The Dissertation Committee for Melissa Lorena Macasieb
certifies that this is the approved version of the following dissertation:

Derived Arithmetic Fuchsian Groups of Genus Two

Committee:

Alan Reid, Supervisor

Robert Gompf

Cameron Gordon

Darren Long

John Luecke

Derived Arithmetic Fuchsian Groups of Genus Two

by

Melissa Lorena Macasieb, B.A.; M.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

December 2005

To my husband and my parents.

Acknowledgments

I would like to thank the many people in the UT Department of Mathematics who have given me support, both intellectually and emotionally, during my time here. I would especially like to thank my advisor, Alan Reid, for suggesting the problem in this dissertation and for many useful and enlightening mathematical conversations. Special thanks are also due to Cameron Gordon, Fernando Rodriguez-Villegas, and Felipe Voloch for their helpful comments. Most of all, I would like to thank my husband, Antoine Mellet, for his infinite patience, encouragement, and understanding.

Derived Arithmetic Fuchsian Groups of Genus Two

Publication No. ____________________

Melissa Lorena Macasieb, Ph.D.
The University of Texas at Austin, 2005

Supervisor: Alan Reid

We classify all torsion-free derived arithmetic Fuchsian groups of genus two by commensurability class. In particular, we show that there exist no such groups arising from quaternion algebras over number fields of degree greater than 5. We also prove some results on the existence and form of maximal orders for a certain class of quaternion algebras. These can in turn be used to find an explicit set of generators for each derived arithmetic group containing a torsion-free subgroup of genus two. We show this for a number of examples.

Table of Contents

Chapter 1

Introduction

A cocompact Fuchsian group Γ acts properly discontinuously on $\mathbf{H}^2$ with quotient $\mathbf{H}^2/\Gamma$, a hyperbolic 2-orbifold with a finite number of cone points. An arithmetic Fuchsian group has finite coarea and therefore is necessarily of the first kind. It is a well-known result that there are finitely many conjugacy classes of arithmetic Fuchsian groups with a given signature (see [11], [20]). Extensive work has been done classifying the space of $PGL_2(\mathbb{R})$-conjugacy classes of various two-generator arithmetic groups: triangle groups (see [19]), groups of signature (1;e) (see [20]), and groups of signature $(0; 2, 2, 2, q)$ (see [12], [1]). However, it is significantly more difficult to classify $PGL_2(\mathbb{R})$-conjugacy classes of arithmetic groups of genus two since these groups have larger areas. We can nonetheless determine all commensurability classes of derived arithmetic Fuchsian groups of genus two using area estimates. There is a finite list of signatures of groups Γ' that can possibly contain a subgroup Γ of signature $(2; 0)$. Following [12], we determine all commensurability classes of derived arithmetic groups with these signatures by invariant quaternion algebra. We then determine all $PGL_2(\mathbb{R})$-conjugacy classes of the groups Γ'. However, if $\Gamma \subsetneq \Gamma'$, then the number of conjugacy classes of Γ is not necessarily equal to that of Γ'. In [19],[20] and [12], the $PGL_2(\mathbb{R})$-conjugacy classes for all of the groups Γ' are classified except for those of signatures $(1; 2, 2)$, $(0; 2, 2, 2, 2, 2, 2)$, and $(2; 0)$. For each group with one of these signatures, we determine a fundamental region and an explicit set of generators using a computer program.

In the remainder of this chapter, we give a brief overview of the theory of arithmetic Fuchsian groups. This includes a small section with the definitions and theorems in elementary number theory which figure prominently in our methods. In Chapter 2, we classify all commensurability classes of derived genus two surface groups using invariant quaternion algebras and arithmetic data. Using Pari and estimates on the degree of the number field, we find that there exist no derived arithmetic Fuchsian groups Γ of signature (2;0) arising from quaternion algebras over number fields of degree greater than 5. We list all possible quaternion algebras giving rise to the groups along with the signatures and number of conjugacy classes of their unit groups, $\Gamma^1_{\mathcal{O}}$. In Chapter 3, we describe the general technique used to find a Ford fundamental domain for an arithmetic Fuchsian group and we also prove some general results on the structure of maximal orders in these quaternion algebras. In Chapter 4, we exhibit the technique used to determine the Ford domain for a few illustrative examples of $\Gamma^1_{\mathcal{O}}$. The Ford domain yields a list of generators for $\Gamma^1_{\mathcal{O}}$ and, hence, allows us to the determine the generators of the genus two subgroup Γ explicitly. We show this for a few examples. Finally, we collect a list of generators for the arithmetic groups $\Gamma^1_{\mathcal{O}}$ of signatures (2;0), (1;2,2), and (0;2,2,2,2,2,2) in Chapter 5.

1.1 Number Theoretic Preliminaries

In this section we collect some definitions and well-known theorems in number theory that will be used to prove the main results.

1.1.1 Number Fields

A *number field* k is a finite extension of $\mathbb{Q}$ of the form $\mathbb{Q}(\alpha)$ where α is a root of a monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. The polynomial $f(x)$ is called the minimal polynomial of α and the degree d of f is the degree of the extension $|k : \mathbb{Q}|$.

The roots $\alpha_1, \ldots, \alpha_d$ of the minimal polynomal are called the *conjugates* of α. Each of the roots α_i corresponds exactly to one of the d Galois field monomorphisms $k \to \mathbb{C}$ via the assignment $\alpha \mapsto \alpha_i$. These field monomorphisms are denoted by $\sigma_1, \ldots, \sigma_d$. Since $f(x) \in \mathbb{Q}[x]$, the roots α_i are real or pairs of complex conjugates. If $\sigma_i(k) \subset \mathbb{R}$, the monomorphism σ_i is referred to as *real*. Otherwise, the monomorphisms occur in complex conjugate pairs $(\sigma_i, \bar{\sigma_i})$ where $\sigma_i(k) \not\subset \mathbb{R}$. If we denote the number of real roots by r_1 and number of complex conjugate pairs by r_2, then $d = r_1 + 2r_2$ and we say that k has r_1 real places and r_2 complex places. We will be concerned with *totally real* fields, i.e., the cases in which $r_2 = 0$.

Let K denote the Galois closure of the extension $k|\mathbb{Q}$. K is the compositum of the fields $\sigma_i(k), 1 \le i \le d$. Recall that, for $\alpha \in k$, the norm and trace of α are defined by:

$$\mathrm{N}_{k|\mathbb{Q}}(\alpha) = \prod_{i}^{d} \sigma_i(\alpha) \quad \mathrm{Tr}_{k|\mathbb{Q}}(\alpha) = \sum_{i}^{d} \sigma_i(\alpha).$$

If $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is a basis of the field $k|\mathbb{Q}$, then the *discriminant* of $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is defined by

$$\mathrm{disc}\{\alpha_1, \alpha_2, \ldots, \alpha_d\} = \det[\sigma_i(\alpha_j)]^2 = \det[\mathrm{Tr}(\alpha_i \alpha_j)].$$

Note that *disc*$\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is invariant under each $\sigma_i \in \mathrm{Gal}(K|\mathbb{Q})$ and, hence, lies in its fixed field, $\mathbb{Q}$.

Let A be a ring contained in some field k and x be an element of k. Then x is *integral* over A provided that x satisfies an monic equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \in A$ and $n \in \mathbb{Z}^+$. The set of elements of k which are integral over A form a ring, called the *integral closure* of A in k.

The set of elements of a number field k that are integral over $\mathbb{Z}$ is a ring and is called the ring of *algebraic integers* and will be denoted by R_k. A $\mathbb{Z}$-basis for the abelian group R_k is called an integral basis of k. Furthermore, the *discriminant*, d_k, of a number field k is the discriminant of any integral basis of k.

Theorem 1.1.1. *For any positive integer D, there are only finitely many number fields k with $|d_k| \leq D$.*

The relative discriminant for a finite extension of number fields $\ell|k$ is defined as follows. Let $\ell|k$ be a finite extension of number fields of degree $|\ell : k| = n$. Let R_ℓ and R_k denote the rings of integers of ℓ and k, respectively. The set $\{\alpha_1, \ldots, \alpha_n\}$ is a *relative integral basis* of $\ell|k$ if it is an R_k-basis of R_ℓ. However, since R_k is not necessarily a principal ideal domain and R_ℓ is not necessarily a free R_k-module, a relative integral basis for the extension $\ell|k$ need not exist. If such a basis does exist, then the *relative discriminant* $\delta_{\ell|k}$ is defined to be the ideal generated by the set of elements $\{\text{disc}\{\alpha_1, \alpha_2, \ldots, \alpha_d\}\}$ where $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ runs through the bases of $\ell|k$ consisting of algebraic integers. Furthermore, the (relative) discriminant $\text{disc}_{\ell|k}$ is related to the (absolute) discriminant d_ℓ over $\mathbb{Q}$ by the following formula:

$$|d_\ell| = |N(\delta_{\ell|k})d_k^d|. \tag{1.1}$$

1.1.2 Ideals and Factorization in Rings of Integers

Let R be a ring and K its quotient field. A *fractional ideal* of R in K is an R-module I contained in K such that there exists an element $c \neq 0$ in R for which $cI \subset R$. A *principal fractional ideal* is an ideal of the form αR, where α is a nonzero element of the quotient field of R.

