first embedding of discriminant 5 as given in Table 7.3, and let σ_1, σ_2 be the first two embeddings of discriminant 381 as given in the same table. For each intersection of ϕ_1 with σ_i , we take a pair (ϕ'_1, σ_i) representing the intersection, and record the data in Table 7.5 (the signed level is the product of the sign and the level).

Table 7.5: Intersection of ϕ_1 with σ_1, σ_2 .

| Intersections with σ_1 | | | Intersections with σ_2 | | |
|---|-----|--------------|---|-----|--------------|
| $\phi'_1 \left(\frac{1+\sqrt{5}}{2} \right)$ | x | Signed level | $\phi'_1 \left(\frac{1+\sqrt{5}}{2} \right)$ | x | Signed level |
| $\frac{1-13i-55j-29k}{2}$ | 3 | -1 | $\frac{1+i-j-k}{2}$ | 3 | 1 |
| $\frac{1-13i+197j-113k}{2}$ | 3 | -1 | $\frac{1+101i+359j-181k}{2}$ | 3 | 1 |
| $\frac{1+31i+131j+69k}{2}$ | -9 | 2 | $\frac{1-i-j+k}{2}$ | -9 | -2 |
| $\frac{1+31i-469j+269k}{2}$ | -9 | 2 | $\frac{1-41i-145j+73k}{2}$ | -9 | -2 |
| $\frac{1-87i-373j-197k}{2}$ | -21 | -1 | $\frac{1+i+5j-3k}{2}$ | -21 | 1 |
| $\frac{1-711i-3031j-1599k}{2}$ | -21 | -1 | $\frac{1+11i+41j-21k}{2}$ | -21 | 1 |
| $\frac{1+223i+953j+503k}{2}$ | 27 | 7 | $\frac{1-3i-13j+7k}{2}$ | 27 | -7 |
| $\frac{1-i-j+k}{2}$ | 39 | 4 | $\frac{1-29i+71j+29k}{2}$ | 39 | -4 |

This data agrees with the theoretical claim. For the other orientation of 381, we have essentially the same data, except the x 's are all negated.

For another interesting example, we consider a non-maximal Eichler order, and compare it to the results for the maximal order.

Example 7.4.2. Let $D_1 = 73$, $D_2 = 937$, and $x = 89$. Then D_1, D_2 are coprime, fundamental, and have class number 1 each. Let $Q = \left(\frac{7,5}{\mathbb{Q}}\right)$, which is ramified at 5, 7. Let O be a maximal order and O^3 an Eichler order of level 3, given by

$$O = \left\langle 1, \frac{1+j}{2}, i, \frac{1+i+j+k}{2} \right\rangle, \quad O^3 = \left\langle 1, i, \frac{1+3j}{2}, \frac{1+i+j+k}{2} \right\rangle.$$

There are 4 embedding classes into O and 8 embedding classes into O^3 of each discriminant, each corresponding to a distinct orientation. Since

$$\frac{73 \cdot 937 - 89^2}{4} = (5^1 7^1) (2^4 3^3),$$

with $\epsilon(5) = \epsilon(7) = -1$ and $\epsilon(2) = \epsilon(3) = 1$ (the empty parentheses indicate the absence of q_i 's), the sets $\text{Emb}(O', 73, 937, 89)$ should be non-empty for $O' = O, O^3$. Fix the optimal embeddings

$$\phi_1 \left(\frac{1 + \sqrt{73}}{2} \right) = \frac{1 - 2i + 3j}{2}, \quad \phi_2 \left(\frac{1 + \sqrt{937}}{2} \right) = \frac{1 + 14i + 5j - 4k}{2},$$

which land in and are optimal with respect to both O and O^3 . Since

$$\frac{1}{2} \text{trd}(\phi_1(\sqrt{73})\phi_2(\sqrt{937})) = -121 \equiv 89 \pmod{2 \cdot 3 \cdot 5 \cdot 7},$$

$\text{Int}(\phi_1, \phi_2)$ should have 89-linkage. As the class numbers are both one, this is all of the 89-linkage for the given orientations. Corollary 7.2.5 predicts the levels and counts, which is recorded in Table 7.6.

Table 7.6: Theoretical prediction for counts of levels.

| ℓ | $ \text{Emb}_{o_1, o_2}^+(O, 73, 937, 89, \ell) $ | $ \text{Emb}_{o_1, o_2}^+(O^3, 73, 937, 89, \ell) $ |
|--------|---|---|
| 1 | 4 | 4 |
| 2 | 4 | 4 |
| 3 | 4 | 2 |
| 4 | 2 | 2 |
| 6 | 4 | 2 |
| 12 | 2 | 1 |

The difference in counts comes only at $w_i = 3$, where $2g_i'' < g_i - g_i' = 3 - g_i'$ is true for $g_i'' = 0, 1$ when the level is maximal, but is only true for $g_i'' = 0$ when $g_i' = 1$, i.e. the Eichler order of level 3.

We compute the 89–linkage using the algorithm described in Section 10.3.2. For each intersection with positive sign, we take a representative pair (ϕ_1, ϕ_2') , and record ϕ_2' and the level in Tables 7.7 and 7.8

Table 7.7: Positive 89–linking of ϕ_1 with ϕ_2 in O .

| $\phi_2' \left(\frac{1+\sqrt{937}}{2} \right)$ | ℓ | $\phi_2' \left(\frac{1+\sqrt{937}}{2} \right)$ | ℓ |
|---|--------|---|--------|
| $\frac{1+22559i+21061j-12851k}{2}$ | 1 | $\frac{1+119i+117j-69k}{2}$ | 3 |
| $\frac{1+1769i+1657j-1009k}{2}$ | 1 | $\frac{1+1428689i+1333449j-813783k}{2}$ | 3 |
| $\frac{1+1769i+1657j+1009k}{2}$ | 1 | $\frac{1+14i+19j-8k}{2}$ | 4 |
| $\frac{1+22559i+21061j+12851k}{2}$ | 1 | $\frac{1+14i+19j+8k}{2}$ | 4 |
| $\frac{1+584i+551j+334k}{2}$ | 2 | $\frac{1+6907484i+6446991j-3934506k}{2}$ | 6 |
| $\frac{1+584i+551j-334k}{2}$ | 2 | $\frac{1+4664i+4359j+2658k}{2}$ | 6 |
| $\frac{1+44i+47j+26k}{2}$ | 2 | $\frac{1+6907484i+6446991j+3934506k}{2}$ | 6 |
| $\frac{1+44i+47j-26k}{2}$ | 2 | $\frac{1+4664i+4359j-2658k}{2}$ | 6 |
| $\frac{1+119i+117j+69k}{2}$ | 3 | $\frac{1+179534i+167571j-102264k}{2}$ | 12 |
| $\frac{1+1428689i+1333449j+813783k}{2}$ | 3 | $\frac{1+179534i+167571j+102264k}{2}$ | 12 |

Table 7.8: Positive 89–linking of ϕ_1 with ϕ_2 in O^3 .

| $\phi_2' \left(\frac{1+\sqrt{937}}{2} \right)$ | ℓ | $\phi_2' \left(\frac{1+\sqrt{937}}{2} \right)$ | ℓ |
|---|--------|---|--------|
| $\frac{1+1769i+1657j+1009k}{2}$ | 1 | $\frac{1+1428689i+1333449j+813783k}{2}$ | 3 |
| $\frac{1+119i+117j+69k}{2}$ | 1 | $\frac{1+119i+117j-69k}{2}$ | 3 |
| $\frac{1+1428689i+1333449j-813783k}{2}$ | 1 | $\frac{1+14i+19j-8k}{2}$ | 4 |
| $\frac{1+22559i+21061j-12851k}{2}$ | 1 | $\frac{1+179534i+167571j+102264k}{2}$ | 4 |
| $\frac{1+44i+47j+26k}{2}$ | 2 | $\frac{1+6907484i+6446991j-3934506k}{2}$ | 6 |
| $\frac{1+584i+551j-334k}{2}$ | 2 | $\frac{1+4664i+4359j-2658k}{2}$ | 6 |
| $\frac{1+6907484i+6446991j+3934506k}{2}$ | 2 | $\frac{1+179534i+167571j-102264k}{2}$ | 12 |
| $\frac{1+4664i+4359j+2658k}{2}$ | 2 | | |

This data agrees with Table 7.6.

For a final example, we introduce a non-fundamental discriminant.

Example 7.4.3. Let $D_1 = 241$ and $D_2 = 2736$, which are coprime, and let $x = 324$. Note that D_1 is fundamental, but $D_2 = 2^2 3^2 76$, where 76 is fundamental. Take $Q = \left(\frac{77,-1}{\mathbb{Q}} \right)$, which is ramified at 7, 11. Let O be the maximal order spanned by $\left\{ 1, \frac{1+i}{2}, j, \frac{j+k}{2} \right\}$. We have $h^+(241) = 1$ and $h^+(2736) = 4$, and consider the 5 optimal embeddings in Table 7.9 (one being of discriminant 241, and the other 4 being one entire orientation of discriminant 2736).

Table 7.9: Optimal embedding classes for $D = 241, 2736$.

| Label | D | $o_7(\phi)$ | $o_{11}(\phi)$ | $\phi \left(\frac{p_D + \sqrt{D}}{2} \right)$ |
|------------|------|-------------|----------------|--|
| ϕ | 241 | 1 | 1 | $\frac{1+i-12j+2k}{2}$ |
| σ_1 | 2736 | 1 | 1 | $\frac{2i-50j+8k}{2}$ |
| σ_2 | 2736 | 1 | 1 | $\frac{10i-281j+31k}{2}$ |
| σ_3 | 2736 | 1 | 1 | $\frac{2i-50j-8k}{2}$ |
| σ_4 | 2736 | 1 | 1 | $\frac{10i-281j-31k}{2}$ |

Factorize

$$\frac{241 \cdot 2736 - 324^2}{4} = (7^1 11^1) (2^3 3^2 5^2),$$

where $\epsilon(7) = \epsilon(11) = -1$ and $\epsilon(2) = \epsilon(3) = \epsilon(5) = 1$. As $PB(241, 2736) = 2 \cdot 3$, factors of 2, 3 are not allowed in the level. In particular, for 324–linking, the only valid levels are 1, 5 (whereas if D_1, D_2 were fundamental, we could get all divisors of 30). The table of predicted levels and counts is found in Table 7.10.

Table 7.10: Theoretical prediction for counts of levels.

| ℓ | $ \text{Emb}_{o_1, o_2}^+(O, 241, 2736, 324, \ell) $ |
|--------|--|
| 1 | 8 |
| 5 | 4 |

Since

$$\frac{1}{2} \text{trd}(\phi(\sqrt{241})\sigma_1(\sqrt{2736})) = 786 \equiv 324 \pmod{2 \cdot 7 \cdot 11},$$

intersections of ϕ with σ_i should exhibit the above 324–linking behaviour. We compute the possible positive 324–linking between ϕ and σ_i for $i = 1, 2, 3, 4$, and represent each intersection by a pair (ϕ', σ_i) . The corresponding data is found in Table 7.11.

Table 7.11: Positive 324–linking of ϕ_1 with σ_i .

| i | $\phi'_1\left(\frac{1+\sqrt{241}}{2}\right)$ | ℓ | i | $\phi'_1\left(\frac{1+\sqrt{241}}{2}\right)$ | ℓ |
|-----|--|--------|-----|--|--------|
| 1 | $\frac{1+51079i+839827j-80937k}{2}$ | 1 | 3 | $\frac{1-5i-89j-9k}{2}$ | 1 |
| 1 | $\frac{1+39i-397j+23k}{2}$ | 1 | 3 | $\frac{1-449i+4531j+255k}{2}$ | 1 |
| 1 | $\frac{1+2433i-24575j+1387k}{2}$ | 5 | 3 | $\frac{1-7i+65j+3k}{2}$ | 5 |
| 2 | $\frac{1-17i+1220j-138k}{2}$ | 1 | 4 | $\frac{1-87657i+1615987j+161959k}{2}$ | 1 |
| 2 | $\frac{1+259i-4786j+480k}{2}$ | 1 | 4 | $\frac{1-21i+373j+37k}{2}$ | 1 |
| 2 | $\frac{1+5i-89j+9k}{2}$ | 5 | 4 | $\frac{1-1395i+25706j+2576k}{2}$ | 5 |

This data agrees with the theoretical claim.

Chapter 8

Hecke operators and modularity

Previously, we studied intersection numbers by adapting the point of view of algebraic equations and identities in a quaternion algebra, which were then studied by looking locally and using the local-global principle. In this chapter we take advantage of a different point of view, namely a topological one. The signed intersection number is very special in the sense that it is defined not just on root geodesics coming from pairs of optimal embeddings, but on pairs of homology classes! By exploiting the topological view and translating it to quaternion algebras, we will produce modular forms.

In this section, fix B to be an indefinite quaternion algebra over \mathbb{Q} of discriminant \mathfrak{D} , let O be an Eichler order of level \mathfrak{M} , and let $\phi_i : \mathcal{O}_{D_i} \rightarrow O$ be optimal embeddings of positive discriminants for $i = 1, 2$.

Definition 8.0.1. Let $\text{Emb}(O)$ denote \mathbb{Z} -linear formal sums of equivalence classes of optimal embeddings of quadratic orders into O . Denote by $\text{Emb}^+(O)$ the subspace supported on optimal embeddings of positive discriminants, and denote by $\text{Emb}^-(O)$ the subspace supported on optimal embeddings of negative discriminants.

Remark 8.0.2. The intersection number Int_O can be thought of as a mapping

$$\text{Emb}^+(O) \times \text{Emb}^+(O) \rightarrow \mathbb{Z},$$

by summing up the pairs of intersection numbers multiplied by the coefficients. Furthermore, one can even think of the image as being $\text{Emb}^-(O)$ by using the convention that

$\text{Int}_O([\phi_1], [\phi_2])$ is the sum of $[(\phi'_1 \times \phi'_2)_O]$ taken over all equivalence classes $[(\phi'_1, \phi'_2)]$ of intersections.

In Section 8.2, we will define a Hecke operator $T_n : \text{Emb}^+(O) \rightarrow \text{Emb}^+(O)$ for all integers n coprime to \mathfrak{DM} . In Section 8.3 we will define an Atkin-Lehner operator $W_{p^e} : \text{Emb}^+(O) \rightarrow \text{Emb}^+(O)$ for all prime powers $p^e \parallel \mathfrak{DM}$. By combining the different cases in Definition 8.3.3, we produce a Hecke operator T_n for all positive integers n .

Definition 8.0.3. Let f be a function defined on transversal intersections, and ϕ_1, ϕ_2 optimal embeddings of positive discriminants into O . The intersection series associated to ϕ_1, ϕ_2, f is defined to be the formal power series

$$E_{\phi_1, \phi_2}^f(\tau) := \sum_{n=1}^{\infty} \langle \phi_1, T_n \phi_2 \rangle_f q^n,$$

where $\langle \cdot, \cdot \rangle_f$ is the intersection pairing corresponding to f , and $q = e^{2\pi i \tau}$.

The main result of this chapter is the following theorem.

Theorem 8.0.4. *There exists a modular form $E' \in S_2(\Gamma_0(\mathfrak{DM}))^{\mathfrak{D}-new}$ such that the n^{th} coefficient of E' and E_{ϕ_1, ϕ_2}^{\pm} are equal for all n coprime to \mathfrak{M} . In particular, if O is maximal, then $E_{\phi_1, \phi_2}^{\pm} \in S_2(\Gamma_0(\mathfrak{DM}))^{\mathfrak{D}-new}$.*

To prove Theorem 8.0.4, we first pass from optimal embeddings to homology via $\phi \rightarrow \tilde{\ell}_\phi$. The Eichler-Shimura relation allows us to pass to quaternionic modular forms, and we check that our Hecke operators agree with Hecke operators acting on quaternionic modular forms under the associations. The final step is using Jacquet-Langlands to transfer the result to the theory of classical modular forms.

8.1 Naïve Hecke operators

Before defining Hecke operators on optimal embeddings, we must define a similar concept, the naïve Hecke operators.

Definition 8.1.1. For a positive integer n , write

$$\Theta(n) := O_{N=1} \setminus O_{N=n} = \bigcup_{i=1}^M O_{N=1} \pi_i.$$

If $\gcd(\mathfrak{DM}, N) = 1$, the action of the naïve Hecke operator T'_n on $[\phi] \in \text{Emb}^+(O)$ is defined by the formal sum

$$T'_n[\phi] := \sum_{i=1}^M [(\pi_i \phi \pi_i^{-1})_O].$$

Note that the choice of orbit representatives does not affect the definition of T'_n , as they lead to equivalent embeddings. Furthermore, the choice of ϕ representing the class $[\phi]$ does not affect the definition, as it will just permute the terms of the sum. In particular, if $M < \infty$, then T'_n is well-defined. In the rest of this section we will show that M is finite, as well as describing some properties of T'_n .

Lemma 8.1.2. *Let p be a prime number coprime to \mathfrak{DM} , and let k be a positive integer. Then $\Theta(p^k)$ is finite, of size $1 + p + \cdots + p^k$.*

Proof. If $x, y \in O_{N=p^k}$, then $xy^{-1} = \frac{x\bar{y}}{p^k}$. Since p^k is a unit in \mathbb{Z}_q for all primes $q \neq p$, this lies in O_q for all such q . Thus it suffices to work in the completion at p , i.e. considering the space $O_{p,N=1} \setminus O_{p,N=p^k}$. As $p \nmid \mathfrak{DM}$, we can assume that $O_p = \text{Mat}(2, \mathbb{Z}_p)$. As with the classical case of $\text{SL}(2, \mathbb{Z})$, one can check that the matrices

$$\begin{pmatrix} p^a & b \\ 0 & p^{k-a} \end{pmatrix}, \quad a = 0, 1, \dots, k, \text{ and } 0 \leq b < p^{k-a},$$

give a complete set of representatives. The lemma follows. \square

Lemma 8.1.3. *Let m, n, p be positive integers coprime to \mathfrak{DM} , with p being prime. The following statements are true:*

- (i) *The set $\Theta(n)$ is finite of size $\sigma(n)$ = the sum of the divisors of n ;*
- (ii) *T'_m and T'_n commute;*
- (iii) *$T'_{mn} = T'_m T'_n$ when m, n are coprime;*
- (iv) *$T'_{p^k} T'_p = T'_{p^{k+1}} + p T'_{p^{k-1}}$ for all positive integers k .*

Proof. The first point follows from Lemma 8.1.2 and the proof of the third point. The second point will follow from the third and fourth points, so we focus on those. For the third point,

write

$$\Theta(m) = \bigcup_{i=1}^M O_{N=1}\pi_i;$$

$$\Theta(n) = \bigcup_{i=1}^N O_{N=1}\pi'_i.$$

It suffices to show that the set $\{O_{N=1}\pi_i\pi'_j\}_{i=1}^M, j=1}^N$ is a valid and complete set of representatives for $\Theta(mn)$. First, if $x \in O_{N=mn}$, then by Proposition 4.2.6 we can write $x = yz$ with $\text{nrd}(y) = m$, $\text{nrd}(z) = n$, and $y, z \in O$. Then $z = u_1\pi'_j$ for some j and $u_1 \in O_{N=1}$, and we write $x = (yu_1)\pi'_j$. We have $yu_1 = u_2\pi_i$ for some i and $u_2 \in O_{N=1}$, whence $x = u_2\pi_i\pi'_j$. Thus we have a complete set of representatives for $O_{N=1} \setminus O_{N=mn}$.

To show that they are all distinct, assume otherwise, so that $O_{N=1}\pi_i\pi'_j = O_{N=1}\pi_{i'}\pi'_{j'}$. Thus $O_{N=1}\pi_i\pi'_j\pi'^{-1}_{j'} = O_{N=1}\pi_{i'}$. If $j = j'$, then $i = i'$ and we are done. Otherwise, let $x = \pi'_j\pi'^{-1}_{j'}$; we have $\text{nrd}(x) = 1$ and $x \notin O$ since $j \neq j'$. By taking completions, there exists a prime divisor p of n such that $x_p \notin O_p$. Since $\text{nrd}(\pi_i) = m$ is coprime to n , it is coprime to p , and thus $(\pi_i x)_p \notin O_p$, whence $\pi_i x \notin O$. But $\pi_i x \in O_{N=1}\pi_{i'} \subseteq O$, contradiction. Therefore $i = i'$ and $j = j'$, as claimed.

For the last point, in Lemma 8.1.2 we gave explicit local descriptions of representatives of the orbits. The lemma follows by checking it for these orbits, which is the exact same as in the classical case. \square

The operators T'_n are the “obvious” candidate for Hecke operators acting on optimal embeddings, and they indeed satisfy the typical properties of Hecke operators. However, we desire the map $\text{Emb}^+(O) \rightarrow H_1(X_O, \mathbb{Z})$ (the integral homology) induced by $[\phi] \rightarrow \tilde{\ell}_\phi$ to be Hecke-equivariant, and this fails with T'_n . Furthermore, another desirable property would be for the Hecke operators to be self-adjoint with respect to the intersection pairing, and T'_n fails this as well.

8.2 Good Hecke operators

For $[\phi], [\sigma] \in \text{Emb}^+(O)$, write

$$[\phi] \sim_n [\sigma]$$

if there exists a $\pi \in O_{N=n}$ for which $[(\pi\phi\pi^{-1})_O] = [\sigma]$. Note that this is symmetric: let $\pi\phi\pi^{-1} = u\sigma u^{-1}$ for some $u \in O_{N=1}$. Then $\bar{\pi}u \in O_{N=n}$, and $[\bar{\pi}u\sigma(\bar{\pi}u)^{-1}] = [\phi]$.

Definition 8.2.1. Let $[\phi], [\sigma] \in \text{Emb}^+(O)$ and write $\Theta(n) = \cup_{i=1}^M O_{N=1}\pi_i$ for n coprime to \mathfrak{DM} . The n^{th} weight associated to the ordered pair $([\phi], [\sigma])$ is

$$w_n(\phi, \sigma) := |\{i : 1 \leq i \leq M, [(\pi_i\phi\pi_i^{-1})_O] = [\sigma]\}|.$$

We drop the equivalence class brackets from the inputs for ease of reading.

In particular, the naïve Hecke operator can be expressed as

$$T'_n[\phi] = \sum_{[\sigma] \sim_n [\phi]} w_n(\phi, \sigma)[\sigma].$$

The correct definition of T_n just switches the terms in w_n !

Definition 8.2.2. Let n be coprime to \mathfrak{DM} . The action of the (good) Hecke operator T_n on $[\phi]$ is defined by the formal sum

$$T_n[\phi] := \sum_{[\sigma] \sim_n [\phi]} w_n(\sigma, \phi)[\sigma].$$

Note that the sum subscript is unnecessary, as if $[\sigma] \not\sim_n [\phi]$, then $w_n(\sigma, \phi) = 0$.

Lemma 8.2.3. *Let m, n, p be positive integers coprime to \mathfrak{DM} , with p a prime. The following statements are true:*

- (i) T_m and T_n commute;
- (ii) $T_{mn} = T_m T_n$ if m, n are coprime;
- (iii) $T_{p^k} T_p = T_{p^{k+1}} + p T_{p^{k-1}}$ for all positive integers k .

Proof. As with Lemma 8.1.3, it suffices to prove the second and third points only. Since $T'_{mn} = T'_n T'_m$ for m, n coprime, we have

$$\sum_{[\sigma]} w_{mn}(\phi, \sigma)[\sigma] = T'_n \left(\sum_{[\theta]} w_m(\phi, \theta)[\theta] \right) = \sum_{[\theta]} \sum_{[\sigma]} w_m(\phi, \theta) w_n(\theta, \sigma)[\sigma].$$

By equating the coefficients of $[\sigma]$, we have

$$w_{mn}(\phi, \sigma) = \sum_{[\theta]} w_m(\phi, \theta) w_n(\theta, \sigma).$$

Swapping ϕ, σ gives us

$$w_{mn}(\sigma, \phi) = \sum_{[\theta]} w_m(\sigma, \theta) w_n(\theta, \phi).$$

Expanding out $T_{mn}[\phi]$ and $T_m T_n[\phi]$ in similar fashion to the naïve Hecke operators and using this equality proves that $T_{mn} = T_m T_n$ for coprime m, n .

For the third point, we know that $T'_p T'_{p^k} = T'_{p^k} T'_p = T'_{p^{k+1}} + p T'_{p^{k-1}}$. Expanding this out as above and equating coefficients gives for all $[\sigma]$ that

$$\sum_{[\theta]} w_{p^k}(\phi, \theta) w_p(\theta, \sigma) = w_{p^{k+1}}(\phi, \sigma) + p w_{p^{k-1}}(\phi, \sigma).$$

Swapping ϕ, σ thus gives

$$\sum_{[\theta]} w_{p^k}(\sigma, \theta) w_p(\theta, \phi) = w_{p^{k+1}}(\sigma, \phi) + p w_{p^{k-1}}(\sigma, \phi).$$

By expanding out $T_{p^k} T_p[\phi]$ and $(T_{p^{k+1}} + p T_{p^{k-1}})[\phi]$ and using this equality, we see that all coefficients are equal, hence the third point is proved. \square

See Proposition 8.6.3 for an alternate expression for the good Hecke operators.

8.3 Atkin-Lehner and general Hecke operators

We have defined the Hecke operators T_n for n coprime to \mathfrak{DM} . Working with n not coprime to \mathfrak{DM} is slightly different, and for such n we need the Atkin-Lehner operators W_{p^e} .