An integral domain D with field of fractions K is called a *Dedekind domain* provided the following three conditions hold:

1. D is Noetherian.
2. D is integrally closed in K.
3. Every nonzero prime ideal of D is maximal.

In addition, the set of fractional ideals of the ring of integers R_k of a number field k forms a free abelian group under multiplication and this group will be denoted I_k. The subset P_K of nonzero principal fractional ideals of D is a subgroup of I_K. The group $C_K = I_K/P_K$ of fractional ideals modulo the group of principal ideals is called the *ideal class group* of D. The ideal class group is finite and its order, h, is called the *class number* of K.

Theorem 1.1.2. *Let R_k be the ring of integers in the number field k. Then R_k is a Dedekind domain and for any nonzero ideal I of R_k, R_k/I is a finite ring.*

For a nonzero ideal I of R_k, the norm of I is defined by

$$N(I) = |R_k/I|.$$

Note that the norm is multiplicative by the Chinese Remainder Theorem.

Let D be a Dedekind domain, K its quotient field, L a finite separable extension of K, and R the integral closure of D in L. If D is a prime ideal of D then pR is an ideal of R and has a factorization

$$pR = \mathcal{P}_1^{e_r} \cdots \mathcal{P}_r^{e_r}$$

where, for each i, $e_i \geq 1$ and $R_k/\mathcal{P}_i$ is a finite field of order p^{f_i} for some $f_i \geq 1$. The primes $\mathcal{P}_i$ with $e_i > 1$ are called *ramified*. Furthermore, if $|k : \mathbb{Q}| = d$, then $d = \Sigma e_i f_i$ by multiplicativity of the norm.

1.1.3 Units

The units in the ring of integers R_k, denoted by R_k^* are defined by:

$$R_k^* = \{\alpha \in R_k | \exists \, \beta \in R_k \text{ such that } \alpha\beta = 1\}.$$

The units form an abelian group under multiplication and $\alpha \in R_k$ is a unit if and only if $N_{k|\mathbb{Q}} = \pm 1$.

Theorem 1.1.3. *For any number field k,*

$$R_k^* = W \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where W is a finite cyclic group of even order consisting of the roots of unity contained in k and the rank of R_k^* is $r = r_1 + r_2 - 1$.

The subgroup of squares of units in R_k will be denoted by R_k^{*2}.

1.1.4 Valuations

A *valuation* on an arbitrary field K is a mapping $v : K \to \mathbb{R}^+$ such that

(i) $v(x) \geq 0$ for all $x \in K$ and $v(x) = 0$ if and only if $x = 0$.

(ii) $v(xy) = v(x)v(y)$ for all $x, y \in K$.

(iii) $v(x + y) \leq v(x) + v(y)$ for all $x, y \in K$.

Two valuations v and w on K are *equivalent* if there exists an $s \in R^+$ such that $w(x) = [v(x)]^s$ for $x \in K$.

If, in addition, the valuation v satisfies the property

(iv) $v(x + y) \leq \max\{v(x), v(y)\}$for all $x, y \in K$,

v is called a *non-Archimedean* valuation. If v is not equivalent to a valuation satisfying property (iv), then v is called *Archimedean*.

Fact 1.1.4. *Let v be a non-Archimedean valuation on K. Let*

$$R(v) = \{\alpha \in K | v(\alpha) \leq 1\} \quad M(v) = \{\alpha \in K | v(\alpha) < 1\}.$$

Then $R(v)$ is a local ring with unique maximal ideal $M(v)$ and with field of fractions K.

The ring $R(v)$ is called the *valuation ring* of K (with respect to v).

If k is a number field, then one can explicitly determine all valuations on k as follows. All Archimedian valuations are given by $v_\sigma = |\sigma(x)|$, where $\sigma : K \to \mathbb{C}$ is a Galois embedding. Furthermore, v_σ and $v_{\sigma'}$ are equivalent if and only if (σ, σ') are a complex conjugate pair. Let $\mathcal{P}$ be a prime ideal in R_k and c a real number satisfying $1 < c < 0$. For $x \in R_k \ \{0\}$, the valuation defined by $v_{\mathcal{P}}(x) = c^{n_{\mathcal{P}}(x)}$, where $n_{\mathcal{P}}(x)$ is the largest integer m such that $x \in \mathcal{P}^m$, can be extended to k by $v_{\mathcal{P}}(x/y) = v_{\mathcal{P}}(x)/v_{\mathcal{P}}(y)$. This valuation on k is well-defined and non-Archimedean.

The following theorem completely characterizes the valuations on a number field k.

Theorem 1.1.5. *Let k be a number field. Any non-Archimedean valuation on k is equivalent to a $\mathcal{P}$-adic valuation $v_{\mathcal{P}}$ for some prime ideal $\mathcal{P}$ in R_k and any Archimedean valuation on k is equivalent to a valuation v_σ for some Galois monomorphism of k.*

The equivalence class of valuations is called a *place*, and the classes of Archimedean and non-Archimedean places on k are referred to as the *infinite places* and *finite places* of k, respectively.

Finally, an element $\pi \in R_k$ satisfying $n_{\mathcal{P}}(\pi) = 1$ is called a *uniformizer* for $v_{\mathcal{P}}$. Then the unique maximal ideal $\mathcal{P}(v_{\mathcal{P}}) = \pi R(v_{\mathcal{P}})$ and the quotient field $R(v_{\mathcal{P}})/\pi R(v_{\mathcal{P}})$ coincides with the residue field $R_k/\mathcal{P}$.

1.2 Fuchsian Groups

In this section we give some general well-known results about arbitrary Fuchsian groups. A Fuchsian group is a discrete subgroup of $PSL_2(\mathbb{R})$ that acts properly discontinuously on the hyperbolic plane $\mathbf{H}^2$. A finitely generated Fuchsian group Γ of the first kind has finite coarea, i.e., $\mathbf{H}^2/\Gamma$ has finite hyperbolic area. Any such group Γ has the following standard presentation:

$$\left\langle a_1, b_1, \ldots, a_g, b_g, c_1, \ldots c_r, p_1 \ldots, p_s \middle| \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} c_j \prod_{k=1}^{s} p_k, c_1^{m_1}, \ldots, c_r^{m_r} \right\rangle,$$

where the c_i represent the r conjugacy classes of maximal cyclic subgroups of order m_i for $i = 1, \ldots, r$. The group Γ is said to have *signature*

$$(g; m_1, \ldots, m_r; s). \tag{1.2}$$

Note that Γ is cocompact if and only if $s = 0$. Since we will be concerned only with cocompact groups, we will abbreviate the signature to $(g; m_1, \ldots, m_r)$. Using the signature of a Fuchsian group, we can compute its area using the Reimann-Hurwitz formula:

$$\mu(\Gamma) := \text{area}(\mathbf{H}^2/\Gamma) = 2\pi \left(2g - 2 + \sum_{i=1}^{r} \frac{m_i - 1}{m_i} \right) \tag{1.3}$$

Furthermore, if $\Gamma_1 < \Gamma$ are Fuchsian groups and $|\Gamma : \Gamma_1| = m$ then $\mu(\Gamma_1) = m \cdot \mu(\Gamma)$.

Two Fuchsian groups Γ_1 and Γ_2 are *commensurable* if they share a finite index subgoup, i.e., $|\Gamma_1 : \Gamma_1 \cap \Gamma_2| < \infty$ and $|\Gamma_2 : \Gamma_1 \cap \Gamma_2| < \infty$. The *commensurability class* of a group Γ is the collection of groups with which Γ is commensurable.

1.3 Arithmetic Fuchsian Groups

Arithmetic Fuchsian groups are defined via quaternion algebras over a certain class of number fields. Let k be a totally real number field and let A be a quaternion algebra A over k, i.e., a four-dimensional central simple algebra over k.

Any quaternion algebra is isomorphic to an algebra

$$A = \left(\frac{a, b}{k} \right)$$

where $i^2 = a, j^2 = b, ij = -ji$ for some $a, b \in k^*$. The basis $\{1, i, j, ij\}$ is referred to as the *standard basis* of A.

For any element $x = x_0 + x_1 i + x_2 j + x_3 ij \in A$, the conjugate $\bar{x}$ of x is defined by $\bar{x} = x_0 - x_1 i - x_2 j - x_3 ij$.

For $x \in A$ the (reduced) norm and (reduced) trace of x lie in F and are defined by

$$\mathrm{n}(x) = x\bar{x} \quad \text{and} \quad \mathrm{tr}(x) = x + \bar{x}.$$

The algebra A is *ramified* at the infinite place σ of k if $A \otimes_{\sigma(k)} \mathbb{R} \cong \mathcal{H}$, where $\mathcal{H}$ denotes the Hamiltonian quaternions, and *unramified* at σ if $A \otimes_{\sigma(k)} \mathbb{R} \cong M_2(\mathbb{R})$.

Similarly, if v is a finite place of k and k_v the completion of k corresponding to v, then A is *ramified* at v if $A \otimes_k k_v$ is a division algebra. Otherwise, A is *unramified* at v and $A \otimes_k k_v \cong M_2(k_v)$.

The ramification set of A is denoted by $Ram(A)$ and $Ram(A) = Ram_\infty(A) \cup Ram_f(A)$, where $Ram_f(A)$ is the set of finite places at which A is ramified and $Ram_\infty(A)$ is the set infinite places of A at which A is ramified. The product of the primes at which A is ramified is denoted by $\Delta(A)$. Furthermore, the cardinality of the full ramification set of A is even, and conversely, for any set of places of k of even cardinility there exists a quaternion algebra ramified at that set of places.

Let R denote the ring of integers of the number field k. If V is a vector space over k, an R-*lattice* L is V is a finitely generated R-module contained in V. Moreover, L is *complete* if $L \otimes_R k \equiv V$.

An *order* $\mathcal{O}$ of A is a complete R-lattice which is also a ring with 1. Furthermore, an order $\mathcal{O}$ is maximal if it is maximal with respect to inclusion.

In Section 3.1, we will discuss quaternion algebras and maximal orders in more detail.

Let k be a totally real field with $|k : \mathbb{Q}| = n$ and A a quaternion algebra over k which is ramified at all but one real place. Then

$$A \otimes_k \mathbb{R} \cong M_2(\mathbb{R}) \oplus \mathcal{H}^{n-1}.$$

Let ρ be the unique k-embedding of A into $M_2(\mathbb{R})$. Then for a maximal order $\mathcal{O}$ in A, the image under ρ of the group, $\mathcal{O}^1$, of elements of norm 1 in $\mathcal{O}$ forms a finite coarea Fuchsian group. A subgroup Γ of $PSL_2(\mathbb{R})$ is an *arithmetic Fuchsian group* if it is commensurable with some such $P\rho(\mathcal{O}^1)$. In addition, Γ is called *derived from a quaternion algebra* if $\Gamma \leq P\rho(\mathcal{O}^1)$. We will denote $P\rho(\mathcal{O}^1)$ by $\Gamma^1_{\mathcal{O}}$. Furthermore, the area formula of $\mathbf{H}^2/\Gamma^1_{\mathcal{O}}$ can be computed by using the the following formula [2]:

$$\text{area}(\mathbf{H}^2/\Gamma^1_{\mathcal{O}}) = \frac{8\pi d_k^{3/2}\zeta_k(2)\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{(4\pi^2)^{|k:\mathbb{Q}|}}. \qquad (1.4)$$

Here, d_k is the discriminant of the number field k and ζ_k is the Dedekind zeta function of the field k defined for $\text{Re}(s) > 1$ by $\zeta_k(s) = \sum_I \frac{1}{N(I)^s}$, where the sum is over all ideals in the ring of integers of k, R_k.

Furthermore, if Γ is an arithmetic Fuchsian group, then the corresponding quaternion algebra is uniquely determined up to isomorphism and is called the *invariant quaternion algebra* of Γ. By a result of Takeuchi ([19]), two arithmetic groups are commensurable if and only if their invariant quaternion algebras are isomorphic.

We will use the following two classical theorems on the existence and uniqueness of quaternion algebras:

Theorem 1.3.1. *Let A be a quaternion algebra over a number field k. The number of places v such that A is ramified at v is of even cardinality.*

Theorem 1.3.2. *Given a number field k and a collection of infinite places $S_1 = \{\sigma_1, \ldots, \sigma_r\}$ and a collection of finite places $S_2 = \{\mathcal{P}_1, \ldots, \mathcal{P}_s\}$ of k such that $r + s$ is even, there exists a quaterion algebra defined over k with $Ram_\infty(A) = S_1$ and $Ram_f(A) = S_2$.*

Theorem 1.3.3. *Let A and A' be quaternion algebras over a number field k. Then $A \cong A'$ if and only if $Ram(A) = Ram(A')$.*

Hilbert's Reciprocity Law implies the following theorem about the ramification set of a quaternion algebra over a number field:

Since arithmetic Fuchsian groups are defined over totally real fields k, this implies $|Ram_\infty(A)| = n - 1$, where $|k : \mathbb{Q}| = n$.

1.3.1 Number of Conjugacy Classes

The number of $PGL_2(\mathbb{R})$-conjugacy classes of arithmetic groups will depend on the Galois monomorphisms of the field k and the number of conjugacy classes of maximal orders of the quaternion algebra A. We will be concerned with $PGL_2(\mathbb{R})$-conjugacy classes here, so unless otherwise mentioned conjugacy class should be interpreted as $PGL_2(\mathbb{R})$-conjugacy class.

For a maximal order $\mathcal{O}$, the arithmetic group $\Gamma^+_{\mathcal{O}}$ is defined by

$$\Gamma^+_{\mathcal{O}} = \{x \in A^* | x\mathcal{O}x^{-1} = \mathcal{O}\}.$$

Let $\mathcal{O}$ and $\mathcal{O}'$ be two maximal orders in quaternion algebras A/k and A'/k', respectively. If the groups $\Gamma^+_{\mathcal{O}}$ and $\Gamma^+_{\mathcal{O}'}$ are conjugate, then k and k' are isomorphic and

$$x\Gamma^1_{\mathcal{O}}x^{-1} = \Gamma^1_{\mathcal{O}'}.$$

Theorem 1.3.4. *([21]) The groups $\Gamma^1_{\mathcal{O}}$ and $\Gamma^1_{\mathcal{O}'}$ are conjugate if and only if there exists a $\mathbb{Q}$-isomorphism τ such that $\tau(A) = A'$ and $\mathcal{O}' = \tau(a\mathcal{O}a^{-1})$ with $a \in A$.*

The number of conjugacy classes of maximal orders in a quaternion algebra A is finite and is called the *type number* of A. We will denote the type number of a quaternion algebra A by $t = t(A)$. It is the order of a certain quotient of a ray class group group defined over the number field k with modulus equal to the set of places at which A is ramified. Let $k^*_\infty = \{x \in k | \sigma(k) > 0 \text{ for all } \sigma \in \Delta(A)\}$. Then

$$t = \left| \frac{I_k}{I_k^2 D P_{k,\infty}} \right|, \tag{1.5}$$

where I_k is the group of fraction ideals, D is the subgroup generated by all prime ideals dividing the discriminant $\Delta(A)$, and $P_{k,\infty}$ is the group of principal ideals with generator in k^*_∞.

We remark that t divides

$$h_\infty = \frac{h2^{n-1}}{|R_k^* : R_k^* \cap k^*_\infty|}, \tag{1.6}$$

where h is the class number of k and R_k^* is the group of units of R_k. In many cases, $h_\infty = 1$, and we will use this to show that $t = 1$. Moreover, if $Ram_f(A) = \emptyset$, then $D = R_k$ implies $t = h_\infty$.

1.3.2 Torsion in Arithmetic Fuchsian Groups

Throughout this section and the remainder of the text, we will denote a primitive m-th root of unity by ζ_m. The existence of torsion in an arithmetic group $\Gamma^1_{\mathcal{O}}$ defined over a number field k depends primarily on the subfields of k and the existence of embeddings of suitable quadratic extensions of k into the invariant quaternion algebra A.

There are a number of results on the existence of torsion in arithmetic Fuchsian groups which we will use extensively in our calculations.

One can employ the following general theorem ([18]) to detemine the existence of torsion in $\Gamma^1_{\mathcal{O}}$:

Theorem 1.3.5. *Let A be a quaternion algebra over a number field k and let $\ell|k$ be a quadratic extension. Then ℓ embeds in A if and only if $\ell \otimes_k k_v$ is a field for each $v \in Ram_f(A)$.*

Corollary 1.3.6. *Let A be a quaternion algebra over a number field k and suppose $|k(\zeta_m) : k| = 2$. Then if there exists a prime $\mathcal{P} \in Ram_f(A)$ such that $\mathcal{P}$ splits in $k(\zeta_m)|k$, then the unit group $\Gamma^1_{\mathcal{O}}$ of a maximal order $\mathcal{O}$ will contain no elements of order m.*

Proof. If $\mathcal{P} \in Ram_f(A)$ splits in $k(\zeta_m)|k$, then $\ell \otimes_k k_v$ has zero divisors and hence ℓ does not embed in A by the above theorem. □

The following theorem of Chinburg and Friedman can also be used to determine the existence of torsion in an arithmetic group $\Gamma^1_{\mathcal{O}}$:

Theorem 1.3.7. *([3]) Let k be a number field and A a quaternion division algebra over k such that there is at least one infinite place of k at which A is unramified. Let Ω be a commutative R_k-order whose field of quotients $\mathcal{L}$ is a* *quadratic extension of k such that $\mathcal{L} \subset A$. Then every maximal order in A contains a conjugate of Ω except possibly when the following conditions both hold:*

(a) $\mathcal{L}$ and A are unramified at all finite places and ramified at exactly the same set of real places of k,

(b) all prime ideals $\mathcal{P}$ dividing the relative discriminant ideal $d_{\Omega|R_k}$ of Ω is split in $\mathcal{L}|k$.