Definition 8.3.1. Let p be a prime and e a positive integer such that $p^e \parallel \mathfrak{DM}$. Define ω_{p^e} to be the ω_p as found in Proposition 4.2.8 (i.e. $\omega_{p^e} \in N_{B^\times}(O)$ and $\text{nrd}(\omega_{p^e}) = p^e$). Then the action of the Atkin-Lehner operator W_{p^e} on $[\phi] \in \text{Emb}^+(O)$ is defined by

$$W_{p^e}[\phi] = [\omega_{p^e} \phi \omega_{p^e}^{-1}].$$

If $\phi' \in [\phi]$ and ω'_{p^e} was a different choice, then write $\phi' = u_1 \phi u_1^{-1}$ and $\omega'_{p^e} = \omega_{p^e} u_2$ for some $u_1, u_2 \in O_{N=1}$. As $\omega_{p^e} \in N_{B^\times}(O)$, there exists $u \in O_{N=1}$ for which $u \omega_{p^e} = \omega_{p^e} u_2 u_1$. In particular,

$$[\omega'_{p^e} \phi' \omega_{p^e}^{-1}] = [\omega_{p^e} u_2 u_1 \phi (\omega_{p^e} u_2 u_1)^{-1}] = [u (\omega_{p^e} \phi \omega_{p^e}^{-1}) u^{-1}] = [\omega_{p^e} \phi \omega_{p^e}^{-1}],$$

so the action of W_{p^e} is well-defined. More generally, the same argument also shows that

$$[\phi] = [\sigma] \Rightarrow [\omega_{p^e} \phi \omega_{p^e}^{-1}] = [\omega_{p^e} \sigma \omega_{p^e}^{-1}].$$

Furthermore, since $\omega_{p^e}^2 \in \mathbb{Q}^\times O_{N=1}^\times$, it follows that $W_{p^e}^2$ acts as the identity.

Lemma 8.3.2. *Let n be coprime to \mathfrak{DM} , and let $p^e, q^f \parallel \mathfrak{DM}$. Then*

(i) T_n and W_{p^e} commute;

(ii) W_{p^e} and W_{q^f} commute.

Proof. The key to both parts of the proof is the fact that $\omega_{p^e} \in N_{B^\times}(O)$. For part i, by expanding out $T_n W_{p^e}[\phi]$ and $W_{p^e} T_n[\phi]$, it suffices to prove that

$$\sum_{[\sigma]} w_n(\sigma, \phi^{\omega_{p^e}})[\sigma] = \sum_{[\sigma]} w_n(\sigma, \phi)[\sigma^{\omega_{p^e}}].$$

We can replace σ by $\sigma^{\omega_{p^e}}$ in the first sum, and it is thus equivalent to showing that

$$w_n(\sigma^{\omega_{p^e}}, \phi^{\omega_{p^e}}) = w_n(\sigma, \phi).$$

Writing $\Theta(n) = \sum_{i=1}^M O_{N=1} \pi_i$, the first expression counts the i 's for which

$$[(\pi_i \omega_{p^e} \sigma \omega_{p^e}^{-1} \pi_i^{-1})_O] = [\omega_{p^e} \sigma \omega_{p^e}^{-1}].$$

By conjugating each term by $\omega_{p^e}^{-1}$, this counts the i 's for which

$$[(\omega_{p^e}^{-1} \pi_i \omega_{p^e} \sigma (\omega_{p^e}^{-1} \pi_i \omega_{p^e})^{-1})_O] = [\sigma].$$

As $\omega_{p^e} \in N_{B^\times}(O)$, it follows that $\{\omega_{p^e}^{-1} \pi_i \omega_{p^e}\}$ is also a set of representatives of $\Theta(n)$, which implies the equality.

The second part follows from a similar (but easier) computation. □

We are now ready for the full definition of a Hecke operator acting on $\text{Emb}^+(O)$.

Definition 8.3.3. For a prime power p^e , define the Hecke operator T_{p^e} to be

- T_{p^e} as defined in Section 8.2 if p is coprime to \mathfrak{DM} ;
- W_p^e if $p \mid \mathfrak{D}$;
- 0 if $p \mid \mathfrak{M}$.

For a positive integer $n = \prod_{i=1}^M p_i^{e_i}$, define

$$T_n := \prod_{i=1}^M T_{p_i^{e_i}}.$$

It follows from Lemmas 8.2.3 and 8.3.2 that T_n is well defined (as all of the good Hecke operators and the Atkin-Lehner operators commute), and that T_n agrees with the previous definition of T_n when n is coprime to \mathfrak{DM} .

Remark 8.3.4. We can define an infinite Hecke operator analogously to the Atkin-Lehner involutions. Take $\mu \in O_{N=-1} \subseteq N_{B^\times}(O)$, and then

$$T_\infty[\phi] := [\mu\phi\mu^{-1}].$$

As before, this is well-defined, commutes with all previously defined Hecke operators, and squares to the identity operator.

8.4 Discriminants of conjugated embeddings

Let p be a prime with $p \nmid \mathfrak{DM}$, and write $O_{N=1} \setminus O_{N=p} = \bigcup_{i=1}^{p+1} O_{N=1}\pi_i$. We wish to describe the embeddings in the sum $T_p[\phi]$, namely: what are the discriminants of the corresponding embeddings, and what are the multiplicities of each distinct embedding? This essentially boils down to questions about fundamental units in towers of orders in the number field $\mathbb{Q}(\sqrt{D})$. In this section we will determine the structure of $T'_p[\phi]$, from which one can get the structure of $T_p[\phi]$ (the only change is the weighting of coefficients).

Definition 8.4.1. Let D be a positive discriminant and p a prime, and consider the fundamental units of positive norm $\epsilon_D, \epsilon_{p^2D}, \epsilon_{p^4D}, \dots$. Define $e_k^p(D) = e_k$ for $k \geq 1$ to be the positive integer such that

$$\epsilon_{p^{2k}D} = \epsilon_{p^{2k-2}D}^{e_k}.$$

Write $\epsilon_D = \frac{T+U\sqrt{D}}{2}$, and for $i \geq 1$ write $\epsilon_D^i = \frac{T_i+U_i\sqrt{D}}{2}$. Then e_1 is the minimal i for which $p \mid U_i$, and inductively, e_k is the minimal i for which $p^k \mid U_{e_1 e_2 \dots e_{k-1} i}$.

Proposition 8.4.2. *Let $v_p(U_{e_1}) = m$. Then*

- $e_1 \mid p - \left(\frac{D}{p}\right)$;
- $e_2 = \dots = e_m = 1$ if $m > 1$;
- $e_i = p$ for all $i \geq m + 1$.

Proof. For this whole proof, assume that p is odd; $p = 2$ can be found in Proposition A.2.3. The claim that $e_2 = \dots = e_m = 1$ if $m > 1$ is obvious, so we focus on the other two claims.

Observe that

$$U_i \sqrt{D} = \epsilon_D^i - \epsilon_D^{-i}.$$

Let \mathfrak{p} be a prime ideal of \mathcal{O}_D above p , and let k be the positive integer such that $v_{\mathfrak{p}}(D) = k - 1$. Let e be the reduction of ϵ_D modulo \mathfrak{p}^k . Since ϵ_D is a unit, $e \in \left(\frac{\mathcal{O}_D}{\mathfrak{p}^k}\right)^\times$. Then $p \mid U_i$ is equivalent to $e^i - e^{-i} = 0$, which is equivalent to $e^{2i} = 1$. Therefore all such i 's are a multiple of the minimal i , which is e_1 .

If p is split in \mathcal{O}_D , then $k = 1$ and we are working in \mathbb{F}_p . Since \mathbb{F}_p^\times is cyclic of order $p - 1$, this implies that $e_1 \mid \frac{p-1}{2} \mid p - 1$, as claimed.

If p is inert in \mathcal{O}_D , then $k = 1$ and we are working in \mathbb{F}_{p^2} . Since $\epsilon_D^i - \epsilon_D^{-i} \in \mathbb{Z}\sqrt{D}$, we have $e^i - e^{-i} = 0$ if and only if $e^i - e^{-i} \in \mathbb{F}_p$. The group $\mathbb{F}_{p^2}^\times$ is cyclic of order $p^2 - 1$, and the subgroup \mathbb{F}_p^\times is cyclic of order $p - 1$, hence the quotient group is cyclic of order $p + 1$. Thus $e^{p+1} \in \mathbb{F}_p$, and so $e^{p+1} - e^{-(p+1)} \in \mathbb{F}_p$, whence $e_1 \mid p + 1$, as claimed.

Finally, assume that $p \mid D$. Then $k \geq 2$, and $\frac{U\sqrt{D}}{2} \in \mathfrak{p}^{k-1}$. Raise this to the p^{th} power, since $p \mid \binom{p}{i}$ for $1 \leq i \leq p - 1$ and $p(k - 1) \geq k$ for $k \geq 2$, we see that

$$\epsilon_D^p \equiv (T/2)^p \pmod{\mathfrak{p}^k}.$$

The same holds true for ϵ_D^{-p} , whence $e^p - e^{-p} = 0$, and so $e_1 \mid p$, as claimed.

For the last point, by replacing D with $p^{2m}D$, we can assume that $p \nmid U$ and $p^2 \mid D$, hence $k \geq 3$. Since $e_1 \neq 1$ and $e_1 \mid p$, we must have $e_1 = p$. To complete the claim, we must show that $p \parallel U_p$, as we can then induct. Since $p \nmid U$, we have $\frac{U\sqrt{D}}{2} \in \mathfrak{p}^{k-1} - \mathfrak{p}^k$. Working as before, note that $T/2 \notin \mathfrak{p}$ (otherwise ϵ_D could not be a unit), and taking the p^{th} power of ϵ_D and working modulo \mathfrak{p}^{k+2} gives

$$\epsilon_D^p \equiv (T/2)^p + (T/2)^{p-1}p(U\sqrt{D}/2) \pmod{\mathfrak{p}^{k+2}}.$$

All the other terms of the binomial expansion disappeared, since their \mathfrak{p} -valuation was either at least $2 + 2(k-1) = 2k \geq k+2$ (the next $p-2$ terms), or at least $p(k-1) \geq 3k-3 \geq k+2$ since $k \geq 3$ (the last term). The similar expression for ϵ_D^{-p} holds, and we see that

$$\epsilon_D^p - \epsilon_D^{-p} \equiv pU\sqrt{D}(T/2)^{p-1} \pmod{\mathfrak{p}^{k+2}},$$

which implies that $U_p\sqrt{D} = \epsilon_D^p - \epsilon_D^{-p} \in \mathfrak{p}^{k+1} - \mathfrak{p}^{k+2}$, and thus $p \parallel U_p$, as desired. \square

The term e_1 is closely related to $\frac{h^+(p^2D)}{h^+(D)}$. Specifically, Theorems 7.4, 7.5 of [Bue89] combine into the following proposition.

Proposition 8.4.3. *We have*

$$\frac{h^+(p^2D)}{h^+(D)} = \frac{p - \left(\frac{D}{p}\right)}{e_1^p(D)}.$$

Definition 8.4.4. If D is a discriminant and p is a prime such that $\frac{D}{p^2}$ is not a discriminant, we say D is p -fundamental.

We can now describe the terms of $T'_p\phi$.

Proposition 8.4.5. *Let $D = p^{2k}D'$, where D' is a p -fundamental discriminant, and $p \nmid \mathfrak{DM}$. Consider the multiset $\{[(\pi_i\phi\pi_i^{-1})_O] : 1 \leq i \leq p+1\}$. This contains*

- $p+1$ optimal embeddings of discriminant p^2D if $k=0$ and $\left(\frac{D}{p}\right) = -1$.
- p optimal embeddings of discriminant p^2D and one of discriminant D if $k=0$ and $\left(\frac{D}{p}\right) = 0$.

- $p - 1$ optimal embeddings of discriminant p^2D and two of discriminant D if $k = 0$ and $\left(\frac{D}{p}\right) = 1$.
- p optimal embeddings of discriminant p^2D and one of discriminant $\frac{D}{p^2}$ if $k > 0$.

The optimal embeddings of discriminant p^2D divide into

$$\frac{p - \left(\frac{D}{p}\right)}{e_1^p(D)} = \frac{p - \left(\frac{D}{p}\right)}{e_{k+1}^p(D)}$$

distinct equivalence classes, each with multiplicity $e_1^p(D) = e_{k+1}^p(D)$.

Proof. Assume that p is odd; the intrepid reader can find the proof of $p = 2$ in the appendix, Proposition A.2.4. To calculate the discriminants, it suffices to do the calculations after completing at p . Thus we can assume that $O_p = \text{Mat}(2, \mathbb{Z}_p)$, and $\phi_p(\sqrt{D}) = \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}$. From Lemma 8.1.2, we can take representatives

$$\pi_i = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} : i = 0, 1, \dots, p-1, \quad \pi_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

We compute

$$\pi_\infty \phi(\sqrt{D}) \pi_\infty^{-1} = \begin{pmatrix} 0 & pD \\ \frac{1}{p} & 0 \end{pmatrix}.$$

This gives us an optimal embedding of p^2D in all cases. For $i < \infty$,

$$\pi_i \phi(\sqrt{D}) \pi_i^{-1} = \begin{pmatrix} i & \frac{D-i^2}{p} \\ p & -i \end{pmatrix}.$$

If p is inert with respect to D , then $\frac{D-i^2}{p}$ never lies in \mathbb{Z}_p , whence we get everything of discriminant p^2D . If $p \mid D$, then this gives discriminant p^2D for all $i \neq 0$. When $i = 0$, we get D or $\frac{D}{p^2}$, depending on if $p^2 \mid D$ or not. Finally, if p is split with respect to D , then precisely two values of i allow this to lie in $\text{Mat}(2, \mathbb{Z}_p)$, and we get 2 embeddings of discriminant D and $p - 2$ of p^2D . Therefore the discriminants occur as we claim.

Next, we check when we get similar embeddings of discriminant p^2D . Let $v = \phi(\epsilon_D) \in O_{N=1}$, fix i , and let $\pi_i v = u \pi_j$ for some j and $u \in O_{N=1}$. Then

$$(\pi_j \phi \pi_j^{-1})_O \sim (u \pi_j \phi \pi_j^{-1} u^{-1})_O = (\pi_i v \phi v^{-1} \pi_i^{-1})_O = (\pi_i \phi \pi_i^{-1})_O,$$

i.e. the resulting forms lie in the same equivalence class. We wish to show that in the discriminant p^2D case this is also essentially necessary, i.e. if $(\pi_i\phi\pi_i^{-1})_O \sim (\pi_j\phi\pi_j^{-1})_O$ are embeddings of discriminant p^2D , then $\pi_iv^k = u\pi_j$ for some integer k and $u \in O_{N=1}$.

To prove this, we have $[(\pi_i\phi\pi_i^{-1})_O] = [(\pi_j\phi\pi_j^{-1})_O]$ if and only if there is a $u \in O_{N=1}$ for which $\pi_i\phi\pi_i^{-1} = u^{-1}\pi_j\phi\pi_j^{-1}u$. Rearranging, this is equivalent to $\pi_j^{-1}u\pi_i\phi(\sqrt{D})(\pi_j^{-1}u\pi_i)^{-1} = \phi(\sqrt{D})$, hence $\pi_j^{-1}u\pi_i = \phi(x + y\sqrt{D})$ for rationals x, y (from Proposition 4.2.1). Again rearranging, this is equivalent to $\pi_j\phi(x + y\sqrt{D})\pi_i^{-1} \in O_{N=1}$. Taking norms, we see that $x^2 - Dy^2 = 1$, whence we are done if we can show that $z = x + y\sqrt{D} \in \mathcal{O}_D$. Since $\phi(pz) = \overline{\pi_j}u\pi_i \in O$, we have $z \in \frac{1}{p}\mathcal{O}_D$, and so it suffices to look at the completion at p .

In this completion, we can take the explicit forms of π_i and ϕ as above. Thus $\phi(x+y\sqrt{D}) = \begin{pmatrix} x & yD \\ y & x \end{pmatrix}$. If $i, j < \infty$, then we have

$$\pi_j\phi(x + y\sqrt{D})\pi_i^{-1} = \begin{pmatrix} x + jy & \frac{(j-i)x + (D-ij)y}{p} \\ py & x - iy \end{pmatrix} \in \text{Mat}(2, \mathbb{Z}_p).$$

From above, $px, py \in \mathbb{Z}_p$, so write $X = px, Y = py$. Then we necessarily have $p \mid X + jY$, and $p^2 \mid (j-i)X + (D-ij)Y$. Looking at the second equation modulo p , we derive

$$0 \equiv (j-i)(-jY) + (D-ij)Y \equiv (D-j^2)Y \pmod{p}.$$

Since we have embeddings of discriminant p^2D , $D - j^2 \not\equiv 0 \pmod{p}$, whence $p \mid Y$, and so $p \mid X$, as desired.

If $i = \infty$, then $j < \infty$, and we have

$$\pi_j\phi(x + y\sqrt{D})\pi_\infty^{-1} = \begin{pmatrix} \frac{x+jy}{p} & yD + jx \\ y & px \end{pmatrix} \in \text{Mat}(2, \mathbb{Z}_p).$$

It immediately follows that $y \in \mathbb{Z}_p$, and then $x \in \mathbb{Z}_p$ too, as desired.

Now, we see that we form equivalence classes by right multiplication by $v = \phi(\epsilon_D)$. Thus the size of an orbit corresponds to the minimal k such that $\pi_iv^k = u\pi_i$, for some $u \in O_{N=1}$. Writing $v^k = \phi(X + Y\sqrt{D})$, in the above calculations we can take $i = j$ (as well as repeating for $i = j = \infty$) and it follows that $\pi_iv^k = u\pi_i$ if and only if $p \mid Y$. The smallest k which produces a corresponding Y with $p \mid Y$ is the k such that $\epsilon_D^k = \epsilon_{p^2D}$. By Proposition 8.4.3, the division into orbits follows. \square

With notation as above, note that $\pi_\infty\pi_i$ and $\pi_0\pi_\infty$ lie in $p\mathcal{O}_{N=1}$. Therefore if we can go from $[\phi]$ to $[\sigma]$ with an element of $\Theta(p)$, then we can go back from $[\sigma]$ to $[\phi]$.

Let's study the discriminant D optimal embedding classes formed a bit further. Let D be p -fundamental, and depending on if D is split/ramified/inert, there are 2/1/0 optimal embedding classes of discriminant D that are a conjugation in $\Theta(p)$ away from $[\phi]$. By repeating, we see that they form a cycle, say $\{[\phi_1], [\phi_2], \dots, [\phi_n]\}$, for which $\phi_1 = \phi$ and $[\phi_i], [\phi_{i+1}]$ (indices modulo n) are related by conjugation by an element of $\Theta(p)$ for all i (if D is ramified we necessarily have $n = 1, 2$ only, and if D is inert then $n = 1$).

Proposition 8.4.6. *Let \mathfrak{p} be a prime ideal of \mathcal{O}_D above p . Then n is the order of \mathfrak{p} in $\text{Cl}^+(D)$.*

Proof. If p is inert, then $n = 1$ and $\mathfrak{p} = \langle p \rangle$ is principal.

Otherwise, for all i there will exist an element of norm p taking $[\phi_i]$ to $[\phi_{i+1}]$. Therefore by Theorem 4.5.4, $Q_{\phi_i, \phi_{i+1}}$ is a primitive quadratic form of discriminant D that represents p . Since p is a prime, there are precisely two such forms, they are inverses to each other, and correspond to $\mathfrak{p}, \mathfrak{p}^{-1}$ under the correspondence between primitive indefinite binary quadratic forms and proper fractional ideals of \mathcal{O}_D . In particular, without loss of generality, assume that passing from $[\phi_1]$ to $[\phi_2]$ corresponds to \mathfrak{p} , and then the same is true when passing from $[\phi_i]$ to $[\phi_{i+1}]$ for all i ! We return back to $[\phi_1]$ after doing \mathfrak{p}^n (by Theorem 4.5.4 again), but this must correspond to the identity quadratic form, i.e. this is equivalent to it being principal. Therefore the cycle formed has length being the order of \mathfrak{p} in $\text{Cl}^+(D)$. \square

8.5 Prime power Hecke graph

Proposition 8.4.5 allows one to determine the behaviour of T_p on $[\phi]$. However, it is desirable to visualize the entire action of T_{p^n} on $[\phi]$, and this is accomplished with the prime power Hecke graph.

Let $p \nmid \mathfrak{D}\mathfrak{M}$, let ϕ be an optimal embedding of the positive discriminant D into \mathcal{O} , and assume that D is p -fundamental. Then the prime power Hecke graph is denoted $G_O^p(\phi) = G$: it is a connected graph, all non-loop edges are undirected, there is at most one loop

(which may be either directed or undirected), and there is at most one set of double edges. Concretely, we define:

- The vertices of G are the equivalence classes of embeddings $[(\pi\phi\pi^{-1})_O]$ for all $\pi \in O$ with $\text{nrd}(\pi)$ being a power of p .
- The “level” of a vertex $[\sigma]$ is k , where σ is an optimal embedding of discriminant $p^{2k}D$.
- If $[\sigma]$ is a vertex, draw a single undirected edge between $[\sigma]$ and $[(\pi\sigma\pi^{-1})_O]$ for all $\pi \in O_{N=p}$.
- If p is ramified with respect to D and there is exactly one vertex of level 0, orient the loop at $[\phi]$.
- If p is split with respect to D and there are exactly two vertices of level 0, draw a second edge between them.

The remarks following Proposition 8.4.5 say that we can go backwards, which justifies having the edges undirected. This only fails if we have a loop, and the “going backwards” element was the same as the “going forwards” element. In particular, this is precisely when p is ramified with respect to D and there is exactly one vertex of level 0, which explains the second last point. Furthermore, when p is split with respect to D and there are exactly two vertices of level 0, then having only one edge between the vertices would be incorrect as there are two distinct ways to pass between the two vertices.

While the structure of G follows from the definition and Propositions 8.4.5, 8.4.6, we record it explicitly for clarity.

Theorem 8.5.1. *Let \mathfrak{p} be a prime ideal of \mathcal{O}_D above p . Then the shape of $G_{\mathcal{O}}^{\mathfrak{p}}(\phi)$ is as follows:*

- *If p is inert with respect to D , there is a single level 0 vertex and no loops.*
- *If p is ramified with respect to D , there are one or two vertices of level 0. If \mathfrak{p} is principal, there is a single vertex and a directed loop at it. Otherwise, there are two vertices, and they are connected by a single edge.*

- If p is split with respect to D , the level 0 vertices form a cycle whose length is the order of \mathfrak{p} in $\text{Cl}^+(D)$. If there is one such vertex this is an undirected loop, and if there are two such vertices there is a double edge.
- For each vertex in level 0, there are $\frac{p - (\frac{D}{p})}{e_1^p(D)}$ edges going to level one, and the target vertices are all distinct (as we run over all level 0 vertices).
- From level $k = 1$ to level $k = v_p(U_{e_1}) - 1$ (only if this is at least 1), each vertex splits into p vertices in the next level, again all distinct.
- In levels $v_p(U_{e_1})$ and beyond, each vertex is connected to exactly one vertex in the next level.

When drawing G , one should group all vertices of a fixed level in a column, starting at level 0 and going up by one at each step.

We now present some examples of prime power Hecke graphs. In each example, we note $\mathfrak{D}, \mathfrak{M}, D, p$, draw the graph, and label the levels k and the exponents $e_k^p(D)$. Note that $\mathfrak{D}, \mathfrak{M}$ have essentially no role in these graphs: all that is required is for $p \nmid \mathfrak{D}\mathfrak{M}$, and there needs to exist optimal embeddings into the Eichler level of order \mathfrak{M} in the Eichler level of discriminant \mathfrak{D} . In particular, given a fixed D, p , the graphs will look the same for all choices of $\mathfrak{D}, \mathfrak{M}$ for which the graphs exist.

First, Figure 8.1 is an example where D is inert with respect to p , where the graph is always a tree.

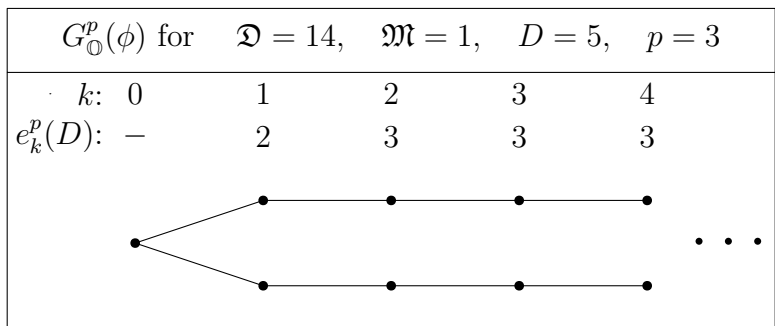


Figure 8.1: p inert.

Proceeding onward, we have two examples when $p \mid D$, demonstrating the two possible level 0 behaviours. Figure 8.2 gives a case where there is only one level 0 vertex.

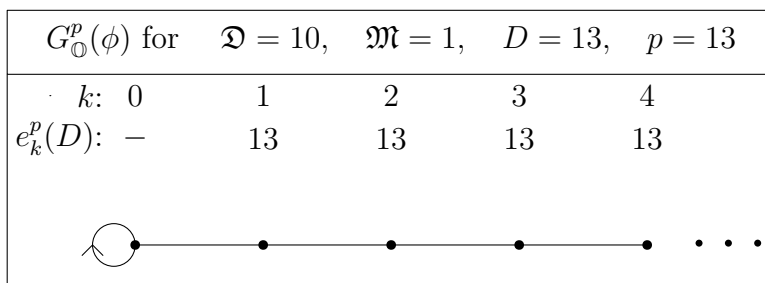


Figure 8.2: p ramified, one level 0 vertex.

In Figure 8.3, there are two level 0 vertices, as well as demonstrating an example with $e_1 = e_2 = 1$.

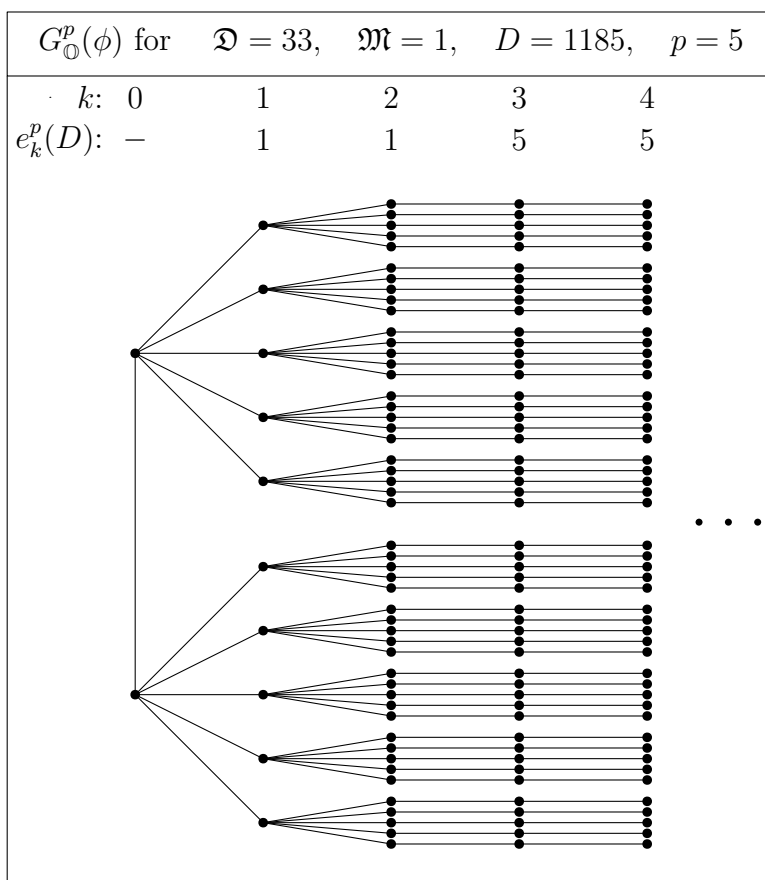


Figure 8.3: p ramified, two level 0 vertices.

When D is split with respect to p , there are three main behaviours. Figure 8.4 demon-

strates a loop at the start, as well as $e_1 = e_2 = e_3 = e_4 = 1$.

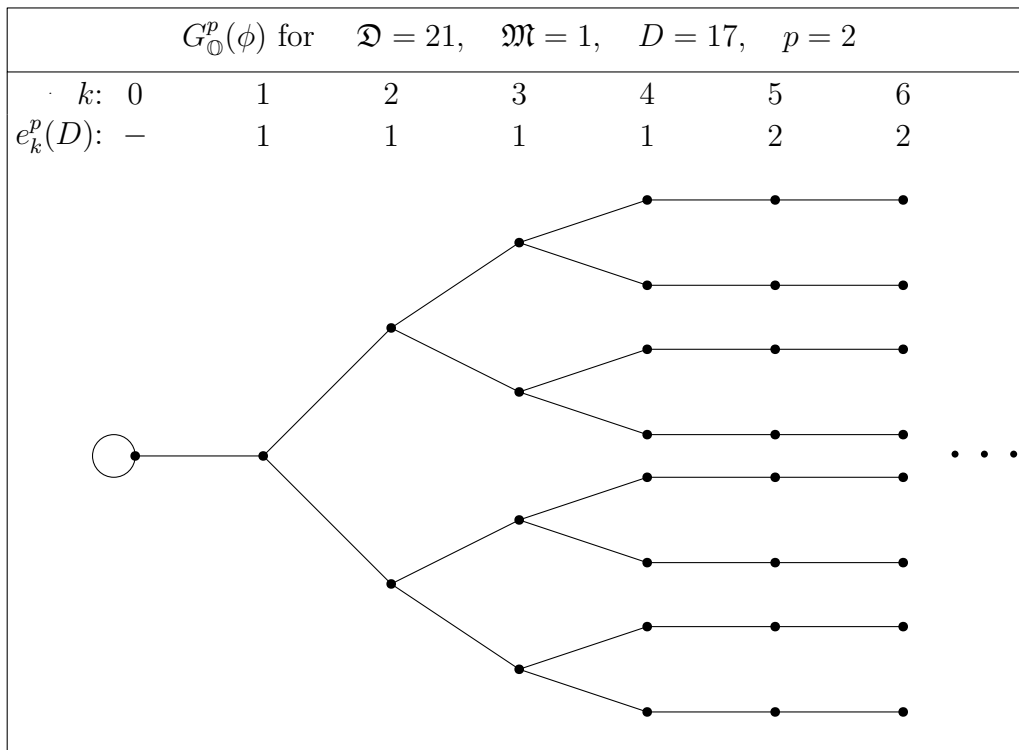


Figure 8.4: p split, loop.

Next, Figure 8.5 has a double edge.

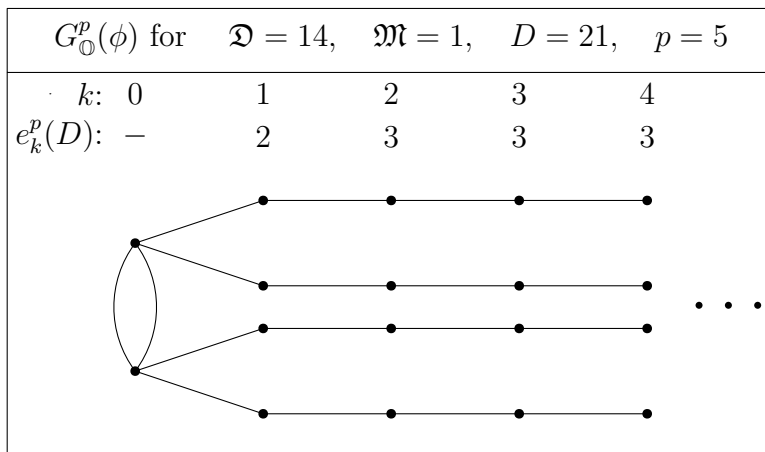


Figure 8.5: p split, double edge.

Finally, when \mathfrak{p} has order at least three, the graph no longer has loops/double edges. Figure 8.6 gives such an example with three level 0 vertices.

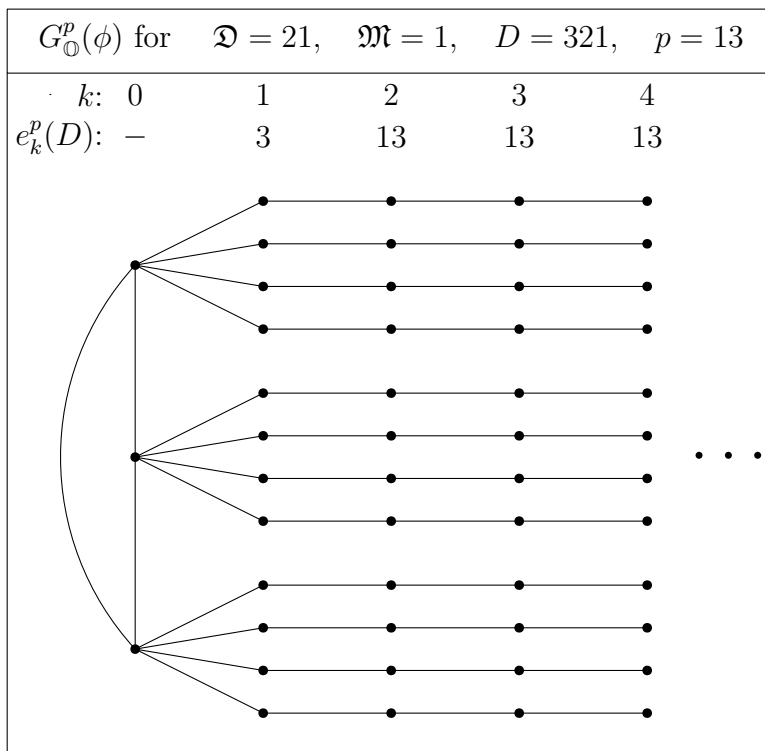


Figure 8.6: p split, three level 0 vertices.

With these examples in hand, we record down how to determine $T_p[\phi]$ from $G_{\mathbb{O}}^p(\phi)$.

Proposition 8.5.2. *Let $[\phi']$ have level k on $G = G_{\mathbb{O}}^p(\phi)$. Then $T_p[\phi']$ is a sum involving only the terms $[\sigma]$ with $[\sigma]$ adjacent to $[\phi']$ in G . The coefficient of such a $[\sigma]$ of level k' (necessarily $k - 1, k,$ or $k + 1$) is*

- The number of length 1 paths from $[\sigma]$ to $[\phi']$ if $k' \geq k$;
- $e_k^p(D)$ if $k' = k - 1$.

In particular, if $k' = k + 1$ there is exactly one such path of length 1. If $k = k'$, then $k = k' = 0$ necessarily, and there will again be only one, except for when p is inert with respect to D and there are at most two level 0 vertices. In this case, the coefficient is 2.

8.6 Properties of Hecke operators

Before diving into two key propositions about Hecke operators, we record that when determining if root geodesics of optimal embeddings intersect, we can ignore the order \mathcal{O} .

Lemma 8.6.1. *Let ϕ_1, ϕ_2 be embeddings into B of discriminants D_1, D_2 , let $b \in B^\times$, let O be any order of B , and let $x = \frac{1}{2} \operatorname{trd}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}))$. Then the root geodesics of $(\phi_1^b)_O$ and $(\phi_2^b)_O$ intersect if and only if*

$$x^2 < D_1 D_2.$$

In particular, when checking for intersection of root geodesics, we can simultaneously conjugate by B^\times at will and ignore the order we are embedding into.

Proof. Let $(\phi_i^b)_O$ have discriminant $k_i^2 D_i$ for $i = 1, 2$ and a positive rational number k_i . Then

$$\frac{1}{2} \operatorname{trd} \left(\phi_1^b \left(\sqrt{k_1^2 D_1} \right) \phi_2^b \left(\sqrt{k_2^2 D_2} \right) \right) = k_1 k_2 x,$$

so Theorem 5.1.4 implies that the root geodesics intersect if and only if

$$(k_1 k_2 x)^2 < k_1^2 D_1 k_2^2 D_2,$$

which is equivalent to $x^2 < D_1 D_2$. □

While the naïve Hecke operators T'_n are not self-adjoint with respect to the intersection pairing, the Hecke operators T_n are.

Proposition 8.6.2. *Let n be any positive integer, and let f represent either the unweighted, signed, or q -weighted intersection for $q \mid \mathfrak{DM}$. Then the f -weighted intersection pairing is Hecke equivariant, i.e.*

$$\operatorname{Int}_O^f(T_n[\phi_1], [\phi_2]) = \operatorname{Int}_O^f([\phi_1], T_n[\phi_2]).$$

Proof. It suffices to prove this proposition for T_p with p coprime to \mathfrak{DM} , as well as W_{p^e} for $p^e \parallel \mathfrak{DM}$. First, consider the case of T_p . Write $\Theta(p) = \cup_{i=1}^{p+1} O_{N=1} \pi_i$, and define the set

$$S_1 = \{(\pi_i, u, \phi) : |\ell_\phi \cap \ell_{\phi_2}| = 1, \phi^{\pi_i} = \phi_1^u, u \in O_{N=1}\}.$$

We claim that every element in the sum $\operatorname{Int}_O^f(T_p([\phi_1]), [\phi_2])$ corresponds to an element of S_1 .

Write

$$T_p[\phi_1] = \sum_{[\sigma] \sim_p [\phi_1]} w_p(\sigma, \phi_1)[\sigma],$$

and then an intersection of this with ϕ_2 corresponds to the equivalence class of the pair (σ^v, ϕ_2) with $v \in O_{N=1}$ and $|\ell_{\sigma^v} \cap \ell_{\phi_2}| = 1$. Since $w_p(\sigma, \phi_1) = w_p(\sigma^v, \phi_1)$ for all $v \in O_{N=1}$, we

can associate an element of S_1 via (π_i, u, σ^v) for all i for which $\sigma^{\pi_i v} = \phi_1^u$. Write $r_i = \phi_i(\epsilon_{D_i})$ for $i = 1, 2$, and then the pair (σ^v, ϕ_2) is well defined up to conjugation by powers of r_2 . Furthermore, u is defined up to multiplication on the right by powers of r_1 . In particular, let $k_1, k_2 \in \mathbb{Z}$, write

$$\pi_i r_2^{-k_2} = \delta_i \pi_{i^*},$$

for a unique π_{i^*} and $\delta_i \in O_{N=1}$, and define an equivalence relation on S_1 via

$$(\pi_i, u, \phi) \sim_{S_1} (\pi_{i^*}, \delta_i^{-1} u r_1^{k_1}, \phi^{r_2^{k_2}}).$$

This relation corresponds exactly to the ambiguity described above in associating an element of S_1 to $\text{Int}_O^f(T_p([\phi_1]), [\phi_2])$. Therefore

$$\text{Intersections of } T_p[\phi_1] \text{ with } [\phi_2] \Leftrightarrow S_1 / \sim.$$

Define S_2 and the equivalence relation \sim_{S_2} in the analogous fashion, i.e. with all indices 1, 2 swapped. In the exact same manner, we have that intersections of $[\phi_1]$ with $T_p[\phi_2]$ biject naturally with S_2 / \sim .

Let $(\pi_i, u, \phi) \in S_1$, and let j, v be uniquely defined so that

$$p \pi_i^{-1} u = v^{-1} \pi_j,$$

where $v \in O_{N=1}$. We define the map $\theta : S_1 \rightarrow S_2$ via

$$\theta((\pi_i, u, \phi)) = \left(\pi_j, v, \phi_2^{\pi_j^{-1} v} \right).$$

First, we check that the image lands in S_2 . Using Lemma 8.6.1 and the shorthand notation (σ_1, σ_2) for “the root geodesics of $(\sigma_1)_O, (\sigma_2)_O$ intersect,” we have

$$(\phi, \phi_2) \Rightarrow \left(\phi^{u^{-1} \pi_i}, \phi_2^{u^{-1} \pi_i} \right) \Rightarrow \left(\phi_1, \phi_2^{\pi_j^{-1} v} \right).$$

Since $(\phi_2^{\pi_j^{-1} v})^{\pi_j} = \phi_2^v$, the image lands in S_2 . Let $\theta' : S_2 \rightarrow S_1$ be the analogously defined map going the other way (swap 1’s and 2’s), and it is straightforward to check that θ, θ' are inverses to each other, whence S_1 bijects with S_2 . To complete the proposition for the unweighted intersection number, it suffices to check that θ descends to a map from S_1 / \sim_{S_1} to S_2 / \sim_{S_2} (the map θ' will do the same in analogous fashion).

Take the equations

$$\begin{aligned} \pi_i r_2^{-k_2} &= \delta_i \pi_{i^*}, & p \pi_i^{-1} u &= v^{-1} \pi_j, & p \pi_{i^*}^{-1} \delta_i^{-1} u r_1^{k_1} &= v'^{-1} \pi_{j'}; \\ \theta((\pi_i, u, \phi)) &= \left(\pi_j, v, \phi_2^{\pi_j^{-1} v} \right), & \theta((\pi_{i^*}, \delta_i^{-1} u r_1^{k_1}, \phi^{r_2^{k_2}})) &= \left(\pi_{j'}, v', \phi_2^{\pi_{j'}^{-1} v' r_2^{k_2}} \right), \end{aligned}$$

and we need to show that the right hand side of the bottom two equations are equivalent under S_2 . Rearranging the above equations gives

$$\begin{aligned} \pi_{j'} r_1^{-k_1} &= v' p (\pi_{i^*}^{-1} \delta_i^{-1}) u \\ &= v' r_2^{k_2} (p \pi_i^{-1} u) \\ &= (v' r_2^{k_2} v^{-1}) \pi_j. \end{aligned}$$

Therefore

$$\begin{aligned} \left(\pi_{j'}, v', \phi_2^{\pi_{j'}^{-1} v' r_2^{k_2}} \right) &\sim_{S_2} \left(\pi_j, (v' r_2^{k_2} v^{-1})^{-1} v' r_2^{k_2}, \phi_2^{r_1^{k_1} \pi_j^{-1} v' r_2^{k_2}} \right) \\ &= \left(\pi_j, v, \phi_2^{\pi_j^{-1} v} \right), \end{aligned}$$

as claimed.

This proves the claim for T_p and the unweighted intersection number, and now we need to consider the sign and level. Under the correspondance θ , we start with the intersection pair (ϕ, ϕ_2) , and end with the pair $(\phi^{\pi_i}, \phi_2^{\pi_i})$. In particular,

$$\phi^{\pi_i} \times \phi_2^{\pi_i} = \pi_i(\phi \times \phi_2) \pi_i^{-1},$$

i.e. we apply conjugation by π_i . Since $\text{nrd}(\pi_i) = p > 0$, this does not change the sign of the intersection. Furthermore, for $q \mid \mathfrak{DM}$, we have $q \neq p$, whence conjugation by π_i does not affect the q -part of the level. In particular, the signed and the q -weighted intersection numbers are equal, as claimed.

All that remains is to show the self-adjointness of W_{p^e} for $p^e \parallel \mathfrak{DM}$. This is similar to the above, though much easier. For $u \in O_{N=1}$, write $u \omega_{p^e} = p^e \omega_{p^e}^{-1} v^{-1}$ with $v \in O_{N=1}$, and then

$$(\phi_1^{u \omega_{p^e}}, \phi_2) \Rightarrow (\phi_1^{\omega_{p^e} u \omega_{p^e}}, \phi_2^{\omega_{p^e}}) = (\phi_1^{v^{-1}}, \phi_2^{\omega_{p^e}}) \Rightarrow (\phi_1, \phi_2^{v \omega_{p^e}}).$$

Similarly to before, this is well-defined and provides the required bijection. The corresponding $\phi_1^{u\omega_{p^e}} \times \phi_2$ gets conjugated by ω_{p^e} , and this does not affect the sign or level since $\text{nrd}(\omega_{p^e}) > 0$ and $\omega_{p^e} \in N_{B^\times}(O)$. \square

In the above proposition, we used the fact that $q \nmid \mathfrak{DM}$ for the q -weighted equivalence. In fact, as seen in the proof, the q -weighted intersection number is self-adjoint for T_p as long as $q \neq p$. When $q = p$, there is no guarantee that it is self-adjoint, as there are examples where it is not.

When we start working with Hecke operators on cohomology, the current expression for T_n is less than ideal, as the coefficient is still quaternionic in nature. As such, it is useful to have an alternative expression, where we still sum over $\Theta(n)$.

Proposition 8.6.3. *Let n be coprime to \mathfrak{DM} . Then*

$$T_n([\phi]) = \sum_{\pi \in \Theta(n)} \frac{\log \epsilon_{D(\phi, O)}}{\log \epsilon_{D(\pi\phi\pi^{-1}, O)}} [(\pi\phi\pi^{-1})_O].$$

Proof. When n is prime, this follows from Propositions 8.4.2, 8.4.5, 8.5.2, and the prime power Hecke graph. The result in general follows from Lemmas 8.1.3 and 8.2.3. \square

There is no need for an alternate description of the Atkin-Lehner operators, as there are no “mysterious” coefficients.

8.7 Quaternionic modular forms

Our reference for this brief overview of quaternionic modular forms is sections 3, 5 of [DV13], and Sections 2, 3 of [GV11]. For uniformity of presentation, assume that $B \neq \text{Mat}(2, \mathbb{Q})$ (see Remark 8.9.4 for details on changes to the $B = \text{Mat}(2, \mathbb{Q})$ case). Fix an embedding $\iota : B \rightarrow \text{Mat}(2, \mathbb{R})$, and recall the definitions $\Gamma_O = \iota(O_{N=1})/\{\pm 1\}$ and $X_O = \Gamma_O \backslash \mathbb{H}$, the corresponding Shimura curve.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \iota(B^\times)/\{\pm 1\}$ and a holomorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$, we define the (weight two) slash operator as

$$(f|\gamma)(z) := \det(\gamma)(cz + d)^{-2} f(\gamma z).$$

Definition 8.7.1. A quaternionic modular form of weight 2 and level \mathfrak{M} for B is a holomorphic function $\mathbb{H} \rightarrow \mathbb{C}$ such that

$$(f|\gamma)(z) = f(z)$$

for all $\gamma \in \Gamma_O$.

Let $M_2^B(O)$ denote the space of weight two quaternionic modular forms with respect to O , and $S_2^B(O)$ the subset of cusp forms. Since $B \neq \text{Mat}(2, \mathbb{Q})$, there are no cusps, hence all quaternionic modular forms are cusp forms.

For a positive integer n coprime to $\mathfrak{D}\mathfrak{M}$, the Hecke operator T_n is defined as

$$(T_n f)(z) := \sum_{\pi \in \Theta(n)} (f|\pi)(z).$$

For $p^e \parallel \mathfrak{D}\mathfrak{M}$, the Atkin-Lehner operator W_{p^e} is defined as

$$(W_{p^e} f)(z) := (f|\omega_{p^e})(z).$$

When we refer to a Hecke operator, we are including the Atkin-Lehner operators.

As with the classical setting, there is an Eichler-Shimura relation. Specifically, if $f \in S_2^B(O)$, then $2\pi i f(z) dz$ defines a holomorphic differential 1-form on X_O (and vice versa). Integration over the homology gives us a Hecke-invariant isomorphism

$$S_2^B(O) \oplus \overline{S_2^B(O)} \xrightarrow{\sim} H^1(X_O, \mathbb{C}).$$

The connection to classical modular forms comes from the Jacquet-Langlands isomorphism, which gives

$$S_2^B(O) \simeq S_2(\mathfrak{D}\mathfrak{M})^{\mathfrak{D}\text{-new}},$$

where the last term is the space of (classical) weight two cusp forms for $\Gamma_0(\mathfrak{D}\mathfrak{M})$ that are new at all primes dividing \mathfrak{D} . The Jacquet-Langlands isomorphism respects the actions of T_p for primes $p \nmid \mathfrak{D}\mathfrak{M}$ and W_{p^e} for prime powers $p^e \parallel \mathfrak{D}\mathfrak{M}$, but we do have to be careful with the Atkin-Lehner involution: see Remark 8.8.2.

To describe the action of Hecke on H^1 , we first identify

$$H^1(X_O, \mathbb{C}) \simeq H^1(\Gamma_O, \mathbb{C}) = \text{Hom}(\Gamma_O, \mathbb{C}).$$

For $p \nmid \mathfrak{DM}$, let $\gamma \in \Gamma_O$, and then multiplication on the right by γ permutes $\Theta(p)$. Therefore there is a unique permutation γ^* of $\{1, 2, \dots, p+1\}$ for which

$$\pi_a \gamma = \delta_a \pi_{\gamma^* a}$$

for some $\delta_a \in \Gamma_O$ for all a . For $f \in \text{Hom}(\Gamma_O, \mathbb{C})$, we define

$$(T_p f)(\gamma) := \sum_{a=1}^{p+1} f(\delta_a).$$

Similarly, the action of W_{p^e} is defined as

$$(W_{p^e} f)(\gamma) := f(\omega_{p^e} \gamma \omega_{p^e}^{-1}).$$

To distinguish the holomorphic and anti-holomorphic components of $H^1(X_O, \mathbb{C})$, there is an action of complex conjugation, denoted T_∞ , that acts as the identity on the holomorphic component, and via -1 on the anti-holomorphic component. Pick any $\mu \in O_{N=-1}$, and for $\gamma \in O_{N=1}$, define

$$(T_\infty f)(\gamma) := f(\mu \gamma \mu^{-1}).$$

8.8 Weight 2 classical modular forms

The main reference for this section is [AL70]. In order to prove the modularity of E_{ϕ_1, ϕ_2}^\pm , we need to understand the connection between Hecke/Atkin-Lehner operators and Fourier coefficients of modular forms. A special case of Theorem 3 of [AL70] is the following proposition.

Proposition 8.8.1. *Let $f(\tau) = \sum_{n=1}^\infty a_n q^n$ be a weight 2 newform on $\Gamma_0(N)$, normalized so that $a_1 = 1$. Then*

(i) *If $p \nmid N$, then*

$$(a) \quad f|T_p = a_p f;$$

$$(b) \quad a_{np} = a_n a_p - p a_{n/p} \text{ for all } n \geq 1, \text{ with } a_{n/p} = 0 \text{ if } p \nmid n.$$

(ii) *If $p^e \parallel N$ with $e > 0$, then*

$$(a) \quad f|W_{p^e} = \lambda(p) f, \text{ where } \lambda(p) = \pm 1.$$

- (b) $a_{np} = a_n a_p$ for all $n \geq 1$;
- (c) If $e \geq 2$, then $a_p = 0$;
- (d) If $e = 1$, then $a_p = -\lambda(p)$, hence $f|W_{p^e} = -a_p f$.

In particular, if n is coprime to $\mathfrak{D}\mathfrak{M}$ then T_n produces the coefficient a_n , but otherwise we have to be a bit more careful.

Remark 8.8.2. In the Jacquet-Langlands correspondence, the Atkin-Lehner operators W_p for $p \mid \mathfrak{D}$ acting on Shimura curves in fact pick up the Eigenvalue a_p , and not $\lambda(p) = -a_p$ (see Theorem 1.2 of [BD96]). This is why we defined the good Hecke operator T_p to be W_p and not $-W_p$, as one may have initially thought. This choice is reflected in the examples in Section 8.10, as the coefficients of E_{ϕ_1, ϕ_2}^\pm divisible by primes ramifying in B are correct with our convention.