In number fields k whose extensions of $\mathbb{Q}$ are of odd degree, there exists quaternion algebras A with $Ram_f(A) = \emptyset$. In this case, we have the following result about elements of order m in the group $\Gamma^1_{\mathcal{O}}$:

Lemma 1.3.8. *Let k be a totally real number field. Then every maximal order in a quaternion algebra A ramified at all but one real place over a totally real field and with $Ram_f(A) = \emptyset$ will contain elements of order m provided $\mathbb{Q}(\cos(2\pi/m)) \subset k$.*

Proof. Let ζ_m be a primitive m-th root of unity and suppose $\mathbb{Q}(\cos(2\pi/m)) \subset k$. Let $k(\lambda)$ be a quadratic extension of k where λ satisfies

$$x^2 - (\pm 2\cos(2\pi/m))x + 1 = 0.$$

Then $k(\zeta_m)$ is a quadratic extension of k and embeds in A as $k(\lambda)$. Since $k(\zeta_m)$ is a totally imaginary extension of $\mathbb{Q}$, all real places of k are ramified in $k(\zeta_m)|k$. Hence, condition (a) of the above theorem fails. Therefore, all maximal orders of A will contain elements of orders m. □

If a maximal order $\mathcal{O}$ in A contains elements of finite order, then we can calculate the number of conjugacy classes, a_m, of maximal cyclic subgroups of order m in $\Gamma^1_{\mathcal{O}}$, provided $\{1, \zeta_m\}$, where $\zeta_m = e^{2\pi i/m}$, is a relative integral basis for the quadratic extension $k(\zeta_m)|k$ ([18]). In this case,

$$a_m = \frac{h(k(\zeta_m))}{h|R^*_{k(\zeta_m)} : R^{*2}_{k(\zeta_m)}|} \Pi_{\mathcal{P}|D(A)} \left(1 - \left(\frac{k(\zeta_m)}{\mathcal{P}}\right)\right), \qquad (1.7)$$

where $h(k(\zeta_m))$ is the class number of $k(\zeta_m)|\mathbb{Q}$, h is the class number of k, and $\left(\frac{k(\zeta_m}{\mathcal{P}}\right)$ is the Artin symbol, which is equal to 1, 0, or -1, according to whether $\mathcal{P}$ splits, ramifies, or is inert, respectively, in the extension $k(\zeta_m)|k$.

In the case k is a totally real field, the relative class number h^- for the extension $k(\zeta_m)|k$ is defined as

$$h^- = \frac{h(k(\zeta_m))}{h(k)} \in \mathbb{Z}$$

(cf. [22] p.38).

In some cases, we can use the following lemma to simplify the above torsion formula:

Lemma 1.3.9. *Let k be a totally real number field. If $h(k(\zeta_m))/h$ is odd, then $|R^*_{k(\zeta_m)} : R^{*2}_{k(\zeta_m)}| = 1$.*

Proof. Both quantities $h(k(\zeta_m))/h$ and $|R^*_{k(\zeta_m)} : R^{*2}_{k(\zeta_m)}|$ depend only on the number field k and, hence, are independent of the quaternion algebra A. Since $|R^*_{k(\zeta_m)} : R^{*2}_{k(\zeta_m)}|$ is a finite 2-group, its order is 2^m, for some non-negative integer m. If $|k : \mathbb{Q}|$ is odd, then let A be a quaternion algebra unramified at all finite places. Since $a_n = \frac{h(k(\zeta_m))}{h|R^*_{k(\zeta_m)}:R^{*2}_{k(\zeta_m)}|} \in \mathbb{Z}$, we must have $|R^*_{k(\zeta_m)} : R^{*2}_{k(\zeta_m)}| = 1$. If $|k' : \mathbb{Q}|$ is even, then let A be the quaternion algebra ramified at a prime $\mathcal{P}$ such that $\mathcal{P}|p$ is ramified in the extension $k|\mathbb{Q}$. Then $\left(1 - \left(\frac{k(\zeta_m}{\mathcal{P}}\right)\right) = 1$ and the argument follows as above . $\square$

We will also make use of the following useful general fact (cf. [17] Ch. 10):

Fact 1.3.10. *Let k be a totally real number field such that d_k is not divisible by 2. Then $\{1, i\}$ is a relative integral basis for $k(i)|k$. Likewise, if d_k is not divisible by 3, then $\{1, \omega\}$ is a relative integral basis for $k(\omega)|k$ (ω is a primitive third root of unity).*

The following lemma will also be helpful in our calculations.

Lemma 1.3.11. *Suppose that k is a totally real number field, and 2 and 3 are unramified in $k|\mathbb{Q}$. Then*

$$|R^*_{k(i)} : R^{*2}_{k(i)}| = |R^*_{k(\omega)} : R^{*2}_{k(\omega)}| = 1 \tag{1.8}$$

The proof of the above lemma uses the following result ([15]):

Theorem 1.3.12. *Let k be a totally real number field, and K a totally imaginary quadratic extension of k. Then every unit ϵ of K has the form $\epsilon = \zeta \cdot \eta$, where ζ is a root of unity with $\zeta^2 \in K$ and η is a real unit with $\eta^2 \in k$.*

Proof of Lemma 1.3.11: Let us first consider the case $k(i)$. Since 2 does not divide the discriminant of k, $\{1, i\}$ is a relative integral basis for the extension $k(i)|k$. Suppose that $\cos(\frac{\pi}{m}) + i\sin(\frac{\pi}{m})$ is a root of unity in $k(i)$. Then, since this is also an algebraic integer, it can be written as $a + bi$, where $a, b \in R_k$. Now, the only solutions of $\cos(\frac{\pi}{m}) + i\sin(\frac{\pi}{m}) = a + bi$ correspond to the units ± 1 and $\pm i$. By Theorem 1.3.12, any unit ϵ of $k(i)$ is of the form $\epsilon = \zeta \cdot \eta$, where $\zeta^2 = \pm 1, \pm i$ and $\eta \in k$ is a real unit. Again, using the relative integral basis, let $\epsilon = a + bi$ for some $a, b \in R_k$. Now, any unit $\epsilon \in k(i)$ must satisfy the equation:

$$\epsilon^2 = \zeta^2\eta^2 = (a + bi)^2 = (a^2 - b^2) + 2abi.$$

In light of Theorem 1.3.12, there are two possible cases to consider:

Case 1: $\pm i\eta^2 = (a^2 - b^2) + 2abi$.

Case 2: $\pm\eta^2 = (a^2 - b^2) + 2abi$.

In Case 1, the solution is $a \pm b$ and $i\eta^2 = \pm 2a^2 i$. Since a is real, this implies $\eta^2 = 2a^2$. But since a is an algebraic integer, $2a^2$ is not a unit. Therefore, no unit ϵ corresponds to this case. In Case 2, either $a = 0$ or $b = 0$. Hence, $\pm\eta^2 = a^2$ or b^2, and since $a, b \in k$, this implies $\pm\eta \in k$. Therefore, the units in $k(i)$ are of the form $\epsilon = \pm i\eta$ and

$$N_{k(i)|k}(\epsilon) = N_{k(i)|k}(\pm\eta) = \eta^2.$$

This means that every unit of $k(i)$ has norm lying in R_k^{*2}, and so

$$|R_{k(i)}^* : R_{k(i)}^{*2}| = 1.$$

The proof for $k(\omega)$ is similar. $\square$

Furthermore, in light of (1.1), if $k_m = \mathbb{Q}(\cos(2\pi/m)) \subset k$, then $|k_m : \mathbb{Q}|$ divides $|k : \mathbb{Q}|$ and d_{k_m} divides d_k. We will use this fact frequently to determine which periods can arise in the various number fields k. With this in mind, we list the discriminants of cyclotomic field $\mathbb{Q}(\zeta_p)$ and its proper subfield $k_p = \mathbb{Q}(\cos(2\pi/p))$ when $p > 3$ is a prime.

Proposition 1.3.13. *Let $p > 3$ be a prime. Then:*

1. $|k_p : \mathbb{Q}| = \frac{p-1}{2}$.
2. $d_{\mathbb{Q}(\zeta_p)} = p^{p-2}$.
3. $d_{k_p} = p^{\frac{p-3}{2}}$.

Proof. This first part follows from the fact that $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$ and k_p is a proper subfield of index 2 corresponding to the fixed field of complex conjugation. The second and third parts can be found in [22] p. 9, p. 28, respectively. □

One can use these facts to determine which number fields contain k_p as a proper subfield since if $k_p \subset k$, then $d_{k_p}^{|k:k_p|}$ divides d_k.

Chapter 2

Classification of Derived Arithmetic Groups of Genus Two

In this chapter, we give a complete list of commensurability classes of derived genus two surface groups by invariant quaternion algebra. First, we list all possible signatures for Fuchsian groups which can contain a surface of genus two. Then we use arithmetic data to determine all groups $\Gamma^1_{\mathcal{O}}$ with one of these signatures.

2.1 Existence of Genus Two Subgroups

The existence of torsion-free subgroups of a given index in a Fuchsian group of any signature is characterized in the following theorem:

Theorem 2.1.1 ([6]). *Let Γ be a finitely generated Fuchsian group with the standard presentation:*

$$< a_1, b_1, \ldots, a_g, b_g, c_1, \ldots c_r, p_1 \ldots, p_s | \prod_{i=1}^{n}[a_i, b_i] \prod_{j=1}^{r} c_j, \prod_{k=1}^{s} p_k, c_1^{m_1}, \ldots, c_r^{m_r} >,$$

Then Γ has a torsion free subgroup of finite index $k \geq 1$ if and only if k is divisible by $2^{\epsilon}\lambda$, where $\lambda = LCM(m_1, \ldots, m_r)$, and $\epsilon = 0$ if Γ has even type, while $\epsilon = 1$ if Γ has odd type. (Γ has odd type if $s = 0$, λ is even, but λ/m_i is odd for exactly an odd number of m_i; otherwise Γ has even type.)

Lemma 2.1.2. *Let Γ be a cocompact Fuchsian group containing a genus two surface group. Then Γ has one of the following signatures:* $(0;2,3,7)$, $(0;2,3,8)$, $(0;2,3,9)$, $(0;2,3,10)$, $(0;2,3,12)$, $(0;2,4,5)$, $(0;2,4,6)$, $(0;2,4,8)$, $(0;2,4,12)$, $(0;2,5,5)$, $(0;2,5,6)$, $(0;2,5,10)$, $(0;2,6,6)$, $(0;2,8,8)$, $(0;3,3,4)$, $(0;3,3,5)$, $(0;3,3,6)$, $(0;3,3,9)$, $(0;3,4,4)$, $(0;3,6,6)$, $(0;4,4,4)$, $(0;5,5,5)$, $(0;2,2,2,3)$, $(0;2,2,2,4)$, $(0;2,2,2,6)$, $(0;2,2,3,3)$, $(0;2,2,4,4)$, $(0;3,3,3,3)$, $(0;2,2,2,2,2)$, $(0;2,2,2,2,2,2)$, $(1;2)$, $(1;3)$, *or* $(1;2,2)$.

Proof. If Γ_1 is a genus two surface subgroup of Γ, then $N\mu(\Gamma) = \mu(\Gamma_1) = 4\pi$, where $N = |\Gamma : \Gamma_1|$. This implies $\mu(\Gamma^1_{\mathcal{O}}) \leq 4\pi$. In particular, the genus g of Γ must be less than or equal to 2. Furthermore, by Theorem 2.1.1, $\lambda = LCM(m_1, \dots, m_r)$ divides the index N. This gives us bounds on the possible torsion of Γ. In particular, for fixed g, this gives us an upper bound on the number of conjugacy classes of elliptic elements.:

(1) If $g = 0$, then Γ has at most six conjugacy classes of elliptic elements.

(2) If $g = 1$, then Γ has at most two conjugacy classes of elliptic elements.

(3) If $g = 2$, then Γ has no elliptic elements and $\Gamma = \Gamma_1$.

For example, suppose $g = 0$ and Γ has four conjugacy classes of elliptic elements x_i of order m_i, $1 \leq i \leq 4$. By the Riemann-Hurwitz formula (1.3),

$$\mu(\Gamma) = 2\pi(-2 + \sum_{i=1}^{4} \frac{m_i - 1}{m_i}).$$

Therefore, if Γ contains a torsion-free subgroup of genus two, then

$$N\mu(\Gamma) = 2n\pi(-2 + \sum_{i=1}^{4} \frac{m_i - 1}{m_i}) = 4\pi = \mu(\Gamma_1).$$

This translates to the existence of integers N, m_i, $1 \leq i \leq 4$ satisfying the equation:

$$\sum_{i=1}^{4} \frac{m_i - 1}{m_i} = \frac{2}{N} + 2, \tag{2.1}$$

where in addition, $\lambda = LCM(m_1, \ldots, m_4)$ divides N. Since $\mu(\Gamma) > 0$, there exists at least one x_i with order $m_i > 2$. Also, we can deduce the following:

(i) There cannot exist more than two distinct m_i corresponding to the x_i,

(ii) If $m_i > 2$ for all $1 \leq i \leq 4$, then $m_1 = \cdots = m_4 = 3$.

This is due to the fact that, in both these cases, $N > \lambda \geq 12$ and this gives the contradiction:

$$\frac{29}{12} \leq \sum_{i=1}^{4} \frac{m_i - 1}{m_i} = \frac{2}{N} + 2 \leq \frac{26}{12}.$$

W.l.o.g, suppose $x_1 \leq x_2 \leq \cdots \leq x_4$.

Case 1: $m_1 = m_2 = m_3 = 2$ and $m_4 = m > 2$.

In this case, equation (2.1) becomes

$$\frac{3}{2} + \frac{m-1}{m} = \frac{2}{N} + 2 \Longleftrightarrow \frac{m-1}{m} = \frac{2}{N} + \frac{1}{2}.$$

The solution $m = N = 6$ gives the maximal value of m. The only other solutions in this case occur when $(m, N) = (3, 12), (4, 8)$.

Case 2: $m_1 = m_2 = 2$ and $m = m_3 = m_4 > 2$.

Again, equation (2.1) translates to

$$1 + \frac{2(m-1)}{m} = \frac{2}{N} + 2 \Longleftrightarrow \frac{2(m-1)}{m} = \frac{2}{N} + 1.$$

Again, the case $m = N$ gives the maximal value for m and this occurs when $m = N = 4$. The only other possible solution occurs when $(m, N) = (3, 6)$.

Case 3: $m_1 = 2$ and $m = m_2 = m_3 = m_4 > 2$.

Again, equation (2.1) translates to

$$\frac{1}{2} + \frac{3(m-1)}{m} = \frac{2}{N} + 2;$$

and one checks that there exist no integer solutions to this equation.

Case 4: $m = m_1 = m_2 = m_3 = m_4 > 2$.

In this situation,

$$\frac{4(m-1)}{m} = \frac{2}{N} + 2,$$

and $m = N = 3$ is the only solution. The existence of a torsion-free subgroup of index N for the solutions obtained in each of these case is guaranteed by Theorem 2.1.1. Therefore, the only Fuchsian group of signature $(0; x_1, x_2, x_3, x_4)$ containing a torsion-free subgroup of genus 2 are $(0; 2, 2, 2, 3)$, $(0; 2, 2, 2, 4)$, $(0; 2, 2, 2, 6)$, $(0; 2, 2, 3, 3)$, $(0; 2, 2, 4, 4)$, and $(0; 3, 3, 3, 3)$. In this manner, we analyze torsion in groups of a fixed signature to obtain the list in the Lemma. □

Proposition 2.1.3. *There exist no derived torsion-free genus two groups arising from quaternion algebras over number fields of degree greater than 5.*

Proof. If $\Gamma^1_{\mathcal{O}}$ contains a genus two surface group Γ of index $M = |\Gamma^1_{\mathcal{O}} : \Gamma|$, then

$$\mu(\Gamma) = 4\pi = M\mu(\Gamma^1_{\mathcal{O}}) = N\frac{8\pi d_k^{3/2}\zeta_k(2)\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{(4\pi^2)^{|k:\mathbb{Q}|}}. \tag{2.2}$$

In particular, this implies

$$4\pi \geq \frac{8\pi d_k^{3/2}\zeta_k(2)\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{(4\pi^2)^{|k:\mathbb{Q}|}}. \tag{2.3}$$

Note that

$$\zeta_k(2)\prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1) > \prod_{\mathcal{P}|\Delta(A)}\frac{(N(\mathcal{P}))^2}{(N(\mathcal{P})+1)} \geq \begin{cases} 1 & \text{if } |k:\mathbb{Q}| \text{ is odd} \\ 4/3 & \text{if } |k:\mathbb{Q}| \text{ is even} \end{cases}. \tag{2.4}$$

Using $\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1) \geq 1$ and $\zeta_k(2) \geq 1$ in the above inequality gives

$$4\pi \geq \frac{8\pi d_k^{3/2}}{(4\pi^2)^{|k:\mathbb{Q}|}} \tag{2.5}$$

We now use Odlyzko's lower bounds on the discriminant of a number field to get an upper bound on the degree of k:

$$|d_k| \geq A^{n-2}B^2e^{-E},$$

where $n = |k:\mathbb{Q}|, A = 24.987, B = 13.157$, and $E = 6.9934$ for all n. Using these estimates in inequality (2.3) gives that $n \leq 8$. However, in degrees $n = 7$ and 8, the smallest discriminants of a totally real field are 20,134,393 and 282,300,416, respectively ([4] and [16]). In each case, inequality (2.5) is violated:

$$4\pi \geq \frac{8\pi d_k^{3/2}}{(4\pi^2)^{|k:\mathbb{Q}|}} \geq \begin{cases} \frac{8\pi(20134393)^{3/2}}{(4\pi^2)^7} \sim 15.1925 > 4\pi \\ \frac{8\pi(282300416)^{3/2}}{(4\pi^2)^8} \sim 20.2036 > 4\pi \end{cases}$$

Hence, there cannot exist derived groups of genus two for $n \geq 7$.