We will be working with the space $S_2(\Gamma_0(\mathfrak{D}\mathfrak{M}))^{\mathfrak{D}\text{-new}}$, hence if $\mathfrak{M} \neq 1$ we also need to work with oldforms. Theorem 5 of [AL70] provides the description of the new and oldforms, restated as follows.

Proposition 8.8.3. *The space $S_2(\Gamma_0(N))$ has a basis which is a direct sum of classes, which consist of newclasses and oldclasses. Every form in a class has the same eigenvalues for T_p with p a prime not dividing N , and forms in different classes have distinct eigenvalues at T_p for infinitely many primes p . Each newclass consists of a single form, which is an eigenform for all T_p and W_{p^e} . Each oldclass consists of a set of forms $\{f(d\tau)\}$, where $f \in S_2(\Gamma_0(N'))$ for some N' dividing N properly, and d ranges over all positive divisors of N/N' . Furthermore, any such set is an oldclass. Each oldclass can be given an alternate basis where the forms are also eigenforms for all W_{p^e} .*

While we can access the pn^{th} Fourier coefficients of an eigenform in $S_2(\Gamma_0(N))$ with $p \mid N$, it requires knowing which oldclass the form belongs to. If we have no a priori knowledge of this, then the task is less feasible. Since Jacquet-Langlands can produce \mathfrak{M} -old forms, we treat this issue by ignoring coefficients that are not coprime to \mathfrak{M} .

8.9 Proof of modularity

As before, assume that $B \neq \text{Mat}(2, \mathbb{Q})$. Write

$$\text{Emb}_{\mathbb{C}}^+(O) = \text{Emb}^+(O) \otimes \mathbb{C},$$

and for simplicity, assume that the quaternion algebra B lives inside $\text{Mat}(2, \mathbb{R})$, so that we drop the map ι . Consider the map $\alpha : \text{Emb}_{\mathbb{C}}^+(O) \rightarrow H_1(X_O, \mathbb{C})$ induced by

$$[\phi] \rightarrow [\tilde{\ell}_{\tau, \phi(\epsilon_D)\tau}],$$

where $\phi : \mathcal{O}_D \rightarrow O$ is optimal and $\tau \in \mathbb{H}$. First, we note that this is independent of the choice of τ since in homology we have

$$\tilde{\ell}_{\tau, \phi(\epsilon_D)\tau} - \tilde{\ell}_{\tau', \phi(\epsilon_D)\tau'} = \tilde{\ell}_{\tau, \tau'} - \tilde{\ell}_{\phi(\epsilon_D)\tau, \phi(\epsilon_D)\tau'} = \tilde{\ell}_{\tau, \tau'} - \tilde{\ell}_{\tau, \tau'} = 0.$$

The map is also well-defined, as if $u \in O_{N=1}$, then the embedding $u\phi u^{-1}$ is sent to

$$\tilde{\ell}_{\tau, u\phi(\epsilon_D)u^{-1}\tau} = \tilde{\ell}_{(u^{-1}\tau), \phi(\epsilon_D)(u^{-1}\tau)} = \tilde{\ell}_{\tau, \phi(\epsilon_D)\tau},$$

as desired.

Lemma 8.9.1. *The map α is surjective.*

Proof. Let P be a path representing a basis element in $H_1(X_O, \mathbb{C})$; it suffices to show that P lies in the image of α . Lift P to \mathbb{H} , and we get a path between τ and $\gamma\tau$ for some $\tau \in \mathbb{H}$ and $\gamma \in O_{N=1}$. In particular, P is equal in homology to $\tilde{\ell}_{\tau, \gamma\tau}$. Since the primitive hyperbolic elements of $O_{N=1}$ generate the group, we can express $\gamma = \prod_{i=1}^N \gamma_i^{n_i}$ as a word in primitive hyperbolic elements, and then

$$P = \alpha \left(\sum_{i=1}^N n_i [\gamma_i] \right),$$

as desired. □

Therefore a general element of $H_1(X_O, \mathbb{C})$ can be written as a \mathbb{C} -linear combination of terms $\tilde{\ell}_{\tau, \gamma\tau}$ for $\gamma \in \Gamma_O$ primitive and hyperbolic.

Let β be the isomorphism from $H_1(X_O, \mathbb{C})$ to its dual $H^1(X_O, \mathbb{C})$, given by

$$\beta(\psi)(\psi') = \langle \psi, \psi' \rangle_{\pm},$$

where $\psi, \psi' \in H_1(X_O, \mathbb{C})$ and $\langle \cdot, \cdot \rangle_{\pm}$ is the signed intersection pairing. The translated action of T_p for $p \nmid \mathfrak{DM}$ on $H^1(X_O, \mathbb{C})$ is induced by

$$T_p(f)(\gamma_{\tau, \gamma\tau}) = \sum_{\pi_a \in \Theta(p)} f(\ell_{\tau, \delta_a \tau}),$$

for any $f \in H^1(X_O, \mathbb{C})$, $\tau \in \mathbb{H}$, $\gamma \in \Gamma_O$ primitive hyperbolic, where as before $\pi_a \gamma = \delta_a \pi_{\gamma^* a}$. Similarly, if $p^e \parallel \mathfrak{DM}$,

$$W_{p^e}(f)(\gamma_{\tau, \gamma\tau}) = f(\ell_{\tau, \omega_{p^e} \gamma \omega_{p^e}^{-1} \tau}),$$

and a similar expression holds for T_{∞} .

By composing $\beta \circ \alpha$, we get a map from $\text{Emb}_{\mathbb{C}}^+(O)$ to $H^1(X_O, \mathbb{C})$, where we have defined Hecke operators on each end.

Lemma 8.9.2. *The map $\beta \circ \alpha$ is Hecke-equivariant for T_p with $p \nmid \mathfrak{DM}$, W_{p^e} for $p^e \parallel \mathfrak{DM}$, and T_{∞} .*

Proof. Start with T_p for $p \nmid \mathfrak{DM}$. Let $[\phi]$ be an optimal embedding class of discriminant D , let σ be an optimal embedding of discriminant D' , let $\gamma = \sigma(\epsilon_{D'})$, and the map $T_p(\beta \circ \alpha([\phi]))$ is induced by

$$T_p(\beta \circ \alpha([\phi]))(\tilde{\ell}_{\tau, \gamma\tau}) = \sum_{\pi_a \in \Theta(p)} \langle \tilde{\ell}_{\tau, \phi(\epsilon_D)\tau}, \tilde{\ell}_{\tau, \delta_a \tau} \rangle_{\pm},$$

where $\pi_a \gamma = \delta_a \pi_{\gamma^* a}$.

Applying T_p to $[\phi]$ first gives

$$\begin{aligned} \beta \circ \alpha(T_p([\phi]))(\tilde{\ell}_{\tau, \gamma\tau}) &= \langle \alpha(T_p[\phi]), \alpha([\sigma]) \rangle_{\pm} \\ &= \langle \alpha([\phi]), \alpha(T_p[\sigma]) \rangle_{\pm} \\ &= \sum_{\pi_a \in \Theta(p)} \frac{\log \epsilon_{D'}}{\log \epsilon_{D(\sigma^{\pi_a}, O)}} \langle \tilde{\ell}_{\tau, \phi(\epsilon_D)\tau}, \tilde{\ell}_{\tau, \sigma_O^{\pi_a}(\epsilon_{D(\sigma^{\pi_a}, O)})\tau} \rangle_{\pm}, \end{aligned}$$

where we used that the intersection pairing is Hecke-adjoint, Proposition 8.6.2. Thus it suffices to prove that in homology,

$$\sum_{\pi_a \in \Theta(p)} \tilde{\ell}_{\tau, \delta_a \tau} = \sum_{\pi_a \in \Theta(p)} \frac{\log \epsilon_{D'}}{\log \epsilon_{D(\sigma^{\pi_a}, O)}} \tilde{\ell}_{\tau, \sigma_O^{\pi_a}(\epsilon_{D(\sigma^{\pi_a}, O)})\tau}.$$

Consider $\delta_a = \pi_a \gamma \pi_{\gamma^* a}^{-1}$, and note that if a_1, a_2, \dots, a_r is a sequence, then

$$\sum_{i=1}^r \tilde{\ell}_{\tau, \delta_{a_i} \tau} = \tilde{\ell}_{\tau, \delta_{a_1} \delta_{a_2} \cdots \delta_{a_r} \tau}.$$

Decompose the permutation γ^* into cycles, and say (a_1, a_2, \dots, a_r) is one such cycle. The intermediate terms all cancel, and we derive that

$$\delta_{a_1} \delta_{a_2} \cdots \delta_{a_j} = \pi_{a_1} \gamma^j \pi_{a_{\gamma^* j}}^{-1},$$

for all j . Thus

$$\phi^{\pi_{a_1}}(\epsilon_{D'}^j) = \delta_{a_1} \delta_{a_2} \cdots \delta_{a_j} \pi_{a_{\gamma^* j}} \pi_{a_1}^{-1},$$

so if $r > 1$ this does not lie in O for $j = 1, 2, \dots, r-1$, but does for $j = r$. In particular, $\sigma^{\pi_{a_1}}$ has fundamental unit $\epsilon_{D'}^r$, when $r > 1$. Since cycles are cyclic, the same is true for $\sigma^{\pi_{a_i}}$ for all $1 \leq i \leq r$. Using the equation

$$\delta_{a_i} \delta_{a_{i+1}} \cdots \delta_{a_{i-1}} = \pi_{a_i} \gamma^r \pi_{a_i}^{-1},$$

we derive

$$\begin{aligned} \sum_{i=1}^r \tilde{\ell}_{\tau, \delta_{a_i} \tau} &= \sum_{i=1}^r \frac{1}{r} \tilde{\ell}_{\tau, \pi_{a_i} \gamma^r \pi_{a_i}^{-1} \tau} \\ &= \sum_{i=1}^r \frac{\log \epsilon_{D'}}{\log \epsilon_{D(\sigma^{\pi_{a_i}}, O)}} \tilde{\ell}_{\tau, \sigma^{\pi_{a_i}}(\epsilon_{D(\sigma^{\pi_{a_i}}, O)})^\tau}, \end{aligned}$$

which has the desired form. When $r = 1$, let $a_1 = a$ and then $\delta_a = \pi_a \gamma \pi_a^{-1}$. The fundamental unit of σ^{π_a} is $\epsilon_{D'}^{1/r'}$ for some positive integer r' , and we get the analogous result to the above by writing $\gamma = \sigma^{\pi_a}(\epsilon_{D'}^{1/r'})^{r'}$. By summing over all cycles in γ^* , the result follows for T_p .

The cases of W_{p^e} for $p^e \parallel \mathfrak{DM}$ and T_∞ are much easier, and follow directly from the definitions. \square

At last, we are ready to tackle modularity. By combining Eichler-Shimura, Jacquet-Langlands, and β , we have an Hecke-invariant isomorphism

$$H_1(X_O, \mathbb{C}) \simeq S_2(\mathfrak{DM})^{\mathfrak{D}-\text{new}} \oplus \overline{S_2(\mathfrak{DM})}^{\mathfrak{D}-\text{new}}.$$

The eigenvalues of $\overline{S_2(\mathfrak{DM})}^{\mathfrak{D}-\text{new}}$ are complex conjugates of the eigenvalues of $S_2(\mathfrak{DM})^{\mathfrak{D}-\text{new}}$, but since this space is fixed under $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can pair them up. In particular, by Proposition 8.8.3 there exists a decomposition,

$$H_1(X_O, \mathbb{C}) = \bigoplus_{m \mid \mathfrak{M}} V_m,$$

where each V_m can be decomposed into eigenspaces corresponding to the eigensystems for newforms on $S_2(\Gamma_0(\mathfrak{D}m))$. Each eigenspace of V_m can then be decomposed into a basis of eigenforms for all T_p and W_{p^e} ; such bases will have twice the size of the corresponding bases in $S_2(\mathfrak{D}\mathfrak{M})^{\mathfrak{D}-\text{new}}$, since they also include the conjugated forms.

Take two basis elements, call them γ, γ' , say that they correspond to $V_m, V_{m'}$ respectively, as well as to the eigensystems $T_p\gamma = a_p\gamma$, $W_{p^e}\gamma = a_p\gamma$ (and the same with γ' and a'_p). By Proposition 8.8.3, if these are distinct eigensystems, there exists a $p \nmid \mathfrak{D}\mathfrak{M}$ with $a_p \neq a'_p$. Then

$$a_p \langle \gamma, \gamma' \rangle_{\pm} = \langle T_p \gamma, \gamma' \rangle_{\pm} = \langle \gamma, T_p \gamma' \rangle_{\pm} = a'_p \langle \gamma, \gamma' \rangle_{\pm},$$

whence $\langle \gamma, \gamma' \rangle_{\pm} = 0$. Therefore the only way for this pairing to be non-zero is if $m = m'$ and $a_p = a'_p$ for all p . Assume this, and for simplicity assume that the elements are normalized so that $\langle \gamma, \gamma' \rangle_{\pm} = 1$.

Proposition 8.9.3. *There exists a modular form $E' \in S_2(\Gamma_0(\mathfrak{D}\mathfrak{M}))^{\mathfrak{D}-\text{new}}$ such that the n^{th} coefficient of E' equals $\langle \gamma, T_n \gamma' \rangle_{\pm}$ for all n coprime to \mathfrak{M} .*

Proof. Let E' correspond to the modular form with coefficients a_n , and let $c_n = \langle \gamma, T_n \gamma' \rangle_{\pm}$. If $p \nmid \mathfrak{D}\mathfrak{M}$, then as above, $c_p = a_p$. If $p \mid \mathfrak{D}$, then $c_p = a_p$ follows from Remark 8.8.2. Therefore, by combining Lemma 8.2.3 with Proposition 8.8.1, it follows that $c_n = a_n$ for all n coprime to \mathfrak{M} . \square

In particular, Theorem 8.0.4 follows immediately from this.

Remark 8.9.4. When $B = \text{Mat}(2, \mathbb{Q})$, then we are initially working with the open curve $Y_O = \Gamma_O \backslash \mathbb{H}$. In this case, Poincaré duality (via the map β) instead lands in the cohomology of the closed curve X_O , relative to the cusps. Eichler-Shimura gives the isomorphism to $S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$, as desired (N being the level of O).

8.10 Examples

It is instructive to demonstrate that we are able to generate non-trivial modular forms, that they do not have to be eigenforms, and that they need not be \mathfrak{M} -new. The labels of newforms correspond to the labels given in LMFDB ([LMF20]).

For a first example, we consider a situation where we get a combination of newforms, so the resulting form is not an eigenform.

Example 8.10.1. Let $B = \left(\frac{7,5}{\mathbb{Q}}\right)$ be ramified at 5, 7, and let O be the maximal order spanned by $\{1, \frac{1+j}{2}, i, \frac{1+i+j+k}{2}\}$. Thus $\mathfrak{D} = 35$, $\mathfrak{M} = 1$, and the dimension of weight two newforms on $\Gamma_0(35)$ is 3. Label the forms f, g, \bar{g} , where f is given by 35.2.a.a in LMFDB, and g is given by 35.2.a.b. The coefficients of g are given in terms of $\beta = \frac{1+\sqrt{17}}{2}$, and the first 50 coefficients of f, g are given by

$$\begin{aligned} f(\tau) = & q^1 + q^3 - 2q^4 - q^5 + q^7 - 2q^9 - 3q^{11} - 2q^{12} + 5q^{13} - q^{15} + 4q^{16} \\ & + 3q^{17} + 2q^{19} + 2q^{20} + q^{21} - 6q^{23} + q^{25} - 5q^{27} - 2q^{28} + 3q^{29} - 4q^{31} - 3q^{33} - q^{35} \\ & + 4q^{36} + 2q^{37} + 5q^{39} - 12q^{41} - 10q^{43} + 6q^{44} + 2q^{45} + 9q^{47} + 4q^{48} + q^{49} + O(q^{51}), \end{aligned}$$

and

$$\begin{aligned} g(\tau) = & q^1 - \beta q^2 + (-1 + \beta)q^3 + (2 + \beta)q^4 + q^5 - 4q^6 - q^7 + (-4 - \beta)q^8 + (2 - \beta)q^9 - \beta q^{10} \\ & + (1 - \beta)q^{11} + (2 + 2\beta)q^{12} + (3 - \beta)q^{13} + \beta q^{14} + (-1 + \beta)q^{15} + 3\beta q^{16} + (-3 + \beta)q^{17} \\ & + (4 - \beta)q^{18} + (-2 - 2\beta)q^{19} + (2 + \beta)q^{20} + (1 - \beta)q^{21} + 4q^{22} + (-2 + 2\beta)q^{23} - 4\beta q^{24} + q^{25} \\ & + (4 - 2\beta)q^{26} + (-3 - \beta)q^{27} + (-2 - \beta)q^{28} + (-1 + 3\beta)q^{29} - 4q^{30} + (-4 - \beta)q^{32} + (-5 + \beta)q^{33} \\ & + (-4 + 2\beta)q^{34} - q^{35} - \beta q^{36} + 6q^{37} + (8 + 4\beta)q^{38} + (-7 + 3\beta)q^{39} + (-4 - \beta)q^{40} + 2\beta q^{41} \\ & + 4q^{42} + (6 - 2\beta)q^{43} + (-2 - 2\beta)q^{44} + (2 - \beta)q^{45} - 8q^{46} + (-1 - 3\beta)q^{47} + 12q^{48} + q^{49} - \beta q^{50} + O(q^{51}). \end{aligned}$$

Take the optimal embeddings of discriminants 5, 12 given by

$$\phi_1 \left(\frac{1 + \sqrt{5}}{2} \right) = \frac{1 - j}{2}, \quad \phi_2 \left(\frac{\sqrt{12}}{2} \right) = -\frac{-i - 8j - 3k}{2}.$$

We compute the first 50 terms of E_{ϕ_1, ϕ_2}^{\pm} to be

$$\begin{aligned} & q^2 - q^3 - q^4 + q^8 + q^9 + q^{10} + q^{11} - 2q^{12} + q^{13} - q^{14} - q^{15} - 3q^{16} \\ & - q^{17} + q^{18} + 2q^{19} - q^{20} + q^{21} - 2q^{23} + 4q^{24} + 2q^{26} + q^{27} + q^{28} - 3q^{29} + q^{32} - q^{33} \\ & - 2q^{34} + q^{36} - 4q^{38} - 3q^{39} + q^{40} - 2q^{41} + 2q^{43} + 2q^{44} + q^{45} + 3q^{47} + q^{50} + O(q^{51}). \end{aligned}$$

By matching the coefficients, we have

$$E_{\phi_1, \phi_2}^{\pm} = \frac{-g(\tau) + \bar{g}(\tau)}{\sqrt{17}}.$$

Next, take the optimal embedding of discriminant 173 given by

$$\phi_3 \left(\frac{1 + \sqrt{173}}{2} \right) = \frac{1 - 2i + 27j - 10k}{2},$$

and we compute the first 50 terms of E_{ϕ_2, ϕ_3}^{\pm} to be

$$\begin{aligned} & 2q^1 - q^2 + 3q^4 + q^5 - 6q^6 - q^7 - 7q^8 + q^9 - q^{10} - q^{11} + 4q^{12} + 6q^{13} + q^{14} - q^{15} \\ & + 5q^{16} - 2q^{17} + 5q^{18} - 4q^{19} + 5q^{20} + q^{21} + 6q^{22} - 4q^{23} - 4q^{24} + 2q^{25} + 4q^{26} - 8q^{27} \\ & - 5q^{28} + 3q^{29} - 6q^{30} - 2q^{31} - 7q^{32} - 8q^{33} - 4q^{34} - 2q^{35} + q^{36} + 10q^{37} + 16q^{38} - 5q^{39} \\ & - 7q^{40} - 4q^{41} + 6q^{42} + 2q^{43} - 2q^{44} + 3q^{45} - 12q^{46} + 20q^{48} + 2q^{49} - q^{50} + O(q^{51}). \end{aligned}$$

By matching the coefficients, we have

$$E_{\phi_2, \phi_3}^{\pm} = \frac{1}{2}f(\tau) + \frac{51 + \sqrt{17}}{68}g(\tau) + \frac{51 - \sqrt{17}}{68}\bar{g}(\tau).$$

Next, consider a non-maximal Eichler order.

Example 8.10.2. Let $B = \left(\frac{7, -1}{\mathbb{Q}} \right)$ be ramified at 2, 7, and let O be the Eichler order of level 3 spanned by $\left\{ 1, 3i, 2i + j, \frac{1+5i+j+k}{2} \right\}$. Thus $\mathfrak{D} = 14$, $\mathfrak{M} = 3$, and the dimensions of the space of weight two newforms on each of $\Gamma_0(14)$ and $\Gamma_0(42)$ is 1. Let the eigenforms be f, g respectively, so that f is given by the label 14.2.a.a in LMFDB, and g is 42.2.a.a. The first 100 terms of the forms are given by

$$\begin{aligned} f(\tau) = & q^1 - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 - 2q^{12} - 4q^{13} - q^{14} + q^{16} + 6q^{17} - q^{18} + 2q^{19} \\ & - 2q^{21} + 2q^{24} - 5q^{25} + 4q^{26} + 4q^{27} + q^{28} - 6q^{29} - 4q^{31} - q^{32} - 6q^{34} + q^{36} + 2q^{37} - 2q^{38} + 8q^{39} \\ & + 6q^{41} + 2q^{42} + 8q^{43} - 12q^{47} - 2q^{48} + q^{49} + 5q^{50} - 12q^{51} - 4q^{52} + 6q^{53} - 4q^{54} - q^{56} - 4q^{57} + 6q^{58} - 6q^{59} \\ & + 8q^{61} + 4q^{62} + q^{63} + q^{64} - 4q^{67} + 6q^{68} - q^{72} + 2q^{73} - 2q^{74} + 10q^{75} + 2q^{76} - 8q^{78} + 8q^{79} - 11q^{81} \\ & - 6q^{82} - 6q^{83} - 2q^{84} - 8q^{86} + 12q^{87} - 6q^{89} - 4q^{91} + 8q^{93} + 12q^{94} + 2q^{96} - 10q^{97} - q^{98} - 5q^{100} + O(q^{101}), \end{aligned}$$

and

$$\begin{aligned}
 g(\tau) = & q^1 + q^2 - q^3 + q^4 - 2q^5 - q^6 - q^7 + q^8 + q^9 - 2q^{10} - 4q^{11} - q^{12} + 6q^{13} - q^{14} + 2q^{15} + q^{16} \\
 & + 2q^{17} + q^{18} - 4q^{19} - 2q^{20} + q^{21} - 4q^{22} + 8q^{23} - q^{24} - q^{25} + 6q^{26} - q^{27} - q^{28} - 2q^{29} + 2q^{30} + q^{32} + 4q^{33} \\
 & + 2q^{34} + 2q^{35} + q^{36} - 10q^{37} - 4q^{38} - 6q^{39} - 2q^{40} - 6q^{41} + q^{42} - 4q^{43} - 4q^{44} - 2q^{45} + 8q^{46} - q^{48} + q^{49} - q^{50} \\
 & - 2q^{51} + 6q^{52} + 6q^{53} - q^{54} + 8q^{55} - q^{56} + 4q^{57} - 2q^{58} + 4q^{59} + 2q^{60} + 6q^{61} - q^{63} + q^{64} - 12q^{65} + 4q^{66} + 4q^{67} \\
 & + 2q^{68} - 8q^{69} + 2q^{70} + 8q^{71} + q^{72} + 10q^{73} - 10q^{74} + q^{75} - 4q^{76} + 4q^{77} - 6q^{78} - 2q^{80} + q^{81} - 6q^{82} - 4q^{83} + q^{84} \\
 & - 4q^{85} - 4q^{86} + 2q^{87} - 4q^{88} - 6q^{89} - 2q^{90} - 6q^{91} + 8q^{92} + 8q^{95} - q^{96} - 14q^{97} + q^{98} - 4q^{99} - q^{100} + O(q^{101}).
 \end{aligned}$$

Take the embeddings of discriminants 13, 24 given by

$$\phi_1 \left(\frac{1 + \sqrt{13}}{2} \right) = \frac{1 + i - j + k}{2}, \quad \phi_2 \left(\frac{\sqrt{24}}{2} \right) = -5i - 13j.$$

We compute the first 100 terms of E_{ϕ_1, ϕ_2}^{\pm} to be

$$\begin{aligned}
 & -q^1 + q^2 - q^4 - q^7 + q^8 + 4q^{13} + q^{14} - q^{16} - 6q^{17} - 2q^{19} + 5q^{25} - 4q^{26} - q^{28} + 6q^{29} \\
 & + 4q^{31} + q^{32} + 6q^{34} - 2q^{37} + 2q^{38} - 6q^{41} - 8q^{43} + 12q^{47} - q^{49} - 5q^{50} + 4q^{52} - 6q^{53} \\
 & + q^{56} - 6q^{58} + 6q^{59} - 8q^{61} - 4q^{62} - q^{64} + 4q^{67} - 6q^{68} - 2q^{73} + 2q^{74} - 2q^{76} - 8q^{79} \\
 & + 6q^{82} + 6q^{83} + 8q^{86} + 6q^{89} + 4q^{91} - 12q^{94} + 10q^{97} + q^{98} + 5q^{100} + O(q^{101}).
 \end{aligned}$$

By matching the coefficients of q^1, q^2 , we have

$$E_{\phi_1, \phi_2}^{\pm} = -f(\tau) + R(q^3),$$

for some power series R . This continues to hold up until coefficient 100 by the above computations, as is expected. If we want an equality of modular forms, this can be achieved by bumping up the level to access the form $f(9q)$ and using this to erase all coefficients of q^{3n} :

$$E_{\phi_1, \phi_2}^{\pm} = -f(\tau) - 2f(3\tau) - 3f(9\tau).$$

Finally, we demonstrate an example where the old and newforms are non-trivially com-

bined. Let $D_3 = 45$ and $\phi_3\left(\frac{1+\sqrt{45}}{2}\right) = \frac{1-3i-9j+3k}{2}$, and the first 100 terms of E_{ϕ_1, ϕ_3}^\pm are

$$\begin{aligned} & q^1 + q^4 - q^5 - q^{10} - 2q^{11} + q^{13} - q^{14} + q^{16} + 4q^{17} - q^{19} - q^{20} - 2q^{22} + 4q^{23} - 3q^{25} + 5q^{26} - 4q^{29} - 2q^{31} \\ & - 2q^{34} + q^{35} - 4q^{37} - 3q^{38} - q^{40} + 2q^{43} - 2q^{44} + 4q^{46} - 6q^{47} + q^{49} + 2q^{50} + q^{52} + 6q^{53} + 4q^{55} - q^{56} + 2q^{58} \\ & - q^{59} + 7q^{61} + 2q^{62} + q^{64} - 6q^{65} + 4q^{68} + q^{70} + 4q^{71} + 6q^{73} - 6q^{74} - q^{76} + 2q^{77} + 4q^{79} - q^{80} - 6q^{82} - 5q^{83} \\ & - 2q^{85} - 6q^{86} - 2q^{88} - 6q^{89} - 5q^{91} + 4q^{92} + 6q^{94} + 4q^{95} - 12q^{97} - 3q^{100} + O(q^{101}) \end{aligned}$$

Matching coefficients gives

$$E_{\phi_1, \phi_3}^\pm = \frac{f(\tau) + g(\tau)}{2} + R(q^3),$$

for some power series R .