To eliminate the case $[k:\mathbb{Q}] = 6$, we again exploit the area formula (1.4) and inequality (2.4) to the following inequality:

$$\mu(\Gamma) = 4\pi \geq |\Gamma^1_{\mathcal{O}}:\Gamma|\frac{8\pi d_k^{3/2}\zeta_k(2)\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{(4\pi^2)^6} \geq \frac{32\pi d_k^{3/2}}{3(4\pi^2)^6}.$$

This gives us the following upper bound on the discriminant d_k:

$$d_k \leq \left(\frac{3(4\pi^2)^6}{8}\right)^{2/3} < 1263165. \tag{2.6}$$

According to the lists from [4], there are 20 number fields k of degree 6 satisfying the above inequality (see Appendix A). For each field k, we investigate the behavior of small primes and/or estimate $\zeta_k(2)$ using Pari. Since $n = 6$, we must have that $|Ram_f(A)| \neq \emptyset$. Therefore, $\Pi_{\mathcal{P}|\Delta(A)}(N(\mathcal{P}) - 1) \geq N(\mathcal{P}_0) - 1$, where $\mathcal{P}_0$ is the prime of smallest of norm in k.

For example, consider the totally real field k of degree 6 and discriminant $d_k = 722000$. The minimal polynomial for k is $f(x) = x^6 - x^5 - 6x^4 + 7x^3 + 4x^2 - 5x + 1$. By Pari, we find that the prime of smallest norm in R_k is the unique prime $\mathcal{P}$ lying over 2 with $N(\mathcal{P}) = 4$. This implies that any group $\Gamma^1_{\mathcal{O}}$ defined over k has volume at least

$$\frac{8\pi d_k^{3/2}\zeta_k(2)\cdot 3}{(4\pi^2)^6} = \frac{21\pi}{5} > 4\pi.$$

Hence, there exist no derived genus two surface groups defined over the number field k. In this fashion, we obtain a contradiction to the inequality $\mu(\Gamma) \leq 4\pi$ for each totally real field k satisfying (2.6). □

2.2 Classification by Invariant Quaternion Algebra

Johansson ([8]) has determined the signatures of all derived arithmetic groups arising from quaternion algebras over number fields of degree less than or equal to 2, so we will be concerned with fields of degree $|k : \mathbb{Q}| > 2$. Combining Lemma 2.1.2 and our results with the relevant results in [8],[12], and [19], we obtain following theorem.

Theorem 2.2.1. *The following is a complete list of all $\Gamma^1_{\mathcal{O}}$ containing a derived genus two surface group Γ arising from quaternion algebras over totally real number fields. We also list the number of conjugacy classes c of the groups $\Gamma^1_{\mathcal{O}}$ for each case.*

$[k:\mathbb{Q}]$	d_k	$\Delta(A)$	$\|\Gamma^1_{\mathcal{O}}:\Gamma\|$	$\Gamma^1_{\mathcal{O}}$	c
1	1	$2\cdot 3$	6	(0;2,2,3,3)	1
1	1	$2\cdot 5$	3	(0;3,3,3,3)	1
1	1	$2\cdot 7$	2	(1;2,2)	1
1	1	$2\cdot 13$	1	(2;0)	1
2	5	$\mathcal{P}_2$	20	(0;2,5,5)	1
2	5	$\mathcal{P}_5$	15	(0;3,3,5)	1
2	5	$\mathcal{P}_{11}$	6	(0;2,2,3,3)	1
2	5	$\mathcal{P}'_{11}$	6	(0;2,2,3,3)	1
2	5	$\mathcal{P}_{31}$	2	(1;2,2)	1
2	5	$\mathcal{P}'_{31}$	2	(1;2,2)	1
2	5	$\mathcal{P}_{61}$	1	(2;0)	1
2	5	$\mathcal{P}'_{61}$	1	(2;0)	1
2	8	$\mathcal{P}_2$	24	(0;3,3,4)	1
2	8	$\mathcal{P}_5$	1	(2;0)	1
2	12	$\mathcal{P}_2$	12	(0;3,3,6)	1
2	12	$\mathcal{P}_3$	6	(0;2,2,2,6)	1
2	12	$\mathcal{P}_{13}$	1	(2;0)	1
2	12	$\mathcal{P}'_{13}$	1	(2;0)	1
2	13	$\mathcal{P}_{13}$	1	(2;0)	1
2	17	$\mathcal{P}_2$	6	(0;2,2,3,3)	1
2	17	$\mathcal{P}'_2$	6	(0;2,2,3,3)	1
2	24	$\mathcal{P}_3$	2	(0;2,2,2,2,2,2)	1
2	28	$\mathcal{P}_2$	3	(0;3,3,3,3)	1

$[k:\mathbb{Q}]$	d_k	$\Delta(A)$	$\lvert\Gamma^1_{\mathcal{O}}:\Gamma\rvert$	$\Gamma^1_{\mathcal{O}}$	c
3	49	$\mathcal{P}_2\mathcal{P}_7$	2	(1;2,2)	1
3	49	$\emptyset$	84	(0;2,3,7)	1
3	81	$\emptyset$	36	(0;2,3,9)	1
3	148	$\mathcal{P}_2\mathcal{P}_{13}$	1	(2;0)	3
3	148	$\mathcal{P}_2\mathcal{P}_5$	3	(0;3,3,3,3)	3
3	148	$\emptyset$	12	(0;2,2,2,3)	3
3	169	$\emptyset$	12	(0;2,2,2,3)	1
3	229	$\emptyset$	6	(0;2,2,3,3)	4
3	229	$\mathcal{P}_2$,$\mathcal{P}'_2$	2	(1;2,2)	3
3	257	$\emptyset$	6	(0;2,2,3,3)	4
3	316	$\mathcal{P}_2$,$\mathcal{P}'_2$	3	(0;3,3,3,3)	3
4	725	$\mathcal{P}_{61}$	1	(2;0)	2
4	725	$\mathcal{P}'_{61}$	1	(2;0)	2
4	725	$\mathcal{P}_{31}$	2	(1;2,2)	2
4	725	$\mathcal{P}'_{31}$	2	(1;2,2)	2
4	725	$\mathcal{P}_2$	4	(1;2)	2
4	725	$\mathcal{P}_{11}$	6	(0;2,2,3,3)	2
4	725	$\mathcal{P}'_{11}$	6	(0;2,2,3,3)	2
4	1125	$\mathcal{P}_2$	2	(1;2,2)	1
4	1957	$\mathcal{P}_7$	2	(1;2,2)	4
4	1957	$\mathcal{P}_3$	6	(0;2,2,3,3)	4
4	2000	$\mathcal{P}_5$	2	(0;3,3,3,3)	2
4	2304	$\mathcal{P}_3$	1	(2;0)	1
4	2777	$\mathcal{P}_2$	6	(0;2,2,3,3)	1
4	3981	$\mathcal{P}_3$	2	(0;2,2,2,2,2,2)	4
4	4352	$\mathcal{P}_2$	6	(0;3,3,3,3)	1
4	4752	$\mathcal{P}_2$	1	(2;0)	2
5	24217	$\emptyset$	12	(0;2,2,2,3)	5
5	36497	$\emptyset$	6	(0;2,2,3,3)	6
5	38569	$\emptyset$	6	(0;2,2,3,3)	6

Remark 2.2.2. *Using a theorem of Greenberg ([7]) on maximal Fuchsian groups in conjunction with the results in ([12]),([19]),and ([20])), all the conjugacy classes for the groups $\Gamma^1_{\mathcal{O}}$ listed above are known except for those with signatures* $(1;2,2)$, $(0;2,2,2,2,2,2)$, *and* $(2;0)$.

Before beginning the proof of Theorem 2.2.1, we need the following lemma:

Lemma 2.2.3. *If A is a quaternion algebra defined over a totally real field ramified at all but one infinite place and unramified at all finite places, then $\Gamma^1_{\mathcal{O}}$ contains elements of orders 2 and 3. Furthermore, if $Ram_f(A) = \emptyset$, and Γ is a genus two surface group contained in $\Gamma^1_{\mathcal{O}}$ for a $\mathcal{O}$ a maximal order in A, then* $6 || \Gamma^1_{\mathcal{O}} : \Gamma|$.

Proof. Since $Ram_f(A)$ is empty, by Lemma 1.3.8, there is no obstruction to embedding $\mathcal{L}$ in $\mathcal{O}$, where $\mathcal{L} \cong \mathbb{Q}(\mathrm{i}), \mathbb{Q}(\omega)$ (where ω is a primitive third root of unity). Therefore, any order $\mathcal{O}$ in A will contain elements of orders 2 and 3. By Theorem 2.1.1, if $\Gamma^1_{\mathcal{O}}$ has signature $(g; x_1, \ldots, x_r)$ and $\Gamma \subset \Gamma^1_{\mathcal{O}}$ is torsion-free, then 6 divides λ which divides $|\Gamma^1_{\mathcal{O}} : \Gamma|$. □

This lemma will be particularly useful in the case $|k : \mathbb{Q}|$ odd, since $Ram_f(A) = \emptyset$ is a possibility in this case.

The proof of Theorem 2.2.1 is an exhaustive one. Rather than go through an analysis of each number field that can possibly correspond to an arithmetic group of one of the signatures $(1; 2, 2)$, $(0; 2, 2, 2, 2, 2, 2)$, or $(2; 0)$, we give an idea of the overall approach by giving a few illustrative examples.

2.3 Proof of Theorem 2.2.1.

The proof is organized by the degree of the number field.

2.3.1 Quintic Number Fields

Lemma 2.3.1. *For* $|k : \mathbb{Q}| = 5$*, the only derived groups of of signature* $(2; 0)$ *arise from quaternion algebras over the totally real fields of discriminants* $d_k = 38569$*,* 36497*, and* 24217*.*

Proof. Suppose there exists derived arithmetic group $\Gamma < \Gamma^1_{\mathcal{O}}$ of genus two which is defined over the number field k. Using $\zeta_k(2) \geq 1, \prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1) \geq 1$ in (1.4) we get that

$$d_k \leq 131981.$$

However, if $Ram_f(A) = \emptyset$, the index $M = [\Gamma^1_{\mathcal{O}} : \Gamma] \geq 6$ by the Lemma 2.2.3. Substituting back into the area formula (1.4) gives $d_k \leq 39970$. Thus, for those fields with $39970 \leq d_k \leq 131981$, we analyze the behavior of small primes in k to determine which ramifications sets are possible for each field k. According to the lists [4], there are 15 number fields with $d_k < 131981$ (see Appendix A). In a few cases, small primes do exist, but we can investigate torsion to eliminate these cases.

For example, let k be the number field with discriminant $d_k = 106069$. Using the minimal polynomial $f(x) = x^5 - 2x^4 - 4x^3 + 7x^2 + 3x - 4$ in Pari, we compute that

$$\frac{8\pi 106069^{3/2}\zeta_k(2)}{(4\pi^2)^5} = 4\pi.$$

Furthermore, there exists a unique prime $\mathcal{P}_2$ of norm 2 in R_k. Therefore, if we take a quaternion algebra A ramified at all but one infinite place and at the prime $\mathcal{P}_2$, then for a maximal order $\mathcal{O}$ in A, $\mu(\Gamma^1_{\mathcal{O}}) = 4\pi$. However, by the torsion formula (1.7), $a_3 \neq 0$ here since $\mathcal{P}_2$ is inert in $k(\omega)|k$. Hence, $\Gamma^1_{\mathcal{O}}$ is not torsion-free, and since $\mu(\Gamma^1_{\mathcal{O}}) = 4\pi$, it cannot contain a genus two group.

The case $d_k = 38569$ yields a positive result. By Pari, using the minimal polynomial $f(x) = x^5 - 5x^3 + 4x - 1$ for k, we find that

$$\frac{8\pi 38569^{3/2}\zeta_k(2)}{(4\pi^2)^5} = \frac{2\pi}{3}.$$

So if $\Gamma \subset \Gamma^1_{\mathcal{O}}$ has signature $(2;0)$, then the following equation must be satisfied:

$$4\pi = \mu(\Gamma) = M\mu(\Gamma^1_{\mathcal{O}}) = M\frac{2\pi \prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P}) - 1)}{3}, \tag{2.7}$$

where $M = |\Gamma^1_{\mathcal{O}} : \Gamma|$.

The only solution to this equation occurs if $M = 6$, and $Ram_f = \emptyset$. Since $d_k = 38569$ is prime, by (1.1), k contains no proper subfields other than $\mathbb{Q}$. Thus, the only possibilities for elements of finite order in $\mathcal{O}$ are 2 and 3. By Lemma 2.2.3, any group $\Gamma^1_{\mathcal{O}}$ contains elements of orders 2 and 3. So, in this case we get

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{2\pi}{3} = 2\pi\left(2g - 2 + \frac{a_2}{2} + \frac{2a_3}{3}\right).$$

We see that the only solution to this equation is $a_2 = a_3 = 2$. Hence, $\Gamma^1_{\mathcal{O}}$ has signature $(0;2,2,3,3)$ in this case. Furthermore, Theorem 2.1.1 guarantees the existence of a torsion-free subgroup of index 6.

The fields with discriminants $d_k = 36497, 24217$ are the only other number fields yielding positive results. □

2.3.2 Quartic Number Fields

For $[k : \mathbb{Q}] = 3, 4$, there are more possibilities for torsion. This complicates matters slightly, but in many cases, we can still use Theorem 1.7 to determine the signature of $\Gamma^1_{\mathcal{O}}$.

For $|k : \mathbb{Q}| = 4$, we must have $Ram_f \neq \emptyset$. However, there are more possibilities for torsion as we now show.

Lemma 2.3.2. *Let k be a totally real number field with $|k : \mathbb{Q}| = 4$ and denote by k_m the field $\mathbb{Q}(\cos(\frac{2\pi}{m}))$. Then $|k_m : \mathbb{Q}|$ has degree dividing 4 for the following values of m: 2,3,4,5,6,8,10,12,15.*

Proof. The periods 2 and 3 are always possible since $\mathbb{Q}$ is a proper subfield of k. The quadratic fields $k_4 = \mathbb{Q}(\sqrt{2})$, $k_5 = \mathbb{Q}(\sqrt{5})$, $k_6 = \mathbb{Q}(\sqrt{3})$ can be possible proper subfields of k, which yield $4, 5, 6$. We examine the cyclotomic fields ζ_m denote a primitive m-th root of unity for which $|\mathbb{Q}(\zeta_m) : \mathbb{Q}| = 4, 8$. If m is odd, then k_m will be a proper subfield of index two, $|k_m : \mathbb{Q}| = 4$. If m is even, we need to account for the fact that $-\mathrm{Id} \sim \mathrm{Id}$ in $PSL_2(\mathbb{R})$; this means $|k_m : \mathbb{Q}| = \deg\Phi_m$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial. By Prop. 1.3.13, there are no rational primes p with $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = 4$. If m is a prime power p^k, then $\deg\Phi = p^{k-1}(p-1) = 4$. The only solution in this case occurs when $p = 2$ and $k = 3$ and, hence, 8 is a possible period. If $m = p_1^{k_1} \cdots p_r^{k_1}$, then $\deg\Phi_m = p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)$. Analyzing solutions to this equation when $\deg\Phi_m = 4, 8$ yield the periods 10,12,15. This completes the proof of the lemma. $\square$

Using equation 2.2 in conjuction with inequality (2.4), we obtain the following inequality when $|k : \mathbb{Q}| = 4$:

$$4\pi \geq \frac{32\pi d_k^{3/2}}{3(4\pi^2)^4}.$$

Therefore,

$$d_k \leq \left(\frac{3(4\pi^2)^4}{8}\right)^{2/3} < 9397.$$

There are 48 number fields with discriminants satisfying the above inequality on the lists from [4]. We list these number fields in Appendix A. Again, we eliminate all fields except those listed in Theorem 2.2.1 by estimating $\zeta_k(2)$ and examining the factorization of small primes using Pari.

Lemma 2.3.3. *There exist no derived genus two groups defined over the totally real field k with $d_k = 5744$.*

Proof. The minimal polynomial for k is $f(x) = x^4 - 5x^2 - 2x + 1$. Using Pari, we compute that

$$\frac{8\pi 5744^{3/2}\zeta_k(2)}{(4\pi^2)^4} = \frac{5\pi}{3}.$$

Hence, a genus torsion-free genus two subgroup Γ of index $M = |\Gamma^1_{\mathcal{O}} : \Gamma|$ corresponds to a solution of the equation

$$\frac{5M}{3}\prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1) = 4.$$

But as $M, N(\mathcal{P}) \in \mathbb{Z}$, this clearly has no solution. □

We now list some positive results for the case $|k : \mathbb{Q}| = 4$.