Chapter 9

Connection to a real quadratic analogue of the j -function

Let $j(\tau) = \frac{1}{q} + 744 + \dots$ be the classical j -function, where $q = e^{2\pi i\tau}$. If τ is a quadratic irrational number of discriminant D (i.e. $\langle 1, \tau \rangle_{\mathbb{Z}} = \mathcal{O}_D$), then the theory of complex multiplication implies that $j(\tau)$ is an algebraic integer for which $\mathbb{Q}(\sqrt{D})(j(\tau))$ is the ring class field of \mathcal{O}_D (see [Cox13] for a full treatment). Going further, in “On singular moduli” by Gross and Zagier ([GZ85]), the factorization of $j(\tau_1) - j(\tau_2)$ is studied, where τ_1, τ_2 are imaginary quadratic irrationalities of coprime fundamental discriminants D_1, D_2 . They give an expression for $v_p(\text{norm}(j(\tau_1) - j(\tau_2)))$, which is always 0 except for when p divides an integer of the form

$$\frac{D_1 D_2 - x^2}{4},$$

for $x \equiv D_1 D_2 \pmod{2}$ and $|x| < \sqrt{D_1 D_2}$. This work was extended by Dorman in [Dor88], as well as by Lauter and Viray in [LV15] to all pairs of discriminants when $p > 2$. In these works, the computation of $v_p(\text{norm}(j(\tau_1) - j(\tau_2)))$ essentially boils down to a computation of an arithmetic intersection number of optimal embeddings into Eichler orders in the quaternion algebra ramified at p and ∞ .

In “Singular moduli for real quadratic fields” by Darmon and Vonk ([DV20]), a conjectural analogue in to $j(\tau_1) - j(\tau_2)$ is given for real quadratic numbers. More concretely, let $p \in \{2, 3, 5, 7, 13\}$ be a genus zero prime (i.e. there are no cusp forms on $\Gamma_0(p)$), let \mathbb{H}_p denote

the p -adic upper half plane, and let τ_1, τ_2 be real quadratic points in \mathbb{H}_p of discriminants D_1, D_2 . Using rigid meromorphic cocycles, they define the quantity

$$J_p(\tau_1, \tau_2) \in \mathbb{C}_p^\times / \langle \epsilon_{\tau_1}^{\mathbb{Z}} \rangle,$$

where ϵ_{τ_1} is the fundamental unit associated to τ_1 . Lift $J_p(\tau_1, \tau_2)$ to \mathbb{C}_p^\times , assume that D_1, D_2 are coprime, let H_1, H_2 be the ring class fields associated to D_1, D_2 , and let H_{12} be the composition.

Conjecture 9.0.1. *[Conjecture 4.19 of [DV20]] The quantity $J_p(\tau_1, \tau_2)$ belongs to H_{12} . In particular, we can consider the \mathfrak{q} -adic valuation for primes \mathfrak{q} of H_{12} .*

Let \mathfrak{q} lie above the integer prime q , let B be the quaternion algebra ramified at p, q , let O be a maximal order of B .

Conjecture 9.0.2. *[Conjecture 4.26 of [DV20]] If q is split in $\mathbb{Q}(\sqrt{D_1})$ or $\mathbb{Q}(\sqrt{D_2})$, then $\text{ord}_{\mathfrak{q}}(J_p(\tau_1, \tau_2)) = 0$. Otherwise, there exist optimal embeddings ϕ_1, ϕ_2 of discriminants D_1, D_2 into O for which*

$$\text{ord}_{\mathfrak{q}}(J_p(\tau_1, \tau_2)) = \text{Int}_O^{\mathfrak{q}}(\phi_1, \phi_2).$$

In other words, the exponents of primes above q in the factorizations of $J_p(\tau_1, \tau_2)$ are given by q -weighted intersection numbers associated to optimal embeddings of D_1, D_2 into a maximal order in the indefinite quaternion algebra ramified at p, q .

Combining this conjecture with the results of this thesis, we achieve a similar statement about the shape of primes dividing $J_p(\tau_1, \tau_2)$.

Corollary 9.0.3. *Assume that Conjectures 9.0.1 and 9.0.2 hold. Then if \mathfrak{q} lies above q in H_{12} and $\text{ord}_{\mathfrak{q}}(J_p(\tau_1, \tau_2)) \neq 0$, then there exists an integer x with $x \equiv D_1 D_2 \pmod{2}$ and $|x| < \sqrt{D_1 D_2}$ for which the set of prime numbers r with $\epsilon(r) = -1$ that satisfy $v_r\left(\frac{D_1 D_2 - x^2}{4}\right)$ is odd is exactly the set $\{p, q\}$. In particular,*

$$q \mid \frac{D_1 D_2 - x^2}{4p}.$$

We are able to take this analogy a little further by considering the action of class groups. On the Darmon-Vonk side, define

$$J_p^+(\tau_1, \tau_2) = \frac{J_p(\tau_1, \tau_2)}{J_p(p\tau_1, \tau_2)}, \quad J_p^-(\tau_1, \tau_2) = J_p(\tau_1, \tau_2) J_p(p\tau_1, \tau_2).$$

On the quaternionic side, fix $[\phi_i] \in \text{Emb}(O, D_i)$ for $i = 1, 2$, and let $\phi'_1 = \phi_1^{\omega_p}$ be the embedding where we swap orientations at p . Let $G_{12} = \text{Cl}^+(D_1) \times \text{Cl}^+(D_2)$, and then G_{12} acts on $[\phi_1], [\phi_2]$ via the class group action (from Section 4.5) in each component. Form the elements of the formal group $\mathbb{Z}[G_{12}]$ (where we write $g = (g_1, g_2)$):

$$I_{p,q}(D_1, D_2) = \sum_{g \in G_{12}} \text{Int}_O^g(g_1[\phi_1], g_2[\phi_2]) \cdot g,$$

$$I'_{p,q}(D_1, D_2) = \sum_{g \in G_{12}} \text{Int}_O^g(g_1[\phi'_1], g_2[\phi_2]) \cdot g.$$

Define

$$I_{p,q}^+(D_1, D_2) = I_{p,q}(D_1, D_2) + I'_{p,q}(D_1, D_2), \quad I_{p,q}^-(D_1, D_2) = I_{p,q}(D_1, D_2) - I'_{p,q}(D_1, D_2).$$

To put things together, note that G_{12} acts on primes above q in H_{12} ; denote the action of g on \mathfrak{q} by \mathfrak{q}^g .

Conjecture 9.0.4. *We have*

$$\sum_{g \in G_{12}} \text{ord}_{\mathfrak{q}^g}(J_p^\pm(\tau_1, \tau_2)) \cdot g = I_{p,q}^\pm(D_1, D_2) \pmod{G_{12}},$$

where the equality is modulo multiplication by G_{12} .

Besides the theoretical support behind these conjectures, there is vast numerical support. Jan Vonk wrote has efficient algorithms to compute $J_p(\tau_1, \tau_2)$ with large p -adic accuracy, and the resulting quantities then tested for algebraicity. Analogously, I have computed optimal embeddings into orders and the corresponding intersection numbers. I generated a document detailing all possible intersections for $D_1 = 5, 13$ and $D_2 \leq 1000$ (which ran to around 600 pages), and the numbers matched in all cases.

To provide an example, we take Example 4.29 of [DV20]. Let $(D_1, D_2) = (13, 621)$, so that $h^+(D_1) = 1$, and $\text{Cl}^+(D_2) = \mathbb{Z}/6\mathbb{Z}$, generated by g . Let $p = 7$, and there are 6 RM points of discriminant 621. With 200 digits of 7-adic precision, Vonk computed that the resulting invariants $J_7^+(\tau_1, \tau_2)$ (over the six choices of τ_2) were the roots of

$$4378144x^6 - 5762700x^5 + 9490680x^4 - 11616641x^3 + 9490680x^2 - 5762700x + 4378144.$$

Furthermore, the invariants $J_7^-(\tau_1, \tau_2)$ satisfied

$$17932877824x^6 + 69949203456x^5 + 143523182304x^4 + 177833888503x^3 \\ + 143523182304x^2 + 69949203456x + 17932877824.$$

Since we have the factorizations

$$4378144 = 2^5 41^1 47^1 71^1, \quad 17932877824 = 2^{17} 41^1 47^1 71^1,$$

the q -adic valuations of the roots are 0 away from $q = 2, 41, 47, 71$. Similarly, by applying Theorem 7.1.2 to D_1, D_2 , for each odd integer x with $|x| < \sqrt{13 \cdot 621} \leq 89.9$, we can compute the factorization of $\frac{13 \cdot 621 - x^2}{4}$, and this will determine the unique indefinite quaternion algebra for which $\text{Emb}(O, 13, 621, x)$ is non-empty. The set of possible ramification places is computed to be

$$\{[], [2, 7], [2, 19], [2, 37], [2, 41], [2, 47], [2, 59], [2, 67], [2, 97], [2, 109], [2, 229], \\ [2, 241], [2, 379], [2, 631], [2, 709], [2, 733], [2, 1009], [7, 41], [7, 47], [7, 71]\}.$$

The pairs containing 7 are $[2, 7], [7, 41], [7, 47], [7, 71]$, which correspond to $q = 2, 41, 47, 71$ respectively, exactly as before. In particular, for q not in this set, the claimed result holds. For q in this set, fix \mathfrak{q} above q , and let $\text{ord}_{\mathfrak{q}}(\cdot)$ denote the length 6 vector where the i^{th} component is the slope of the Newton polygon of \cdot between $i - 1$ and i . The \mathfrak{q} -adic valuations of the roots correspond to the negative of this set of slopes. Table 9.1 lists the corresponding computations for I, I' and J^+, J^- , as computed by me and Vonk respectively.

Table 9.1: Computation of I, I', J^+, J^- .

| q | $I_{q,7}(13, 621)$ | $I'_{q,7}(13, 621)$ | $\text{ord}_{\mathfrak{q}} J^+(\tau_1, \tau_2)$ | $\text{ord}_{\mathfrak{q}} J^-(\tau_1, \tau_2)$ |
|-----|----------------------------|-----------------------------|---|---|
| 2 | $(1 - g^3)(2 + 5g + 2g^2)$ | $(1 - g^3)(-3 - 2g - 3g^2)$ | $(3, 1, 1, -1, -1, -3)$ | $(7, 5, 5, -5, -5, -7)$ |
| 41 | $1 - g^3$ | 0 | $(1, 0, 0, 0, 0, -1)$ | $(1, 0, 0, 0, 0, -1)$ |
| 47 | $1 - g^3$ | 0 | $(1, 0, 0, 0, 0, -1)$ | $(1, 0, 0, 0, 0, -1)$ |
| 71 | $1 - g^3$ | 0 | $(1, 0, 0, 0, 0, -1)$ | $(1, 0, 0, 0, 0, -1)$ |

By adding and subtracting the first two columns, the coefficients of correspond to the vectors appearing in the third and fourth columns, as claimed.

Chapter 10

Algorithms

This chapter is dedicated to providing overviews of some of the algorithms used in computing intersection numbers. For the sake of brevity, we will focus on the most important algorithms only, as well as just giving a general overview of why they work (as opposed to a fully formal setup with detailed proofs). Most of the algorithms used in the computations are implemented in PARI ([The20]), and publicly available in the GitHub repository [Ric20]. Some of these methods may also be added into future versions of PARI.

We start with some preliminary algorithms that are key in either the setup or execution of the final intersection number algorithms. There are three distinct approaches to computing the intersection number, and they are explored in Sections 10.3.1, 10.3.2, and 10.3.3. Each has their own advantages depending on the setting.

For consistency, all timings were computed on the “math-jcn4” server at McGill.

10.1 Solving the representation problem for binary quadratic forms

Let $q(x, y) = [A, B, C] = Ax^2 + Bxy + Cy^2$ be a primitive integral binary quadratic form with non-square discriminant, and let n be an integer. The PARI/GP function “qfbsolve” can be used to output all solutions (modulo units) to $q(x, y) = n$ (as of version 2.13; in 2.11 and before, it would only output one solutions and was restricted n to being prime).

More generally, let $q(x, y) = Ax^2 + Bxy + Cy^2 + Dx + Ey$, and consider $q(x, y) = n$. Let

$$d = B^2 - 4AC;$$

$$a = 2CD - BE;$$

$$b = 2AE - BD.$$

If $d \neq 0$, take the substitution

$$x = \frac{X + a}{d}, \quad y = \frac{Y + b}{d}.$$

After scaling, the equation $q(x, y) = n$ transforms to the equation $q'(X', Y') = AX^2 + BXY + CY^2 = n'$, i.e. a homogeneous quadratic form in X, Y . Any integral solution (x, y) corresponds to an integral solution $(X, Y) \equiv (-a, -b) \pmod{d}$. Thus solving $q' = n'$ and transforming the solutions back to (x, y) enables us to find a general form for the solutions to the non-homogeneous quadratic equation $q(x, y) = n$ when $d \neq 0$. If d is a square, then this equation can be solved directly (this case has little use for us).

A small issue that arises is we have to scale things by d^2 , so n' may become quite large. Furthermore, only some solutions translate back to valid integral solutions (x, y) , so there may be some “wasted computations.”

10.2 Computing optimal embeddings

Before computing intersection numbers, we need to initialize a quaternion algebra and Eichler order, and compute optimal embeddings. Setting up the algebra B given the discriminant \mathfrak{D} is classical; for example see Proposition 14.2.7 of [Voi21]. Since most computations are done with a maximal order of a quaternion algebra ramified at exactly two primes, it is useful to set this case up explicitly, to keep the numbers small.

Our algorithm to compute optimal embeddings is essentially brute-force. Before detailing it, we need to determine if two optimal embeddings ϕ_1, ϕ_2 are equivalent or not. From Corollary 4.2.2, the set $C_B(\phi_1, \phi_2) = \{v \in B : v\phi_1 = \phi_2v\}$ is a two-dimensional \mathbb{Q} -vector space. By expanding this out, we can give an explicit matrix M whose kernel generates the set of such v . Intersecting the kernel with O produces a pair v_1, v_2 which generates $C_B(\phi_1, \phi_2) \cap O$.

The linear algebra used to produce v_1, v_2 is already implemented in PARI/GP. The question then becomes: does there exist $x, y \in \mathbb{Z}$ for which $\text{nrd}(xv_1 + yv_2) = 1$? Expanding out this equation produces a binary quadratic form in x, y , and using Section 10.1 we can see if this has a solution or not, i.e. whether the two embeddings are conjugate or not over $O_{N=1}$.

With this in mind, let D be a discriminant, and then Theorem 4.4.5 determines if optimal embeddings into O exist. If they do, then Corollary 4.5.5 counts the total number of equivalence classes when $\gcd(D, \mathfrak{M}) = 1$ (if this does not hold, then see Lemma 30.6.17 of [Voi21] for the correct count of local orientations). It then suffices to generate optimal embeddings, testing if we get new equivalence classes, and repeating until we have one for each equivalence class.

To generate these optimal embeddings, there exists positive integers d_1, d_2, d_3, d_4 for which

$$2O \subseteq \frac{1}{d_1}\mathbb{Z} + \frac{i}{d_2}\mathbb{Z} + \frac{j}{d_3}\mathbb{Z} + \frac{k}{d_4}\mathbb{Z}.$$

By writing $\phi(\sqrt{D}) = Fi/d_2 + Gj/d_3 + Hk/d_3$, we get a three variable quadratic form of signature $(0, 2, 1)$ to be solved for $(F, G, H) \in \mathbb{Z}^3$. Running over the variable with sign -1 (with a bit of optimization due to congruence requirements), we get a sequence of definite binary quadratic forms, which can be solved via Section 10.1. Each potential solution must be checked to make sure it lands in O and is optimal with respect to O .

Remark 10.2.1. The algorithm described is not the most efficient possible, but is fast enough for our purposes. One large issue is every potential new embedding is checked against all previously found embeddings, to determine if it is new or not. For small class numbers this is reasonable, but as the class number grows, this becomes unwieldy.

To improve the algorithm, one can pre-compute the normalizer elements ω_p for $p \mid \mathfrak{DM}_\infty$. After finding the $h^+(D)$ embeddings of a single orientation, the ω_p 's allow us to pass between all orientations.

To find an entire class for a single orientation, we can use the described algorithm to produce one optimal embedding. Using the description of the action of $\text{Cl}^+(D)$ found in Definition 4.5.3, we can boost this up to the entire class. The difficulty with this approach is it requires a solution to the principal ideal problem, i.e. given a left ideal I specified by

generators over \mathbb{Z} , finding an element c_I for which $I = Oc_I$. The algorithm by Page in [Pag14] provides a reasonable solution to this problem.

We provide some sample average running times to compute all optimal embeddings of a single discriminant D into a maximal order in Table 10.1. Implementing the optimizations described in Remark 10.2.1 should significantly decrease the running times when the class number grows.

Table 10.1: Average running times to compute optimal embeddings.

| \mathfrak{D} | D range | Avg time (s) | \mathfrak{D} | D range | Avg time (s) |
|----------------|-------------------|--------------|----------------|-------------------|--------------|
| $2 \cdot 3$ | $[1, 200]$ | 0.002 | $3 \cdot 37$ | $[1, 200]$ | 0.003 |
| $2 \cdot 3$ | $10^3 + [1, 200]$ | 0.005 | $3 \cdot 37$ | $10^3 + [1, 200]$ | 0.007 |
| $2 \cdot 3$ | $10^6 + [1, 200]$ | 0.169 | $3 \cdot 37$ | $10^6 + [1, 200]$ | 1.051 |
| $5 \cdot 11$ | $[1, 200]$ | 0.004 | $7 \cdot 71$ | $[1, 200]$ | 0.007 |
| $5 \cdot 11$ | $10^3 + [1, 200]$ | 0.014 | $7 \cdot 71$ | $10^3 + [1, 200]$ | 0.021 |
| $5 \cdot 11$ | $10^6 + [1, 200]$ | 1.113 | $7 \cdot 71$ | $10^6 + [1, 200]$ | 5.846 |

In all of the above cases, finding a single optimal embedding of the given discriminant was instant (< 1 millisecond). Magma also has algorithms to compute a single optimal embedding, that work in a more general situation. The downside is they are much slower, taking several hundred milliseconds in the simplest of cases, and quickly scaling up.

10.3 Computing the intersection number

Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion algebra of discriminant \mathfrak{D} with Eichler order O of level \mathfrak{M} , generated over \mathbb{Z} by v_1, v_2, v_3, v_4 . Let ϕ_1, ϕ_2 be fixed optimal embeddings of discriminants D_1, D_2 into O . We have three algorithms that can compute the intersection number of ϕ_1 with ϕ_2 , and each has its own advantages and disadvantages. In the following four sections, we describe the algorithms, and give sample running times.

10.3.1 Intersection numbers via intersecting root geodesics

We can turn Proposition 2.4.4 into a reasonable algorithm to compute intersection numbers. Assume that $a > 0$, and fix the inclusion map $\iota : B \rightarrow \text{Mat}(2, \mathbb{R})$ given by

$$\iota : e + fi + gj + hk \rightarrow \begin{pmatrix} e + f\sqrt{a} & b(g + h\sqrt{a}) \\ g - h\sqrt{a} & e - f\sqrt{a} \end{pmatrix}.$$

For $[\phi] \in \text{Emb}(O, D)$, write $\phi(\sqrt{D}) = fi + gj + hk$, with $af^2 + bg^2 - abh^2 = D$. Let ϕ_f, ϕ_s be the first and second roots respectively of $\iota(\phi(\epsilon_D))$, and we can compute them explicitly as

$$\phi_f = \frac{f\sqrt{a} + \sqrt{D}}{g - h\sqrt{a}}, \quad \phi_s = \frac{f\sqrt{a} - \sqrt{D}}{g - h\sqrt{a}},$$

when $g - h\sqrt{a} \neq 0$.

Let $\gamma_2 = \iota(\phi_2(\epsilon_{D_2}))$, assume that neither root of γ_2 is ∞ , and furthermore assume that $\gamma_{2,f} > \gamma_{2,s} > 0$. Pick $r \in \mathbb{R}$ outside of ℓ_{γ_2} , so that $\gamma_{2,s} - r \approx \gamma_{2r} - \gamma_{2,f}$. Pictorially, the situation looks like Figure 10.1.

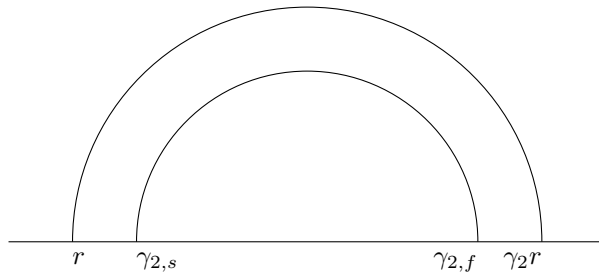


Figure 10.1: Geodesics ℓ_{γ_2} and $\ell_{r, \gamma_{2r}}$.

Proposition 2.4.4 implies that we need to find all conjugates of ϕ_1 so that one root is between $\gamma_{2,s}$ and $\gamma_{2,f}$, and the other is smaller than r or bigger than γ_{2r} (assume for now that no conjugates of ϕ_1 have ∞ as a root). Let σ be a conjugate of ϕ_1 , and write $\sigma(\sqrt{D_1}) = fi + gj + hk$, with $af^2 + bg^2 - abh^2 = D_1$. By negating (f, g, h) , we will assume that $g - h\sqrt{a} > 0$, hence the first root is bigger than the second. If we want the second root to lie underneath ℓ_{γ_2} , we have the equations

$$\gamma_{2,s} < \frac{f\sqrt{a} - \sqrt{D_1}}{g - h\sqrt{a}} < \gamma_{2,f}, \quad \gamma_{2r} < \frac{f\sqrt{a} + \sqrt{D_1}}{g - h\sqrt{a}}. \quad (10.3.1)$$

The equations rearrange to give

$$\sqrt{\frac{D_1}{a}} < f < \sqrt{\frac{D_1}{a} \frac{\gamma_2 r + \gamma_{2,f}}{\gamma_2 r - \gamma_{2,f}}}.$$

As in Section 10.2, write

$$2O \subseteq \frac{1}{d_1}\mathbb{Z} + \frac{i}{d_2}\mathbb{Z} + \frac{j}{d_3}\mathbb{Z} + \frac{k}{d_4}\mathbb{Z},$$

hence $d_2 f \in \mathbb{Z}$. In particular, this gives a finite set of possibilities for f .

By running through a similar argument in all of the cases (the first root lies underneath ℓ_{γ_2} , $\gamma_{2,s} < 0$, either ϕ_2 or σ has an infinite root, etc.), we can always produce an explicit finite set of possibilities for f . Using $(g, h) = (G/d_3, H/d_4)$ and $af^2 + bg^2 - abh^2 = D_1$, each possible f produces an indefinite binary quadratic form in G, H to be solved for $G, H \in \mathbb{Z}$. By writing the root geodesic of σ in terms of a general solution and considering Equation 10.3.1 (or the corresponding variant), we again get a finite explicit set of possibilities.

By checking which of these embeddings did land in and were optimal with respect to O , we in fact get all intersections of ϕ_1 with an optimal embedding of discriminant D_2 . By taking only those embeddings that are conjugate to ϕ_2 , we at last get the intersection number of ϕ_1, ϕ_2 .

In the computation given, the range of possible f 's is inversely proportional to $\gamma_2 r - \gamma_{2,f}$. Similarly, in other cases we get the range is inversely proportional to $\gamma_{2,s} - r$, and this is why we choose r so that these numbers are approximately equal: we want to minimize case checking.

In the case that D_2 has an extremely large fundamental unit, $\gamma_2^n r$ will converge to the roots extremely fast as $n \rightarrow \pm\infty$. In these cases, the ranges for f will be quite large, and the algorithm will be significantly worse. Thus it is worth swapping ϕ_1, ϕ_2 if the fundamental unit for D_1 is smaller. For example, in the case of $\mathfrak{D} = 7 \cdot 71$, we can optimally embed discriminants 13, 97 via ϕ_1, ϕ_2 respectively. Since

$$\epsilon_{13} = \frac{11 + 3\sqrt{13}}{2}, \quad \epsilon_{97} = \frac{125619266 + 12754704\sqrt{97}}{2},$$

the computation should be faster when ϕ_2 comes first. Indeed, writing $f = F/d_2$, when 97 comes first we end up with two ranges for F being $[-3, 9]$ and $[-9, 3]$ (coming from the two setups of one root being bigger than $\gamma_2 r$ or one root being smaller than r), and thus there

are 26 possibilities total for F . The resulting computation takes 0ms, i.e. is instant. When discriminant 13 comes first, the ranges of F are $[0, 134688040]$ and $[-77647273, 0]$, and the resulting computation takes just over 14 minutes.

10.3.2 Intersection numbers via x -linking

Any intersection pair must exhibit x -linking for $|x| < \sqrt{D_1 D_2}$. Since

$$x^2 \equiv D_1 D_2 \pmod{4\mathfrak{O}\mathfrak{M}},$$

we can compute the square roots of $D_1 D_2$ modulo $4\mathfrak{O}\mathfrak{M}$, find all such x with $|x| < \sqrt{D_1 D_2}$, and compute the corresponding Hilbert symbols for prime divisors of $\frac{D_1 D_2 - x^2}{4}$ to determine if $\text{Emb}(O, D_1, D_2, x)$ is non-empty (we are using Theorem 7.1.2). If D_1, D_2 are not coprime, then for those x with (D_1, D_2, x) not nice we instead use Theorem 6.4.2 to determine if $\text{Emb}(B, D_1, D_2, x)$ is non-empty. This may overcount and we get some x 's for which $\text{Emb}(O, D_1, D_2, x)$ is empty, but this set will be relatively small.

For each such x , we would like to find all embeddings ϕ' of \mathcal{O}_{D_2} which exhibits x -linking with ϕ_1 . Write

$$\phi' \left(\frac{p_{D_2} + \sqrt{D_2}}{2} \right) = a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4,$$

where $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. The following equations must be satisfied:

$$\text{nrd}(a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4) = \frac{p_{D_2} - D_2}{4};$$

$$\text{trd}(a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4) = p_{D_2};$$

$$\text{trd} \left(\phi_1(\sqrt{D_1})(-1 + 2a_1 v_1 + 2a_2 v_2 + 2a_3 v_3 + 2a_4 v_4) \right) = 2x.$$

The second and third lines are linear equations in the a_i , and the first line is a quadratic. By solving the second and third lines and substituting this into the first equation, we get a two variable quadratic form, which must be indefinite. Solving the form using Section 10.1 will produce a finite set of families of solutions. Now, since we are looking for x -linked pairs (ϕ_1, ϕ') up to simultaneous conjugation, the embedding ϕ' will only be defined up to conjugation by $\phi_1(\epsilon_{D_1})$. This will reduce each family to a finite set of non-simultaneously conjugate embeddings (often one), and the intersection number follows.

10.3.3 Intersection numbers via fundamental domains

In [Voi09], algorithms are given to compute the fundamental domain D of a general Fuchsian group. In particular, the algorithms can be applied to generate the fundamental domain of X_O , for O an Eichler order of B . Given an optimal embedding ϕ , we can pick a point on its upper half plane root geodesic, and translate it to the fundamental domain. By following the path of the geodesic and applying the appropriate transformation (via the side pairing) at each edge of D , we can trace out the path of the geodesic in D .

This decomposes the geodesic into r segments, each a geodesic between two sides of D . Given another geodesic that decomposes into s parts, computing the intersections of the two sets is very easy, as it suffices to see if each of the rs pairs intersects (if they intersect, they will intersect precisely once).

For example, let $B = \left(\frac{55, -3}{\mathbb{Q}}\right)$ be ramified at 5, 11, let O be the maximal order given by $\langle 1, i, \frac{1+j}{2}, \frac{3+3i+j+k}{6} \rangle_{\mathbb{Z}}$. Let $D_1 = 2013$ and $D_2 = 2020$, and take

$$\phi_1 \left(\frac{1 + \sqrt{2013}}{2} \right) = \frac{3 + 12i + 11j + 8k}{6}, \quad \phi_2 \left(\frac{\sqrt{2020}}{2} \right) = \frac{12i + 50j + 5k}{3}.$$

We compute the fundamental domain and the images of the root geodesics of ϕ_i in the fundamental domain, and obtain Figure 10.2, which is generated using Matplotlib ([Hun07]). We are working in the unit disc model, where the border of the fundamental domain is in green, the root geodesic of ϕ_1 is in red, and the root geodesic of ϕ_2 is in blue. In particular, there are two intersections, so the unweighted intersection number is 2.

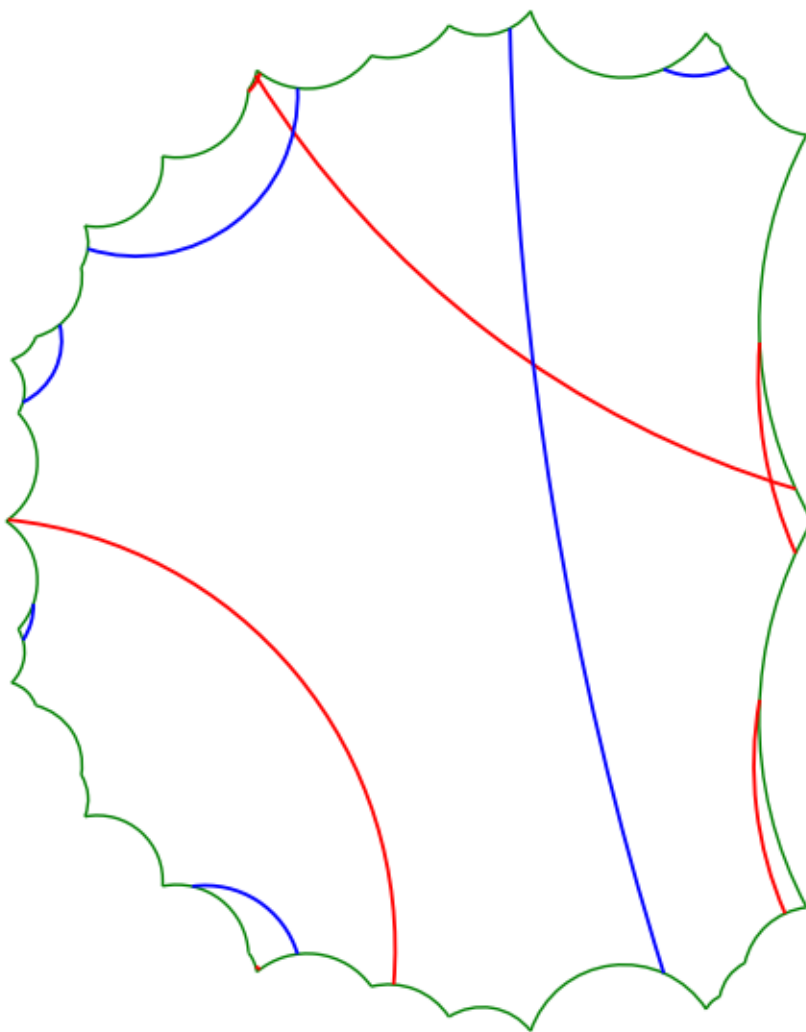


Figure 10.2: Root geodesics of ϕ_1, ϕ_2 in the fundamental domain.

The extra difficulty with this approach is the computation of the fundamental domain. The aforementioned algorithm of Voight is implemented in Magma, and I have implemented this algorithm in PARI. Improvements in my implementation (compared to Magma) include:

- Computation of an exterior domain in $O(n \log(n))$ time instead of $O(n^2)$ (n is the number of circles);
- Reduction of elements to a given exterior domain with each step in $O(\log(n))$ time instead of $O(n)$ (n is the number of boundary arcs);
- Adapting the (probabilistic) enumeration of elements by Aurel Page in [Pag15] to the

Shimura curve case.

Table 10.2 gives sample running times in six examples. The Magma computation for the ramified at 101, 103 case was left running for 2 weeks, and did not terminate.

Table 10.2: Running times for the computation of the fundamental domain.

| Ramification | Sides | t(Magma) (s) | t(PARI) (s) |
|--------------|-------|--------------|-------------|
| 2, 11 | 12 | 2.430 | 0.030 |
| 2, 101 | 104 | 87.220 | 0.147 |
| 11, 13 | 114 | 170.220 | 0.175 |
| 3, 37 | 72 | 102.830 | 0.401 |
| 23, 29 | 568 | 6186.9 | 1.725 |
| 101, 103 | 10172 | >2 weeks | 40.797 |

10.3.4 Running times

The root geodesic approach of Section 10.3.1 is generally good, as long as one of the fundamental units is reasonably small. If both fundamental units are large, then the running time can blow up.

For a varied quaternion algebra, the x -linking algorithm of Section 10.3.2 is reasonable; it does not suffer any effects from unusually large fundamental units. Furthermore, it can determine x -linking for $|x| > \sqrt{D_1 D_2}$, if that is desired. A downside is it often produces intersection pairs with large numbers, i.e. it does not do a great job of finding “reduced” intersection pairs.

In general, if a fundamental domain has been pre-computed, then computing intersection numbers with it is typically the best. Computing the geodesics is a straightforward process, and the resulting intersection number follows. This also produces intersection pairs with small coefficients, since we have reduced the intersection points. It can be slightly slower in some small examples, but it is the most consistent method, and scales (with unweighted intersection number) the best.

For illustration, in Table 10.3 we computed intersection numbers of a fixed pair of optimal embeddings of discriminants D_1, D_2 into a maximal order of the quaternion algebra ramified at \mathfrak{D} with the three different methods, and recorded the computation times. We also record the positive regulators $R^+(D) = \log(\epsilon_D)$ to three decimal places, and the unweighted intersection number.

The expressions $T(\text{RG})$, $T(x-)$, and $T(\text{FD})$ refer to the times in seconds used to compute the intersection number with the root geodesic method, x -linking method, and the fundamental domain method (with pre-computed domain), respectively. Note that we are using the optimization of swapping D_1, D_2 so that $\epsilon_{D_2} < \epsilon_{D_1}$ in the root geodesic approach.

Table 10.3: Running times for the three intersection number algorithms.

| \mathfrak{D} | (D_1, D_2) | $(R^+(D_1), R^+(D_2))$ | $ \text{Int}^+(\phi_1, \phi_2) $ | $T(\text{RG})$ | $T(x-)$ | $T(\text{FD})$ |
|----------------|---------------|------------------------|----------------------------------|----------------|---------|----------------|
| $2 \cdot 3$ | (5, 141) | (0.962, 5.247) | 6 | 0.0016 | 0.0044 | 0.0025 |
| $2 \cdot 3$ | (236, 10013) | (6.966, 11.683) | 98 | 3.277 | 0.328 | 0.020 |
| $3 \cdot 17$ | (12, 10001) | (1.317, 10.597) | 1 | 0.0045 | 0.0096 | 0.0026 |
| $3 \cdot 17$ | (1013, 10001) | (13.655, 10.597) | 14 | 3.825 | 0.161 | 0.008 |
| $11 \cdot 23$ | (21, 20009) | (1.567, 55.255) | 2 | 0.069 | 0.003 | 0.007 |
| $11 \cdot 23$ | (2020, 2021) | (7.389, 3.806) | 1 | 0.013 | 0.013 | 0.002 |

Chapter 11

Future research

There are quite a few directions to take intersection numbers. I will give a brief overview of various directions, separated into sections.

11.1 A more general topograph

In Section 3.4.5, we started with a primitive indefinite binary quadratic form equivalence class, computed the river of its topograph, and computed the intersection number with another form via a combinatorial formula. This is very similar to what we do in Section 10.3.3, i.e. computing intersection numbers via the fundamental domain. However, there are a few key differences:

- Given a word coming from the generating set of $O_{N=1}^\times$, it is not obvious if it generates a hyperbolic element or not;
- We must draw the physical geodesics in the fundamental domain to determine the intersections, whereas this is not necessary for the topograph.

There are certain times when we can be sure that two geodesic pieces intersect/don't intersect, but if two geodesics intersect the same side of fundamental domain it is not clear unless we actually draw them.

It is worth investigating whether we can modify the fundamental domain approach into being more topograph-like, i.e. describing an analogue of the Conway topograph for Shimura

curves.

11.2 More modularity

Chapter 8 was dedicated to proving that E_{ϕ_1, ϕ_2}^{\pm} was a modular form. What about E_{ϕ_1, ϕ_2} and E_{ϕ_1, ϕ_2}^q for primes q ? As long as $q \mid \mathfrak{DM}$, the Hecke operator is self-adjoint with respect to the q -weighted intersection number, which is a key fact. Even when $q \nmid \mathfrak{DM}$, the only prime Hecke operator which this will fail at is T_q , so there may be a natural modification of the q -weighting or T_q in this case to make the Hecke operator self-adjoint.

While these series do not appear to be modular forms of weight 2 on $\Gamma_0(\mathfrak{DM}\mathfrak{M}')$, it is reasonable to expect that they are a related concept, for instance mock modular forms.

11.3 Distribution questions

In this section we describe various distribution questions. We will mostly focus on the case of $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$, as this is where we have been able to compute the most data.

11.3.1 Distribution of intersection points and angles

Given a pair of PIBQFs q_1, q_2 , lifting the intersection points to \mathbb{H} gives a set of size $\mathrm{Int}(q_1, q_2)$ of $\mathrm{PSL}(2, \mathbb{Z})$ equivalence classes of CM points. The points all have discriminants being a square divisor of a number of the form $x^2 - D_1 D_2$, but what more can be said about them? In [Duk88], Duke considers the images on the modular curve of Heegner points and modular geodesics coming from fundamental discriminants D . With reference to convex regions with piece-wise smooth boundary, he proves that the Heegner points are equidistributed as $D \rightarrow -\infty$, and the modular geodesics are equidistributed as $D \rightarrow \infty$. We would like to formulate similar results for the case of intersecting modular geodesics.

Fix q_1, q_2 , let $z \in \ell_{q_1}$, and let $\ell = \ell_{z, \gamma_{q_1} z}$. The intersection points of $\tilde{\ell}_{q_1}$ with $\tilde{\ell}_{q_2}$ lift uniquely to ℓ , so we can study the distribution of intersections on $\tilde{\ell}_{q_1}$ by lifting to ℓ .

A natural guess would be to say that the intersection points become uniformly distributed on ℓ as $\mathrm{disc}(q_2) \rightarrow \infty$, and this appears to be true in many examples. However, Example 3.6.2

gives a family $q_n = [1, n, -1]$ for which $\text{disc}(q_n) = n^2 + 4 \rightarrow \infty$ and $\text{Int}([1, 1, -1], q_n) = 8$ for all n , which contradicts this. The next reasonable alternative would be to fix q_1 and take all forms of discriminant D as $D \rightarrow \infty$. For example, let $q_1 = [1, 1, -1]$, let $D = 1000^2 + 4 = 1000004$, and let $z = \frac{-4 + \sqrt{5}i}{3}$ (to optimize the symmetry). We find that $h^+(D) = 52$, there are 1640 intersection points, and they generate Figure 11.1. They seem reasonably well distributed, and the “deficiency” of intersections between q_1 and $[1, 1000, -1]$ has been compensated for.

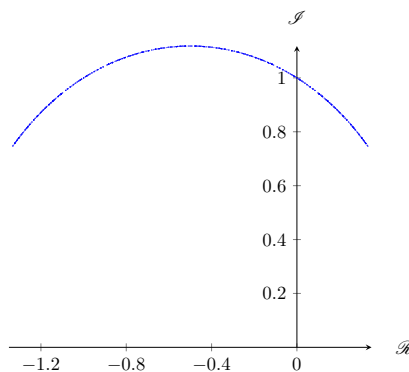


Figure 11.1: Intersection of $[1, 1, -1]$ with discriminant 1000004.

Taking this one step further, let D range between $10^7 + 1$ and $10^7 + 100$ (we take a small range of discriminants to increase the number of data points). There are 507159 intersections points, and we calculate the hyperbolic distance (along $\tilde{\ell}_{q_1}$) between the image of $z = \frac{-4 + \sqrt{5}i}{3}$ and the intersection points. By using 4816 bins of length 0.0004, we generate a histogram in Figure 11.2. The data appears fairly equidistributed, and we formalize this statement in a conjecture.

Conjecture 11.3.1. *Let q be fixed, let D be a positive discriminant, and let $I_q(D)$ denote the set of points on $\tilde{\ell}_q$ that appear as intersections between q and a form of discriminant D . Then the set $I_q(D)$ is equidistributed (with respect to the hyperbolic metric) on $\tilde{\ell}_q$ as $D \rightarrow \infty$.*

A similar topic of study would be the distribution of the intersection angles. We take the domain of arctan to be $[0, \pi)$, and as before, fix $q_1 = [1, 1, -1]$ and let D range between $10^7 + 1$ and $10^7 + 100$. By using 6287 bins of length 0.0005 radians, we generate a histogram in Figure 11.3.

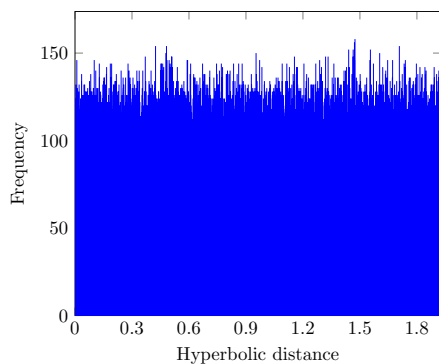


Figure 11.2: 507159 intersection points.

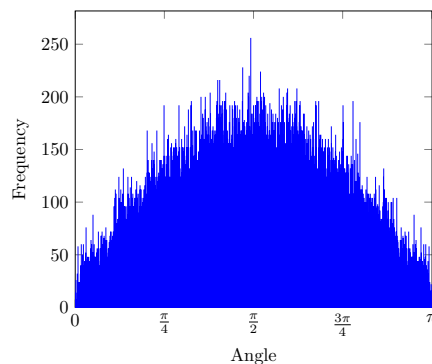


Figure 11.3: 507159 intersection angles.

Small values of B_Δ correspond to angles close to $\frac{\pi}{2}$, and large values correspond to angles close to 0 (if $B_\Delta > 0$) or π (if $B_\Delta < 0$). The histogram indicates that the distribution of the angles is likely not uniform; it is closer to a semi-circle.

The analogous conjectures in the Shimura curve setting are expected to be true as well.

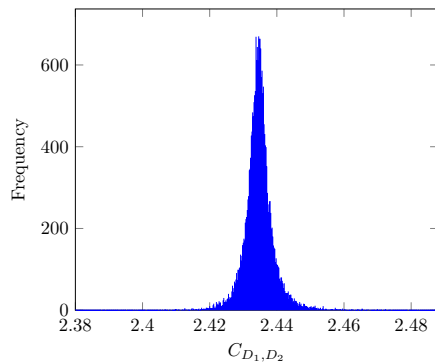
11.3.2 Distribution of the total intersection number

Adapting Corollary 7.1.3 gives us a formula for $\text{Int}(D_1, D_2) = \sum_{[q_i] \in \text{Cl}^+(D_i)} \text{Int}(q_1, q_2)$ when D_1, D_2 are coprime and fundamental, but this formula is still somewhat mysterious. For example, it is not even clear that $\text{Int}(D_1, D_2) \neq 0$!

If D is a discriminant, let $R^+(D) = \log(T+U\sqrt{D})$ denote the positive regulator associated to D (where (T, U) is the smallest solution to $T^2 - DU^2 = 4$). Let

$$C_{D_1, D_2} := \frac{\text{Int}(D_1, D_2)}{h^+(D_1)h^+(D_2)R^+(D_1)R^+(D_2)}$$

be the average intersection of forms of discriminant D_1, D_2 divided by the product of the positive regulators. We took 23000 pairs of distinct discriminants between 5 and 1.6 million, and calculated C_{D_1, D_2} for each pair. By using 541 boxes of length 0.0002, we generate the histogram Figure 11.4.

Figure 11.4: 23000 trials of C_{D_1, D_2} .

It seems that C_{D_1, D_2} is very close to 2.434 most of the time, though it is not clear what the exact relationship is.

In general, let O be an Eichler order in the indefinite quaternion algebra B , and let D_1, D_2 be discriminants for which there exist optimal embeddings of D_i into O . Define C_{D_1, D_2}^O to be the average intersection of the optimal embeddings of discriminants D_1, D_2 into O divided by $R^+(D_1)R^+(D_2)$.

Conjecture 11.3.2. *Let ϕ_1, ϕ_2 be optimal embeddings of discriminants D_1, D_2 . There exists an absolute constant C (that does not depend on D_i or O) for which on average we have*

$$\text{Int}_O(\phi_1, \phi_2) \approx C \frac{R^+(D_1)R^+(D_2)}{\text{Area}(X_O)}.$$

Besides the data in Figure 11.4, we have computed examples for the maximal order in quaternion algebras ramified at 2, 3 and 3, 5, and this data also supports Conjecture 11.3.2.

On a more theoretical level, the corresponding root geodesics have length $2R^+(D_i)$, so it would be reasonable for them to intersect proportionally to this product on average. If the ambient space has a larger area, then it would be “harder” for geodesics to intersect, which is also reflected in the conjecture.

11.4 Towards explicit class field theory for real quadratic fields

In Chapter 9 a conjectural connection was made to the work of Darmon and Vonk on a conjectural analogue of $j(\tau_1) - j(\tau_2)$ for τ_1, τ_2 real quadratic. A recently started project aims to make this connection more concrete by removing the cocycles and replacing them with quaternionic objects. In this section we make some preliminary definitions, and outline the general approach. Most of the original ideas and definitions in this section originated with Darmon and Vonk.

First, we shift from considering intersection numbers to an analogue, which we call the intersection product.

Definition 11.4.1. Let f be a function on pairs of optimal embeddings that is invariant under simultaneous conjugation by O . Let $\Gamma_i = \langle \phi_i(\epsilon_{D_i}) \rangle$ for $i = 1, 2$, and let $\Gamma = O_{N=1}^\times / \{\pm 1\}$. Then the *intersection product* Intprod_O^f is defined by

$$\text{Intprod}_O^f(\phi_1, \phi_2) = \prod_{u \in \Gamma_1 \backslash \Gamma / \Gamma_2} f(\phi_1, \phi_2^u),$$

when this product has finitely many terms. If $f(\phi_1, \phi_2^u) = 1$ whenever ℓ_{ϕ_1} and $\ell_{\phi_2^u}$ do not intersect, then this is satisfied. We will only consider such f 's in this section.

By Proposition 2.4.2, it follows that $\log(\text{Intprod}_O^f(\phi_1, \phi_2)) = \text{Int}_O^{\log(f)}(\phi_1, \phi_2)$, so this is indeed an analogue of the intersection number. The advantage of the intersection product is we can consider functions which we believe will behave well multiplicatively, without having to introduce a logarithm factor.

For optimal embeddings ϕ_1, ϕ_2 , define $\phi_1 \cdot \phi_2$ to be 0 if $\ell_{\phi_1}, \ell_{\phi_2}$ do not intersect, and the sign of the intersection otherwise. Recall Remark 5.1.5, where we noted that the cross ratio of the roots of ϕ_1, ϕ_2 is equal to $\frac{x - \sqrt{D_1 D_2}}{x + \sqrt{D_1 D_2}}$, which is constant across a simultaneous equivalence class, and does not depend on the embedding into $\text{Mat}(2, \mathbb{R})$.

Definition 11.4.2. Denote $\frac{1}{2} \text{trd}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})) = \langle \phi_1, \phi_2 \rangle$. If

$$f(\phi_1, \phi_2) = \begin{cases} (\phi_{1,f}, \phi_{1,s}; \phi_{2,f}, \phi_{2,s}) = \frac{\langle \phi_1, \phi_2 \rangle - \sqrt{D_1 D_2}}{\langle \phi_1, \phi_2 \rangle + \sqrt{D_1 D_2}} & \text{if } \phi_1 \cdot \phi_2 \neq 0; \\ 1 & \text{else,} \end{cases}$$

we call f the modular cross ratio, and denote the intersection product by $\text{Intprod}_O^{\text{MCR}}$. If $g = f^{\phi_1 \cdot \phi_2}$, we call g the signed modular cross ratio, and denote the intersection product by $\text{Intprod}_O^{\text{SMCR}}$.

The modular cross ratio and signed modular cross ratio products will land in $\mathbb{Q}(\sqrt{D_1 D_2})$, and will have norm one since each term has norm one. As such, it is reasonable to separate out the top and bottom halves of the products.

Definition 11.4.3. If

$$f(\phi_1, \phi_2) = \begin{cases} \langle \phi_1, \phi_2 \rangle - \sqrt{D_1 D_2} & \text{if } \phi_1 \cdot \phi_2 = 1; \\ (\langle \phi_1, \phi_2 \rangle + \sqrt{D_1 D_2})^{-1} & \text{if } \phi_1 \cdot \phi_2 = -1; \\ 1 & \text{else,} \end{cases}$$

we call f the half modular cross ratio, and denote the intersection product by $\text{Intprod}_O^{\text{HMCR}}$.

If

$$g(\phi_1, \phi_2) = \begin{cases} \langle \phi_1, \phi_2 \rangle - \sqrt{D_1 D_2} & \text{if } \phi_1 \cdot \phi_2 = 1; \\ (\langle \phi_1, \phi_2 \rangle - \sqrt{D_1 D_2})^{-1} & \text{if } \phi_1 \cdot \phi_2 = -1; \\ 1 & \text{else,} \end{cases}$$

we call g the signed half modular cross ratio, and denote the intersection product by $\text{Intprod}_O^{\text{SHMCR}}$.

For an example of these definitions, take the setup from Example 7.4.1. Specifically, take $Q = \left(\frac{3, -1}{\mathbb{Q}}\right)$ to be the quaternion algebra ramified at 2, 3, let O be the maximal order spanned by $\{1, i, j, \frac{1+i+j+k}{2}\}$, let $D_1 = 5$, and let $D_2 = 381$. Take the optimal embeddings

$$\phi_1 \left(\frac{1 + \sqrt{5}}{2} \right) = \frac{1 - i - j + k}{2}, \quad \phi_2 \left(\frac{1 + \sqrt{381}}{2} \right) = \frac{1 - 11i - 3j + 3k}{2}.$$

We computed that $\text{Int}_O(\phi_1, \phi_2) = 8$, with the 4 positive signed intersections corresponding to $x = -9, -9, 27, 39$, and the 4 negative signed intersections corresponding to $x = 3, 3, -21, -21$. We compute the (signed) (half) modular cross ratio intersection products, and display the results in Table 11.1

Table 11.1: (Signed) (half) modular cross ratio intersection products of ϕ_1, ϕ_2 .

| f | $\text{Intprod}_O^f(\phi_1, \phi_2)$ | Norm |
|-------|--|----------------------------|
| MCR | $\frac{147348057442184993 - 3142496007640631\sqrt{1905}}{53842728626290688}$ | 1 |
| SMCR | $\frac{21273227070540593 - 487376583294887\sqrt{1905}}{210323158696448}$ | 1 |
| HMCR | $\frac{448542959 - 7006009\sqrt{1905}}{743128352}$ | $\frac{4528384}{23222761}$ |
| SHMCR | $\frac{146572679 - 3325153\sqrt{1905}}{46445522}$ | $\frac{4528384}{23222761}$ |

The last two norms factorize as

$$2^8 7^2 19^2 61^{-2} 79^{-2} = \left(\frac{1905 - 3^2}{4}\right)^{-2} \left(\frac{1905 - (-9)^2}{4}\right)^2 \\ \left(\frac{1905 - (-21)^2}{4}\right)^{-2} \left(\frac{1905 - 27^2}{4}\right)^1 \left(\frac{1905 - 39^2}{4}\right)^1.$$

The corresponding formula clearly holds in general. Furthermore, if $p \mid \mathfrak{D}$, then it follows that

$$2 \text{Int}_O^p(\phi_1, \phi_2) = v_p \left(\text{Norm} \left(\text{Intprod}_O^{\text{HMCR}}(\phi_1, \phi_2) \right) \right) + \text{Int}_O^\pm(\phi_1, \phi_2),$$

and the same with the signed half modular cross ratio.

At the moment it is not obvious which of the four defined functions is the most natural, which is why we included the definitions of all of them.

In any case, the above functions only map to $\mathbb{Q}(\sqrt{D_1 D_2})$. To go further, we record a potential generalization the approach of Darmon and Vonk in Chapter 9. Let D_1, D_2 be positive discriminants (for now assume they are coprime and fundamental), and let S be a finite *odd* sized set of primes for which p is inert in \mathcal{O}_{D_i} for all $p \in S$ and $i = 1, 2$. Pick $p \in S$, let B be the quaternion algebra ramified at $S - \{p\}$, let O be a maximal order of B , and let ϕ_1, ϕ_2 be optimal embeddings of discriminants D_1, D_2 into O (which exist from Theorem 4.4.5). Note that ϕ_i induces a map from $\mathcal{O}_{D_i} \left[\frac{1}{p} \right] \rightarrow O \left[\frac{1}{p} \right]$ for $i = 1, 2$. Furthermore, since p is inert with respect to D_i , the group of elements of $\left(O \left[\frac{1}{p} \right] \right)_{N=1}$ that commute with ϕ_i is $\pm \Gamma_i$, where $\Gamma_i = \langle \phi_i(\epsilon_{D_i}) \rangle$. Let $\Gamma = \left(O \left[\frac{1}{p} \right] \right)_{N=1} / \{\pm 1\}$, and if $u \in \Gamma$ has denominator p^k , then ϕ_2^u corresponds to an optimal embedding of discriminant $p^{2k} D_2$, and furthermore

$$\frac{\langle \phi_1, \phi_2^u \rangle - \sqrt{D_1 D_2}}{\langle \phi_1, \phi_2^u \rangle + \sqrt{D_1 D_2}} = \frac{\langle \phi_1, (\phi_2^u)_O \rangle - \sqrt{D_1 p^{2k} D_2}}{\langle \phi_1, (\phi_2^u)_O \rangle + \sqrt{D_1 p^{2k} D_2}}. \quad (11.4.1)$$

If $x = \langle \phi_1, (\phi_2^u)_O \rangle$ is divisible by p , then $p \mid \frac{D_1 D_2 - x^2}{4}$, whence $\text{Emb}(O, D_1, p^{2k} D_2, x)$ is empty by Theorem 7.1.2. Thus $p \nmid x$, and the expression in Equation 11.4.1 is then equivalent to 1 (mod p^k).

Consider the infinite product

$$IP_p^{\text{MCR}}(\phi_1, \phi_2) = \prod_{\substack{u \in \Gamma_1 \backslash \Gamma[\frac{1}{p}]/\Gamma_2 \\ \phi_1 \cdot \phi_2^u \neq 0}} \frac{\langle \phi_1, \phi_2^u \rangle - \sqrt{D_1 D_2}}{\langle \phi_1, \phi_2^u \rangle + \sqrt{D_1 D_2}}, \quad (11.4.2)$$

and the analogous definition for SMCR, HMCR, SHMCR. Arrange the terms of the product by increasing negative p -adic valuation of the denominator of u , and the fact that Equation 11.4.1 is equivalent to 1 (mod p^k) implies that the product converges under this ordering.

By considering the prime power Hecke graph, it can be shown by induction that since p is inert with respect to D_i , then $T_{p^{2k}}[\phi_i]$ is the sum of all optimal embedding classes of even level $\leq 2k$ in $G_O^p(\phi_i)$, and similarly that $T_{p^{2k+1}}[\phi_i]$ is the sum of all optimal embedding classes of odd level $\leq 2k + 1$ in $G_O^p(\phi_i)$ (with all coefficients being 1). In particular, we have proven the following proposition.

Proposition 11.4.4. *With $f \in \{\text{MCR}, \text{SMCR}, \text{HMCR}, \text{SHMCR}\}$, we have*

$$IP_p^f(\phi_1, \phi_2) = \lim_{k \rightarrow \infty} \text{Intprod}_O^f(\phi_1, T_{p^k} \phi_2) \text{Intprod}_O^f(\phi_1, T_{p^{k+1}} \phi_2).$$

The analogue of Conjecture 9.0.1 is as follows.

Conjecture 11.4.5. *Let T be a Hecke operator that kills $S_2(\Gamma_0(\mathfrak{D})^{\text{new}})$. Then for some $f \in \{\text{MCR}, \text{SMCR}, \text{HMCR}, \text{SHMCR}\}$, the value of $IP_p^f([\phi_1], T[\phi_2])$ is algebraic over \mathbb{Q} , belonging to the composition of the Hilbert class fields associated to D_1, D_2 . Furthermore, it is essentially independent of which prime $p \in S$ was chosen.*

In Conjecture 11.4.5 we have to pass between optimal embeddings of different quaternion algebras, and it is not immediately clear on how we should do this. While we have yet to attempt computations of IP_p^f , the motivation for the conjecture is it is a generalization of the setup in Chapter 9, where S consisted of a singular prime. The justification for the Hecke operator T is that is what is required to generalize Chapter 9 from genus 0 primes to all primes, noting that $T = 1$ is a valid choice when there are no cusp forms on $\Gamma_0(p)$.

Appendix A

Extra proofs

This appendix is devoted to various results and proofs that do not fit into the main text well. This includes proofs that are too long, too messy, or for the prime $p = 2$ (the proof is often similar in style to p odd, but with subtle modifications).

A.1 Pell's equation over p-adics

Proposition A.1.1. *Let p be a prime, A a non-zero integer, and D a non-zero integer. Let $e = v_p(A)$, let $f = v_p(D)$, let k be the largest non-negative integer such that $2k \leq e, f$, let $(e', f', A', D') = (e - 2k, f - 2k, A/p^{2k}, D/p^{2k})$, and let A'' be the unique positive integer so that A'/A'' is a power of 4 and $4 \nmid A''$. The existence of $X, Y \in \mathbb{Z}_p$ that satisfy the equation*

$$X^2 - DY^2 = A$$

is characterized in Tables A.1 and A.2.

| f' | e' | Conditions | Solutions |
|----------|------|--|-----------|
| 0 | - | $\left(\frac{D'}{p}\right) = 1$ | Yes |
| | even | $\left(\frac{D'}{p}\right) = -1$ | Yes |
| | odd | $\left(\frac{D'}{p}\right) = -1$ | No |
| 1 | even | $\left(\frac{A'/p^{e'}}{p}\right) = 1$ | Yes |
| | | $\left(\frac{A'/p^{e'}}{p}\right) = -1$ | No |
| | odd | $\left(\frac{-A'/(p^{e'-1}D')}{p}\right) = 1$ | Yes |
| | | $\left(\frac{-A'/(p^{e'-1}D')}{p}\right) = -1$ | No |
| ≥ 2 | 0 | $\left(\frac{A'}{p}\right) = 1$ | Yes |
| | | $\left(\frac{A'}{p}\right) = -1$ | No |
| | 1 | - | No |

 Table A.1: Solutions for p odd.

| f' | e' | D' conditions | A'' conditions | Solutions |
|----------|-----------|-----------------|-----------------------------|--------------|
| 0 | $\neq 1$ | 1 (mod 8) | - | Yes |
| | $= 1$ | | - | No |
| | - | 3 (mod 8) | 1, 5, 6 (mod 8) | Yes |
| | | | 2, 3, 7 (mod 8) | No |
| | even | 5 (mod 8) | - | Yes |
| | odd | | - | No |
| - | 7 (mod 8) | 1, 2, 5 (mod 8) | Yes | |
| | | 3, 6, 7 (mod 8) | No | |
| 1 | ≥ 1 | - | $-D', 4 - D' \pmod{16}$ | Yes |
| | | | $8 - D', 12 - D' \pmod{16}$ | No |
| | 0 | 2 (mod 8) | 1, 7 (mod 8) | Yes |
| | | | 3, 5 (mod 8) | No |
| | | | 6 (mod 8) | Yes |
| | | | | 5, 7 (mod 8) |
| ≥ 2 | 1 | - | - | No |
| 2 | 0 | - | 1 (mod 4) | Yes |
| | | | 3 (mod 4) | No |
| ≥ 3 | 0 | - | 1 (mod 8) | Yes |
| | | | 3, 5, 7 (mod 8) | No |

 Table A.2: Solutions for $p = 2$.

Proof. Looking modulo p^{2k} shows that $p^{2k} \mid X^2$, hence we can write $X = p^k X_1$ where $X_1 \in \mathbb{Z}_p$. Thus we reduce to solving

$$X_1^2 - D'Y^2 = A',$$

and $\min(e', f') \leq 1$. Start with the case of $p > 2$.

- If $f' = 0$, then $\left(\frac{D'}{p}\right) = \pm 1$.

– Say $\left(\frac{D'}{p}\right) = 1$.

If $A' \equiv 0 \pmod{p}$, then there exists a solution to this equation modulo p with $Y = 1$, which can be lifted to \mathbb{Z}_p via Hensel's lemma (and then $p \nmid Y$). Otherwise, assume the equation has no solution modulo p . The term $D'Y^2$ ranges over all quadratic residues (QR) modulo p , so we have a QR plus A' is a quadratic non-residue (QNR). There are $\frac{p+1}{2}$ QR modulo p (counting 0), and $\frac{p-1}{2}$ QNR modulo p , so two distinct QR must be sent to the same QNR when we add $A' \pmod{p}$, contradiction. Therefore there is a solution modulo p , and it is automatic that

$(X, Y) \not\equiv (0, 0) \pmod{p}$ as $p \nmid A'$. Thus by Hensel's lemma it lifts to \mathbb{Z}_p , and we also have $p \nmid \gcd(X_1, Y)$.

– Say $\left(\frac{D'}{p}\right) = -1$.

If $e' > 0$, then $X_1^2 \equiv D'Y^2 \pmod{p}$, whence $p \mid X_1, Y$. By repeating this argument, the power of p dividing $X_1^2 - D'Y^2$ must be even, whence if e' is odd there is no solution. If e' is even, then the above argument shows that we can scale the equation by $p^{e'}$, so that $p \nmid A'$. By Hensel's lemma, it suffices to consider the equation modulo p . Since $D'Y^2$ will range over all QNR modulo p , if there are no solutions then we must have a QNR plus A' remains a QNR. But $p \nmid A'$, so applying this p times it will imply that every residue modulo p is a QNR, contradiction. Thus there is a solution in this case.

• If $f' = 1$, then $X_1^2 \equiv A' \pmod{p}$.

– If $e' = 0$, then if $\left(\frac{A'}{p}\right) = -1$ there are no solutions. Otherwise, this equivalence has a solution, which lifts to \mathbb{Z}_p by Hensel's lemma, and thus gives a solution with $Y = 0$.

– If $e' = 1$, then $p \mid X_1$. Dividing by p and looking modulo p , we have $-D'/pY^2 \equiv A'/p \pmod{p}$, and so $Y^2 \equiv -A'/D' \pmod{p}$. If $\left(\frac{-A'/D'}{p}\right) = -1$ there are no solutions, and otherwise a solution to the equivalence lifts to \mathbb{Z}_p by Hensel's lemma, which gives a solution with $X' = 0$.

– If $e' \geq 2$, then by looking modulo p, p^2 we have $p \mid X_1, Y$. Dividing through by p^2 replaces (A', D') by $(A'/p^2, D')$, and so we repeat until we are in the case of $e' = 0, 1$.

• If $f' \geq 2$, then $X_1^2 \equiv A' \pmod{p}$.

– If $e' = 0$, then this follows exactly as the case of $(f', e') = (1, 0)$.

– If $e' = 1$, then $p \mid X_1$, but then $p \mid X_1^2 - D'Y^2 = A'$, contradiction. Thus there are no solutions.

If $p = 2$, we are solving $X_1^2 - D'Y^2 = A'$ in \mathbb{Z}_2 . We can assume that $2 \nmid \gcd(X_1, Y)$, and scale the possible A' 's by powers of 4 at the end. Since squares in \mathbb{Z}_2 are of the form $4^w(1 + 8w')$, the possible values of $(X_1^2, Y^2) \pmod{8}$ are $(1, 0), (1, 1), (1, 4), (0, 1), (4, 1)$. This gives us 5 residue classes modulo 8 for $X_1^2 - D'Y^2 = A'$. In the first three, we do get a lift to \mathbb{Z}_2 since there is a value of Y making $D'Y^2 + A' \equiv 1 \pmod{8}$, which is a square. In the last two cases, if D' is odd then the same holds, so this is an equivalent condition. If D' is even, then equivalently we are solving for an X_1 so that $\frac{X_1^2 - A'}{D'} \equiv 1 \pmod{8}$, which is equivalent to $X_1^2 \equiv A' + D' \pmod{2^{3+f'}}$, so we get equivalences modulo $2^{3+f'}$ instead.

- If $f' = 0$, by the above it suffices to calculate the 5 residue classes.
 - If $D' \equiv 1 \pmod{8}$, we get $X_1^2 - D'Y^2 \equiv 0, 1, 3, 5, 7 \pmod{8}$. Scaling this by powers of 4, we see that all A' are valid except for $e' = 1$.
 - If $D' \equiv 3 \pmod{8}$, we get $X_1^2 - D'Y^2 \equiv 1, 5, 6 \pmod{8}$.
 - If $D' \equiv 5 \pmod{8}$, we get $X_1^2 - D'Y^2 \equiv 1, 3, 4, 5, 7 \pmod{8}$. Scaling by powers of 4, this is equivalent to e' is even.
 - If $D' \equiv 7 \pmod{8}$, we get $X_1^2 - D'Y^2 \equiv 1, 2, 5 \pmod{8}$.
- If $f' = 1$,
 - If $e' \geq 1$, then X_1 is necessarily even, landing us in the Y odd case by our assumption. Since $f' = 1$ and the even squares modulo 16 are 0, 4, we get the result.
 - If $e' = 0$, then X_1 must be odd, landing us in the first three residue classes. If $D' \equiv 2 \pmod{8}$, we get $A' \equiv 1, 7 \pmod{8}$, and if $D' \equiv 6 \pmod{8}$, then $A' \equiv 1, 3 \pmod{8}$.
- If $f' \geq 2$, then $A' \equiv X_1^2 \pmod{4}$.
 - If $e' = 1$, then $X_1^2 \equiv A' \equiv 2 \pmod{4}$, contradiction.
 - If $e' = 0$ and $f' = 2$, then $A' \equiv 1 \pmod{4}$ is necessary. Given such an A' , one of $Y = 0, 1$ make $A' + D'Y^2$ equivalent to 1 $\pmod{8}$, and so an X_1 exists.

- If $e' = 0$ and $f' \geq 3$, then $X_1^2 \equiv A' \pmod{8}$. In this case, $A' \equiv 1 \pmod{8}$ is both necessary and sufficient.

□

A.2 Proofs for the prime 2

Proposition A.2.1. *Let D be a discriminant, let $B = \text{Mat}(2, \mathbb{Q}_2)$, and let O be an Eichler order of level 2^e . Then there exists an embedding of \mathcal{O}_D into O if and only if any of the following are satisfied:*

- $\left(\frac{D^{\text{fund}}}{2}\right) = 1$;
- $e \leq v_2\left(\frac{D}{4}\right)$;
- $e = v_2\left(\frac{D}{4}\right) + 1$ and $v_2(D)$ is even;
- $e = v_2\left(\frac{D}{4}\right) + 2$ and D^{fund} is odd.

Furthermore, if there exists an embedding, then there exists an optimal embedding.

Proof. Continue as the p odd case, where we have $e > 0$ ($e = 0$ hits the second bullet if D is even and the fourth if D is odd). An embedding is given by $\phi\left(\frac{p_D + \sqrt{D}}{2}\right) = \begin{pmatrix} a & b \\ 2^e c & p_D - a \end{pmatrix}$, for any $a, b, c \in \mathbb{Z}_2$ which satisfy $a^2 - p_D a + bc2^e = \frac{D - p_D}{4}$. The embedding is optimal if and only if either D is odd or D is even and $2 \nmid \gcd(a - D/4, b, c)$. If such an embedding exists, then replacing (a, b, c) by $(a, bc, 1)$ will thus give an optimal embedding, which is the last claim. Such a triple will exist if and only if there exists an $a \in \mathbb{Z}_2$ for which $2^e \mid \frac{D - p_D}{4} + p_D a - a^2$, which translates to

$$2^{e+2} \mid D - (2a - p_D)^2.$$

If D is odd, then $(2a - p_D)^2 \equiv 1 \pmod{8}$, whence $D \equiv 1 \pmod{8}$ necessarily. If $D \equiv 1 \pmod{8}$, then it is a quadratic residue modulo all powers of two, hence we have a valid solution. Note that this satisfies the first bullet, and $D \equiv 5 \pmod{8}$ will not satisfy any of the bullet points.

Finally, we consider when D is even. We get $2^e \mid \frac{D}{4} - a^2$, so write $D = 2^{2+2s+\epsilon}d$, with d odd, s non-negative, and $\epsilon = 0, 1$. If $e \leq 2s + \epsilon = v_2\left(\frac{D}{4}\right)$ we will have a solution, so assume otherwise. We must have $a = 2^s a'$, and we get the equation $2^{e-2s} \mid 2^\epsilon d - a'^2$.

- If $\epsilon = 1$, then $e - 2s \geq \epsilon + 1 = 2$, whence $4 \mid 2d - a'^2$, which is a contradiction since $v_2(2d - a'^2) \leq 1$. All four bullet points fail in this case.
- If $\epsilon = 0$, we have the equation $2^{e-2s} \mid d - a'^2$, i.e. d is a quadratic residue modulo 2^{e-2s} . This is true if and only if $d \equiv 1 \pmod{2^{\min(e-2s, 3)}}$. When $e - 2s = 1, 2$ we get the third and fourth bullets, and if $e - 2s \geq 3$ we get the first bullet.

□

Proposition A.2.2. *Let ϕ_1, ϕ_2 be optimal embeddings into O of discriminants D_1, D_2 , such that $2 \nmid \gcd(D_1, D_2)$ and $2 \mid \mathfrak{D}$. Let N be the largest nonnegative integer such that the images of \mathcal{O}_{D_i} in $\frac{O}{2^N O}$ are equal. Then we have $v_2(\ell(\phi_1, \phi_2)) = N$.*

Proof. Without loss of generality, assume that D_2 is odd. As in Proposition 5.2.3, we work in the completion $\frac{O_2}{2^n O_2}$. The images of $\phi_i(\mathcal{O}_{D_i})$ in $\frac{O_2}{2^n O_2}$ are the same if and only if there exists $a, b \in \mathbb{Z}_2$ with b odd for which

$$\frac{p_{D_1} + \phi_1(\sqrt{D_1})}{2} \equiv a + b \frac{1 + \phi_2(\sqrt{D_2})}{2} \pmod{2^n O_2}. \quad (\text{A.2.1})$$

Multiplying by 2 and rearranging, this is equivalent to

$$\phi_1(\sqrt{D_1}) - b\phi_2(\sqrt{D_2}) \equiv 2a + b - p_{D_1} \pmod{2^{n+1} O_2}, \quad (\text{A.2.2})$$

for some integers a, b with b odd.

Assuming Equation A.2.2, taking traces implies that $0 \equiv 2(2a + b - p_{D_1}) \pmod{2^{n+1} O_2}$, hence $2^n \mid 2a + b - p_{D_1}$. Let $2a + b - p_{D_1} = 2^n A$ for $A \in \mathbb{Z}_2$, and multiplying by $\phi_2(\sqrt{D_2})/2^n$ on the right implies that

$$\frac{\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) - bD_2}{2^n} \equiv A\phi_2(\sqrt{D_2}) \equiv A \pmod{2O_2}.$$

In particular,

$$\frac{A + (x - bD_2)/2^n + \phi_1 \times \phi_2(\sqrt{(x^2 - D_1 D_2)/2^{2n}})}{2} \in O_2,$$

which implies that $\phi_1 \times \phi_2$ descends to an embedding of discriminant $\sqrt{(x^2 - D_1 D_2)/2^{2n}}$. In particular, $v_2(\ell(\phi_1, \phi_2)) \geq N$.

Next, consider the case when D_1 is even: in this case we claim that $v_2(\ell(\phi_1, \phi_2)) = N = 0$. Assume that $v_2(\ell(\phi_1, \phi_2)) > 0$; we seek a contradiction. This is equivalent to $\phi_1 \times \phi_2$ descending to an embedding of $\frac{x^2 - D_1 D_2}{4}$, which implies that this is a discriminant. By Theorem 4.4.5, we have $\frac{D_1}{4}$ is not a discriminant and $\left(\frac{D_2}{2}\right) = -1$, whence $D_1 \equiv 8, 12 \pmod{16}$ and $D_2 \equiv 5 \pmod{8}$. If $D_1 \equiv 8 \pmod{16}$, then

$$\frac{x^2 - D_1 D_2}{4} \equiv (x/2)^2 - 2 \equiv 2, 3 \pmod{4},$$

whence $\frac{x^2 - D_1 D_2}{4}$ is not a discriminant, contradiction. Therefore we can assume that $D_1 \equiv 12 \pmod{16}$. Then,

$$\frac{x^2 - D_1 D_2}{4} \equiv (x/2)^2 - 3 \equiv 1, 2 \pmod{4},$$

so the only valid case is $4 \mid x$. Since $\frac{x^2 - D_1 D_2}{4}$ is then odd, we have an embedding if and only if

$$O_2 \supseteq \phi_1 \times \phi_2 \left(\frac{1 + \sqrt{(x^2 - D_1 D_2)/4}}{2} \right) = \frac{2 - x + \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2})}{4}.$$

In particular, $\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) \equiv 2 \pmod{4O_2}$, and this rearranges to

$$D_2 \phi_1(\sqrt{D_1/4}) \equiv \phi_2(\sqrt{D_2}) \pmod{2O_2}.$$

Squaring gives

$$\frac{D_2^2 D_1}{4} \equiv D_2 \pmod{4O_2},$$

which implies that $\frac{D_1 D_2}{4} \equiv 1 \pmod{4}$, a contradiction. Therefore $v_2(\ell(\phi_1, \phi_2)) = 0$, as desired.

All that remains to show is the inequality $v_2(\ell(\phi_1, \phi_2)) \leq N$ when D_1 and D_2 are odd. We can assume that $v_2(\ell(\phi_1, \phi_2)) = n \geq 1$ (we would be done if $n = 0$ by the opposite inequality). In particular, we have $u \in \{0, 1\}$ for which

$$\frac{u + \phi_1 \times \phi_2(\sqrt{(x^2 - D_1 D_2)/2^{2n}})}{2} \in O_2.$$

Multiplying by 2^{n+1} gives

$$2^n u - x + \phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}) \in 2^{n+1} O_2.$$

Using the fact that $\phi_2(\sqrt{D_2}) \equiv 1 \pmod{2O_2}$, multiplying by $\phi_2(\sqrt{D_2})/D_2$ on the right and rearranging gives

$$\begin{aligned} \frac{1 + \phi_1(\sqrt{D_1})}{2} &\equiv \frac{1 + (x - 2^n u)/D_2 \phi_2(\sqrt{D_2})}{2} \pmod{2^n O_2} \\ &\equiv \frac{D_2 + 2^n u - x}{2D_2} + \frac{x - 2^n u}{D_2} \frac{1 + \phi_2(\sqrt{D_2})}{2} \pmod{2^n O_2}. \end{aligned}$$

Since $x \equiv p_{D_1} p_{D_2} \equiv 1 \pmod{2}$ and $n \geq 1$, we have $(x - 2^n u)/D_2 \in \mathbb{Z}_2^\times$, as well as $\frac{D_2 + 2^n u - x}{2D_2} \in \mathbb{Z}_2$. By Equation A.2.1, the images are the same modulo 2^n , and thus $N \geq n$ as required. \square

Proposition A.2.3. *Write $\epsilon_D = \frac{T+U\sqrt{D}}{2}$, where D is a positive discriminant. Let e_i be defined by*

$$\epsilon_{2^{2i}D} = \epsilon_{2^{2i-2}D}^{e_i},$$

write $\epsilon_D^i = \frac{T_i + U_i \sqrt{D}}{2}$, and let $v_2(U_{e_1}) = m$. Then

- $e_1 \mid 2 - \left(\frac{D}{2}\right)$;
- $e_2 = \cdots = e_m = 1$ if $m > 1$;
- $e_i = 2$ for all $i \geq m + 1$.

Proof. Instead of following Proposition 8.4.2, we can do everything directly. The claim that $e_2 = \cdots = e_m = 1$ if $m > 1$ is again obvious, so we focus on the other two claims. First, compute that

$$(T_2, U_2) = \left(\frac{T^2 + U^2 D}{2}, TU \right), \quad (T_3, U_3) = \left(T \frac{T^2 + 3DU^2}{4}, U \frac{3T^2 + DU^2}{4} \right).$$

If D is even, then T is even, hence $U_2 = TU$ is even, and so $e_1 \mid 2 = 2 - \left(\frac{D}{2}\right)$. If $D \equiv 1 \pmod{8}$, then if U is odd, we have

$$4 = T^2 - DU^2 \equiv T^2 - 1 \pmod{8}, \text{ hence } T^2 \equiv 5 \pmod{8},$$

contradiction. Thus $e_1 = 1$, and the conclusion follows. Finally, if $D \equiv 5 \pmod{8}$, then if U is even we are done. Otherwise, U is odd, hence T is odd as well. Then U_2 is odd, and

$$3T^2 + DU^2 \equiv 3 + 5 \equiv 0 \pmod{8},$$

whence U_3 is even. Thus $e_1 = 3 \mid 2 - \left(\frac{D}{2}\right)$, as claimed.

To prove the last point, it suffices to assume that D is even, $D/4$ is a discriminant, U is odd, and we need to prove that $2 \parallel U_2$. Since $U_2 = TU$, this is equivalent to $2 \parallel T$. Since $T^2 = 4 + DU^2$, it follows that T is even. If $4 \mid T$, then dividing by 4 and looking modulo 4 gives

$$0 \equiv (T/2)^2 \equiv 1 + (D/4)U^2 \equiv 1 + D/4 \pmod{4}.$$

Since D is even and $D/4$ is a discriminant, $D/4 \equiv 0, 1 \pmod{4}$, both of which are contradictions. \square

Proposition A.2.4. *Let $D = 2^{2k}D'$, where D' is a 2-fundamental discriminant, and $2 \nmid \mathfrak{DM}$. Consider the multiset $\{[(\pi_i \phi \pi_i^{-1})_O] : 1 \leq i \leq 3\}$. This contains*

- 3 optimal embeddings of discriminant $4D$ if $k = 0$ and $\left(\frac{D}{2}\right) = -1$.
- 2 optimal embeddings of discriminant $4D$ and 1 of discriminant D if $k = 0$ and $\left(\frac{D}{2}\right) = 0$.
- 1 optimal embeddings of discriminant $4D$ and 2 of discriminant D if $k = 0$ and $\left(\frac{D}{2}\right) = 1$.
- 2 optimal embeddings of discriminant $4D$ and 1 of discriminant $\frac{D}{4}$ if $k > 0$.

The optimal embeddings of discriminant $4D$ divide into

$$\frac{2 - \left(\frac{D}{2}\right)}{e_1^2(D)} = \frac{2 - \left(\frac{D}{2}\right)}{e_{k+1}^2(D')}$$

distinct equivalence classes, each with multiplicity $e_1^2(D) = e_{k+1}^2(D')$.

Proof. We mostly mirror the proof of Proposition 8.4.5. We can work locally, so that $O_2 = \text{Mat}(2, \mathbb{Z}_2)$, and we can assume that

$$\phi_2(\sqrt{D}) = \begin{pmatrix} p_D & (D-p_D)/2 \\ 2 & -p_D \end{pmatrix}.$$

From Lemma 8.1.2, we can take representatives

$$\pi_i = \begin{pmatrix} 1 & i \\ 0 & 2 \end{pmatrix} : i = 0, 1, \quad \pi_\infty = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

We compute

$$\pi_\infty \phi(\sqrt{D}) \pi_\infty^{-1} = \begin{pmatrix} p_D & D - p_D \\ 1 & -p_D \end{pmatrix},$$

which is an optimal embedding of $4D$. For $i = 0, 1$,

$$\pi_i \phi(\sqrt{D}) \pi_i^{-1} = \begin{pmatrix} p_D + 2i & \frac{D - p_D}{4} - p_D i - i^2 \\ 4 & -2i - p_D \end{pmatrix}.$$

If $D \equiv 5 \pmod{8}$, the top right coefficient is odd for $i = 0, 1$, whence this is an optimal embedding of discriminant $4D$. If $D \equiv 1 \pmod{8}$, these are optimal of discriminant D for $i = 0, 1$. Finally, if D is even, then the top right coefficient is $D/4 - i^2$ which is odd and even for the two choices of i . Since all other coefficients are even, this will be an optimal embedding of discriminant $4D$ for exactly one of the two choices of i , and an embedding of discriminant D for the other. The only way the embedding of discriminant D is not optimal is if either $16 \mid D$ and i is even, or $D \equiv 4 \pmod{16}$ and $i = 1$. In both of these cases the embedding is optimal of discriminant $D/4$, and these cases are equivalent to $k > 0$. Therefore the discriminants occur as claimed.

Next, we check when we get similar embeddings of discriminant $4D$. Let $v = \phi(\epsilon_D) \in O_{N=1}$, fix i , and let $\pi_i v = u \pi_j$ for some j and $u \in O_{N=1}$. As before, $(\pi_j \phi \pi_j^{-1})_O \sim (\pi_i \phi \pi_i^{-1})_O$, and we want to show that if this equation holds then $\pi_i v^k = u \pi_j$ for some integer k and $u \in O_{N=1}$.

As in Proposition 8.4.5, this rearranges to $\pi_j \phi(x + y\sqrt{D}) \pi_i^{-1} = u \in O_{N=1}$ for some rationals x, y . Taking norms, $x^2 - Dy^2 = 1$, whence we are done if we can show that $z = x + y\sqrt{D} \in \mathcal{O}_D$. As $\phi(2z) = \bar{\pi}_j u \pi_i \in O$, we have $z \in \frac{1}{2}\mathcal{O}_D$, hence $4x, 4y \in \mathbb{Z}$. Take the explicit forms of π_i and ϕ as above; in particular,

$$\phi(x + y\sqrt{D}) = \begin{pmatrix} x + p_D y & y(D - p_D)/2 \\ 2y & x - p_D y \end{pmatrix}.$$

If $i, j \in \{0, 1\}$, we can assume they are distinct, hence $i = 0, j = 1$, and $D \equiv 5 \pmod{8}$ (as the embeddings have discriminant $4D$). Then,

$$\pi_j \phi(x + y\sqrt{D}) \pi_i^{-1} = \begin{pmatrix} x + 3y & \frac{1}{2}x + \frac{D-3}{4}y \\ 4y & x - y \end{pmatrix},$$

has \mathbb{Z}_2 entries. Write $4x = X$ and $4y = Y$, and this implies that

$$X \equiv Y \pmod{4}, \quad 2X + (D - 3)Y \equiv 0 \pmod{16}, \quad X^2 - DY^2 = 16.$$

If X is odd, then Y is odd, hence $0 \equiv X^2 - DY^2 \equiv 1 - 5 \equiv 4 \pmod{8}$, contradiction. Thus X, Y are even, and $X/2 \equiv Y/2 \pmod{2}$. Since $z = \frac{(X/2) + (Y/2)\sqrt{D}}{2}$, this implies that $z \in \mathcal{O}_D$, as required.

If $i = \infty$ and $j = 0, 1$, we have

$$\pi_j \phi(x + y\sqrt{D})\pi_\infty^{-1} = \begin{pmatrix} \frac{x}{2} + \frac{(p_D + 2j)y}{2} & jx + ((D - p_D)/2 - p_D j)y \\ 2y & 2x - 2yp_D \end{pmatrix} \in \text{Mat}(2, \mathbb{Z}_2).$$

Thus $2x, 2y \in \mathbb{Z}$, write $2x = X$ and $2y = Y$, and it requires to show that $X \equiv YD \pmod{2}$. But $X^2 - DY^2 = 4$, so they solve Pell's equation, and the conclusion follows.

The finish is exactly as in Proposition 8.4.5. □

A.3 Hermite normal form calculation

We calculate the determinant of the row-space of the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{p_1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{p_2}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{p_1 p_2 + x}{4} & \frac{p_2}{4} & \frac{p_1}{4} & \frac{\ell}{4} \\ 0 & \frac{-x}{4\ell} & \frac{D_1}{4\ell} & \frac{p_1}{4} \\ 0 & \frac{-D_2}{4\ell} & \frac{x}{4\ell} & \frac{p_2}{4} \\ \frac{x^2 - D_1 D_2}{8\ell} & \frac{-p_2 x - p_1 D_2}{8\ell} & \frac{p_1 x + p_2 D_1}{8\ell} & \frac{p_1 p_2 + x}{8} \end{pmatrix},$$

where:

- D_1, D_2 are discriminants with parities p_1, p_2 respectively;
- $\gcd\left(D_1, D_2, \frac{D_1 D_2 - x^2}{4}\right) = 1$
- $4\ell^2 \mid D_1 D_2 - x^2$.

Let L be this rowspace, and label the rows r_1, \dots, r_8 . Since $L \supseteq \mathbb{Z}^4$ and \mathbb{Z}^4 has determinant 1, we see that the determinant of L is $\frac{1}{N}$ for some positive integer N . Our aim is to show that $N = 16\ell$. We can compute N by tensoring our space with \mathbb{Z}_p for all primes p , and determining the power of p dividing the determinant of the corresponding \mathbb{Z}_p lattice.

Note that all denominators of M divide 8ℓ . Hence $p \nmid 2\ell$ implies that $L_p = \mathbb{Z}_p^4$, and so $v_p(N) = 0$, as desired.

Next, assume that $p \mid 2\ell$ is odd. Thus $p \mid \ell \mid D_1 D_2 - x^2$, which implies that D_1 and D_2 are not both divisible by p . The first four rows of M_p span \mathbb{Z}_p^4 , and the fifth row is already in this span. Since $\ell \mid \ell^2 \mid D_1 D_2 - x^2$, by removing the powers of 2 and applying row operations, the last three rows (labeled r'_6, r'_7, r'_8 in order) become

$$\begin{pmatrix} 0 & \frac{-x}{\ell} & \frac{D_1}{\ell} & 0 \\ 0 & \frac{-D_2}{\ell} & \frac{x}{\ell} & 0 \\ 0 & \frac{-p_2 x - p_1 D_2}{\ell} & \frac{p_1 x + p_2 D_1}{\ell} & 0 \end{pmatrix}.$$

First, $r'_8 = p_2 r'_6 + p_1 r'_7$, so we can ignore r'_8 . Next, we have

$$x r'_6 - D_1 r'_7, D_2 r'_6 - x r'_7 \in \langle r_1, r_2, r_3, r_4 \rangle_{\mathbb{Z}_p}.$$

Without loss of generality assume that $p \nmid D_1$, whence $r'_7 \in \langle r_1, r_2, r_3, r_4, r'_6 \rangle_{\mathbb{Z}_p}$. Then $r_3 \in \langle r_1, r_2, r_4, r'_6 \rangle_{\mathbb{Z}_p}$, and thus our basis is spanned by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \frac{-x}{\ell} & \frac{D_1}{\ell} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The power of p dividing the denominator of this determinant is $v_p(\ell) = v_p(16\ell)$, as desired.

The remaining case is $p = 2$. Let $v_2(\ell) = k \geq 0$, write $\ell = 2^k \ell'$ with ℓ' odd, and assume

that D_1 is odd. Working over \mathbb{Z}_2 , we multiply out by odd factors to obtain the row-space

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{p_2}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{p_2+x}{4} & \frac{p_2}{4} & \frac{1}{4} & \ell' 2^{k-2} \\ 0 & \frac{-x}{2^{k+2}} & \frac{D_1}{2^{k+2}} & \frac{\ell'}{4} \\ 0 & \frac{-D_2}{2^{k+2}} & \frac{x}{2^{k+2}} & \frac{p_2 \ell'}{4} \\ \frac{x^2 - D_1 D_2}{2^{k+3}} & \frac{-p_2 x - D_2}{2^{k+3}} & \frac{x + p_2 D_1}{2^{k+3}} & \frac{(p_2 + x) \ell'}{8} \end{pmatrix}.$$

We now find the span of the first 5 rows, and successively add in rows 6 through 8 in the various cases.

- If D_2 is even,

- If $k = 0$,

- * If $2 \parallel x$, rows 1 to 5 give

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Rows 6 and 7 already lie in this span, and row 8 shifts to $(\frac{x^2 - D_1 D_2}{8} \frac{-D_2}{8} \frac{1}{4} \frac{1}{4})$.

If $4 \parallel D_2$, it follows that $8 \mid D_1 D_2 - x^2$, and after a \mathbb{Z}_2^4 shift, row 8 becomes $(0 \frac{1}{2} \frac{1}{4} \frac{1}{4})$, which is already in the span. Otherwise, $8 \mid D_2$, and by a \mathbb{Z}_2^4 shift we arrive at $(\frac{1}{2} 0 \frac{1}{4} \frac{1}{4})$. Thus rows 1 through 5 sufficed, we get the determinant 2^{-4} , so the power of two dividing the denominator is $4 = k + 4$, as desired.

- * If $4 \mid x$, rows 1 to 5 give

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix},$$

and the last three rows already lie in this span. The determinant is again 2^{-4} , as desired.

– If $k = 1$, then $16 \mid D_1 D_2 - x^2$.

* If $2 \parallel x$, then $4 \parallel D_2$ necessarily. The first 5 rows give

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{4} & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Shifting the sixth row gives $(0, \pm\frac{1}{4}, \frac{1}{8}, \frac{1}{4})$ (using $D_1 \equiv 1 \pmod{4}$), which can replace row two, giving

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \pm\frac{1}{4} & \frac{1}{8} & \frac{1}{4} \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

The seventh and eighth rows lie in this span, and the determinant is 2^{-5} , as desired.

* If $4 \mid x$, then $16 \mid D_2$ necessarily. The first 5 rows give

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Rows 7 and 8 already lie in this span, and row 6 shifts to $(0, \frac{-x}{8}, \frac{1}{8}, \frac{1}{4})$. If $4 \parallel x$ we can replace the second row, and if $8 \mid x$ we can replace the third row, giving

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \pm\frac{1}{2} & \frac{1}{8} & \frac{1}{4} \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \text{ and } \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{8} & \frac{1}{4} \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

respectively. This gives determinant 2^{-5} , as desired.

– If $k \geq 2$, then $64 \mid 2^{2k+2} \mid D_1 D_2 - x^2$. The last three rows shift to

$$\begin{pmatrix} 0 & \frac{-x}{2^{k+2}} & \frac{D_1}{2^{k+2}} & \frac{\ell'}{4} \\ 0 & \frac{-D_2}{2^{k+2}} & \frac{x}{2^{k+2}} & 0 \\ 0 & \frac{-D_2}{2^{k+3}} & \frac{x}{2^{k+3}} & \frac{x\ell'}{8} \end{pmatrix}.$$

Since $xxr_6 - D_1r_7$ lies in the span of the first four rows, so we can eliminate r_7 from consideration. Similarly, $\frac{x}{2}r_6 - D_1r_8$ also lies in this span, so we can eliminate r_8 from consideration too; only the first 6 rows are left.

* If $2 \parallel x$, rows 1 to 5 give us

$$\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{2} & \frac{1}{4} & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

We can replace r_2 with r_6 giving

$$\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{-x}{2^{k+2}} & \frac{D_1}{2^{k+2}} & \frac{\ell'}{4} \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix},$$

which has determinant $\frac{-x}{2^{k+5}}$, as desired (since $v_2(x) = 1$).

* If $4 \mid x$, rows 1 to 5 give us

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

In this case we can replace r_3 with r_6 , giving

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \frac{-x}{2^{k+2}} & \frac{D_1}{2^{k+2}} & \frac{\ell'}{4} \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix},$$

which has determinant $\frac{D_1}{2^{k+4}}$, as desired (since D_1 is odd).

- If D_2 is odd,

– If $k = 0$, then the first 5 rows give us

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{-x}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

The last three rows lie in this span, so we get determinant 2^{-4} , as desired.

– If $k \geq 1$, the first five rows give

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{4} & \frac{-x}{4} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

The second row can be replaced by the seventh, giving

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{-D_2}{2^{k+2}} & \frac{x}{2^{k+2}} & \frac{1}{4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

This span also contains the sixth and eighth rows, hence is a valid basis. The 2–adic valuation of this determinant is $-(k + 4)$, as desired.

If D_2 is odd, then the above computations again hold. The final possibility is that D_1, D_2 are both even. Since $\gcd\left(D_1, D_2, \frac{D_1 D_2 - x^2}{4}\right) = 1$, it follows that $2 \parallel x$, and that $k = 0$. Plug this into M , and it follows immediately that the rowspace is spanned by

$$\begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{4} \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

The 2–adic valuation of the determinant is $-4 = -(k + 4)$, as required.

Bibliography

- [AACCC18] Manuel Arenas, Luis Arenas-Carmona, and Jaime Contreras. On optimal embeddings and trees. *J. Number Theory*, 193:91–117, 2018.
- [AC13] Luis Arenas-Carmona. Eichler orders, trees and representation fields. *Int. J. Number Theory*, 9(7):1725–1741, 2013.
- [AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.
- [BD96] M. Bertolini and H. Darmon. Heegner points on Mumford-Tate curves. *Invent. Math.*, 126(3):413–456, 1996.
- [Bue89] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.
- [Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$* . Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.
- [Dic29] L.E. Dickson. *Introduction to the Theory of Numbers*. The University of Chicago Press, 1929.
- [DIT17] W. Duke, Ö. Imamoğlu, and Á. Tóth. Modular cocycles and linking numbers. *Duke Math. J.*, 166(6):1179–1210, 2017.

- [Dor88] David R. Dorman. Special values of the elliptic modular function and factorization formulae. *J. Reine Angew. Math.*, 383:207–220, 1988.
- [Duk88] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.
- [DV13] Lassina Dembélé and John Voight. Explicit methods for Hilbert modular forms. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 135–198. Birkhäuser/Springer, Basel, 2013.
- [DV20] Henri Darmon and Jan Vonk. Singular moduli for real quadratic fields: A rigid analytic approach. *Duke Math. J.*, 2020.
- [GH78] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Wiley-Interscience [John Wiley & Sons], New York, 1978. Pure and Applied Mathematics.
- [Ghy07] Étienne Ghys. Knots and dynamics. In *International Congress of Mathematicians. Vol. I*, pages 247–277. Eur. Math. Soc., Zürich, 2007.
- [GV11] Matthew Greenberg and John Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. *Math. Comp.*, 80(274):1071–1092, 2011.
- [GZ85] Benedict H. Gross and Don B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.
- [Hun07] J. D. Hunter. Matplotlib: A 2d graphics environment. *Computing in Science & Engineering*, 9(3):90–95, 2007.
- [Kan89] Masanobu Kaneko. Supersingular j -invariants as singular moduli mod p . *Osaka J. Math.*, 26(4):849–855, 1989.
- [LMF20] The LMFDB Collaboration. The L-functions and modular forms database. <http://www.lmfdb.org>, 2020. [Online; accessed 26 February 2019].
- [LV15] Kristin Lauter and Bianca Viray. On singular moduli for arbitrary discriminants. *Int. Math. Res. Not. IMRN*, (19):9206–9250, 2015.

- [Mil71] John Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. *Annals of Mathematics Studies*, No. 72.
- [Pag14] A. Page. An algorithm for the principal ideal problem in indefinite quaternion algebras. *LMS J. Comput. Math.*, 17(suppl. A):366–384, 2014.
- [Pag15] Aurel Page. Computing arithmetic Kleinian groups. *Math. Comp.*, 84(295):2361–2390, 2015.
- [Ric20] James Rickards. Q- Quadratic. <https://github.com/JamesRickards-Canada/Q-Quadratic>, 2020.
- [SV18] K. Spalding and A. P. Veselov. Conway river and Arnold Sail. *Arnold Math. J.*, 4(2):169–177, 2018.
- [The20] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.0*, 2020. available from <http://pari.math.u-bordeaux.fr/>.
- [Voi09] John Voight. Computing fundamental domains for Fuchsian groups. *J. Théor. Nombres Bordeaux*, 21(2):469–491, 2009.
- [Voi21] John Voight. Quaternion algebras. To be published, 2021.

Index

- O^{\min} , 44
 (O, p) , 87
 $(a, b)_v$, 41
 B , 40
 B_Δ , 19
 C_B , 43
 D^{fund} , 48
 D_O^ϕ , 47
 E_{ϕ_1, ϕ_2}^f , 114
 $G_O^p(\phi)$, 125
 $N_{B^\times}(O)$, 44
 O , 41
 $O_L(I)$, 41
 $O_{N=f}$, 44
 O_{ϕ_1, ϕ_2} , 80
 $O_{\phi_1, \phi_2}(\ell)$, 92
 $O_{\phi_1, \phi_2}^{\text{Eich}}$, 88
 $Q_{\phi_1, \phi_2}(X, Y)$, 58
 S_{ϕ_1, ϕ_2} , 91
 S_{ϕ_1, ϕ_2}^B , 58
 T'_n , 115
 T_n , 117, 120
 $T_{\phi_1, \phi_2}(\mathfrak{M})$, $T_{\phi_1, \phi_2}(\mathfrak{M}, \ell)$, 98
 W_{p^e} , 118
 $[\phi]$, 48
 $\text{Cl}^+(D)$, 17
 $\Delta(\alpha)$, 87
 $\text{Emb}(O, D_1, D_2, x, \ell)$, 97
 $\text{Emb}(O, \phi_1, \phi_2, x)$, 72
 $\text{Emb}(O, \phi_1, \phi_2, x, \ell)$, 97
 $\text{Emb}(B, D_1, D_2, x)$, 82
 $\text{Emb}(O)$, 113
 $\text{Emb}(O, D)$, 48
 $\text{Emb}(O, D_1, D_2, x)$, 72
 $\text{Emb}^+(O)$, 113
 $\text{Emb}_o(O, D)$, 52
 $\text{Emb}_{o_1, o_2}^+(O, D_1, D_2, x, \ell)$, 101
 Γ , 2
 Γ_O , 69
 Int_O^g , 74
 Int_O , 74
 Int_O^f , 70
 Int_O^\pm , 74
 Int_Γ^f , 8
 $\text{PB}(D_1, D_2)$, 89
 QA_p^{div} , 41
 $\text{QA}_\infty^{\text{div}}$, 41
 $\Theta(n)$, 114
 $\ell(\phi_1, \phi_2)$, 74
 $\ell_{z_1, z_2}, \dot{\ell}_{z_1, z_2}, \ddot{\ell}_{z_1, z_2}$, 5
 ϵ , 85
 γ_q , 17
 $\langle \cdot, \cdot \rangle_f$, 114
 $\left(\frac{\cdot}{p}\right)$, 41
 \mathbb{H} , 5
 \mathcal{O}_D , 47
 \mathfrak{D} , 41
 \mathfrak{M} , 42
 nrd , 41
 ω_p , 45
 $\phi_1 \times \phi_2$, 74
 ϕ_O , 47
 \mathfrak{h} , 8
 sg , 7, 74

- \sim_n , 116
- trd, 41
- $e_k^p(D)$, 121
- $h^+(D)$, 17
- $o(\phi)$, 52, 54, 55
- p_D , 48
- w_n , 117
- x_{o_1, o_2} , 103
- binary quadratic form, 16
 - PIBQF, 17
 - reciprocal, 17
 - topograph, 23
- geodesic
 - closed, 6
 - prime, 6
 - root, 6
- intersection number, 8, 70
 - level, 74
- q-weighted, 74
- sign, 74
- signed, 9, 74
- unweighted, 9, 74
- prime
 - nice, 86
 - potentially bad, 89
- quaternion algebra, 40
 - centralizing algebra, 43
 - discriminant, 41
 - embedding, 47
 - class group action, 60
 - equivalence, 48
 - Hecke operator, 117, 118, 120
 - optimal, 47
 - orientation, 52
- positive/negative
 - definite, 54
- prime power Hecke
 - graph, 125
 - x-linked, 70
- order, 41
 - Bruhat-Tits tree, 46
 - discriminant, 42
 - Eichler symbol, 87
 - inverted triangle, 46
 - level, 42
- roots
 - first/attracting, 5, 18
 - second/repelling, 6, 18
- strong inequivalence, 8, 17
- trefoil knot, 21, 39