Lemma 2.3.4. *Let k be the totally real number field with $d_k = 3981$. Then the only derived arithmetic group of signature $(2;0)$ defined over k arises from the quaternion algebra A with $Ram_f(A) = \mathcal{P}_3$, where $\mathcal{P}_3$ is the unique prime in k lying over 3. Furthermore, there is only one conjugacy class of derived groups of this signature over k.*

Proof. The number field k is equal to $\mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(x) = x^4 - x^3 - 4x^2 + 2x + 1$. Since $d_k = 3 \cdot 1327$, k contains no other proper subfield other than $\mathbb{Q}$; the only possible non-trivial elements of finite order of $\Gamma^1_{\mathcal{O}}$ are those of order 2 or 3. By Pari, we compute

$$\frac{8\pi 3981^{3/2}\zeta_k(2)}{(4\pi^2)^4} = \pi.$$

Therefore, if there exists a subgroup Γ of signature $(2;0)$ of index $M = |\Gamma^1_{\mathcal{O}} : \Gamma|$, then

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 4. \tag{2.8}$$

This implies that $N(\mathcal{P}) \leq 5$ for any prime $\mathcal{P} \in Ram_f(A)$. By Pari, we find that there are only two primes in R_k with norm less than 5: $\mathcal{P}_3$ and $\mathcal{P}_5$ with $N(\mathcal{P}_3) = 3$ and $N(\mathcal{P}_5) = 5$.

Now, $M = 1, Ram_f(A) = \{\mathcal{P}_5\}$ is a possible solution to (2.8). However, $\mathcal{P}_5$ is inert in $k(\omega)|k$, hence $a_3 \neq 0$. By (2.1.1), $3|M = 1$, and this gives a contradiction.

We also have $M = 2$ and $Ram_f(A) = \{\mathcal{P}_3\}$ as a possible solution to (2.8). Furthermore, $6 \nmid d_k$, so by Lemma 1.3.10 we can calculate $a_2 = 6$ and $a_3 = 0$ using (1.7). Since these are the only possible periods for this number field, $\Gamma^1_{\mathcal{O}}$ must have signature $(0; 2, 2, 2, 2, 2, 2)$; finally, $\Gamma^1_{\mathcal{O}}$ contains a torsion free subgroup Γ of index 2 by Theorem 2.1.1 and since $\mathrm{vol}(\Gamma) = 4\pi$, Γ has signature $(2;0)$.

Since the extension $k|\mathbb{Q}$ is not Galois and k contains no proper subfields other than $\mathbb{Q}$, the groups corresponding to the various Galois monomorphisms each contribute at least one conjugacy class. For each of these quaternion algebras, we determine the type number by analyzing the embeddings of the units. By Pari, a fundamental system of R_k^* is $\{-1, \alpha, \alpha - 1, \alpha^2 + \alpha - 1\}$. The signs of these generators at the various embeddings are shown in the table below:

	α	$\alpha - 1$	$\alpha^2 + \alpha - 1$
$\alpha_1 \sim -1.7508$	$-$	$-$	$+$
$\alpha_2 \sim -0.3184$	$-$	$-$	$-$
$\alpha_3 \sim 0.7853$	$+$	$-$	$+$
$\alpha_4 \sim 2.2840$	$+$	$+$	$+$

For each choice of unramified real place σ_i, $h_\infty = 1$. Hence, there are four distinct conjugacy classes of groups of signature $(0; 2, 2, 2, 2, 2, 2)$ defined over this particular k. □

Lemma 2.3.5. *Let $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be the number field with $d_k = 2304$. The only derived arithmetic group of signature $(2; 0)$ arising from a quaternion algebra A over k has $Ram_f(A) = \mathcal{P}_3$ where $\mathcal{P}_3$ is the unique prime of norm 9 in k.*

Proof. The periods 2,3,4,6,12 are all obvious possibilities for torsion since $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ are proper subfields of k. By Lemma. 2.3.2 and using the fact that $5 \nmid 2304 = 2^8 \cdot 3^2$, these are the only possibilities. In this case, the $k = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $f(x) = x^4 - 4x^2 + 1$. Using Pari, we compute that

$$\frac{8\pi 2304^{3/2}\zeta_k(2)}{(4\pi^2)^4} = \frac{\pi}{2}.$$

Therefore, the existence of a torsion-free genus two subgroup amounts to the solution of the equation

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 8. \tag{2.9}$$

The only primes $\mathcal{P}$ with $(N(\mathcal{P}) - 1)$ dividing 8 are the unique primes $\mathcal{P}_2$ and $\mathcal{P}_3$ of norms 2 and 9, respectively. Since $|Ram_f(A)|$ is odd, the only solution to (2.9) is $M = 1$ and $Ram_f(A) = \{\mathcal{P}_3\}$. Since $\mathcal{P}_3$ is inert in both $k(i)|k$ and $k(\omega)|k$, for any maximal order $\mathcal{O}$, $\Gamma^1_{\mathcal{O}}$ will contain no elements of orders 2 or

3 by Theorem 1.3.6. This also implies $\Gamma^1_{\mathcal{O}}$ contains no elements of order 4,6, or 12; therefore, $\Gamma^1_{\mathcal{O}}$ is torsion-free and has therefore has genus 2. Since $k|\mathbb{Q}$ is Galois, there is only one conjugacy class of arithmetic groups $\Gamma^1_{\mathcal{O}}$ defined over k. □

Lemma 2.3.6. *Let k be the number field with $d_k = 1957$. Then the only derived arithmetic groups of signature $(2;0)$ arising from a quaternion algebra A over k containing genus two subgroups are those listed in Theorem 2.2.1.*

Proof. The number field k with discriminant d_k is equal to $\mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(x) = x^4 - 4x^2 - x + 1$. Furthermore, since $d_k = 1957 = 19 \cdot 103$, k contains no proper subfields other than $\mathbb{Q}$. Using Pari, we compute that

$$\frac{8\pi 1957^{3/2}\zeta_k(2)}{(4\pi^{2)^4}} = \frac{\pi}{3}.$$

Again, we consider solutions to the equation

$$4\pi = M\frac{\pi \prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P}) - 1)}{3},$$

or equivalently,

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 12, \tag{2.10}$$

by analyzing the primes in R_k. In particular, any prime $\mathcal{P}$ in the ramification set of A has norm at most 13. The rational primes 2,5, and 13 remain prime in the extension $k|\mathbb{Q}$, so they cannot lie in $Ram_f(A)$. By Pari, there are two primes $\mathcal{P}_3 = (3, 1 + \alpha)R_k$ and $\mathcal{P}_3'$ lying over 3, with norms $N(\mathcal{P}_3) = 3$ and $N(\mathcal{P}_3') = 9$. Also, we check that $N(\alpha - 2) = 3$ by Pari, so that $\mathcal{P}_3 = (\alpha - 2)R_k$. Similarly, there exists a prime $\mathcal{P}_7 = (7, 4 + \alpha)R_k = (2\alpha + 1)R_k$ of norm 7. Coupling this with the fact that $|Ram_f(A)|$ is odd, we get that the only possible solutions $(M, Ram_f(A))$ to the above equation are: $(6, \mathcal{P}_3)$ and $(2, \mathcal{P}_7)$. The quaternion algebras with $Ram_f(A) = \{\mathcal{P}_3\}$ appear in the lists of [12] and the unit groups $\Gamma^1_{\mathcal{O}}$ are of signature $(0; 2, 2, 2, 3)$ in this case.

Let us consider the algebra with $Ram_f(A) = \{\mathcal{P}_7\}$. Since $6 \nmid 1957$ and k contains no other proper subfields other than $\mathbb{Q}$, $\Gamma^1_{\mathcal{O}}$ can only have elements of orders 2 and 3 and we can compute the number of elements of orders 2 and 3 using formula (1.7). Since $\mathcal{P}_7$ splits in $k(\omega)|k$, $\Gamma^1_{\mathcal{O}}$ contains no elements of order 3. Since $\mathcal{P}_7$ is inert in $k(i)|k$, and $h(k(i)) = 1$, there are two conjugacy classes of elements of order 2. Therefore, any group $\Gamma^1_{\mathcal{O}}$ arising from A has signature $(1; 2, 2)$.

In order to determine the conjugacy classes of the groups $\Gamma^1_{\mathcal{O}}$, we again analyze the behavior of the units R_k^* at the various embeddings α_i. The set $\{-1, \alpha, \alpha - 1, \alpha + 2\}$ is a fundamental system of units for R_k^* and the following table encodes the signs of the generators:

	α	$\alpha - 1$	$\alpha + 2$
$\alpha_1 \sim -2.0615$	$-$	$-$	$-$
$\alpha_2 \sim -0.3963$	$-$	$-$	$+$
$\alpha_3 \sim 0.6938$	$+$	$-$	$+$
$\alpha_4 \sim 1.7640$	$+$	$+$	$+$

Since the extension $k|\mathbb{Q}$ is not Galois and contains no proper subfields, we again get at least one conjugacy class corresponding to the algebra unramified at the place $\alpha_i, 1 \leq i \leq 4$. The class number of k is 1, so $h_\infty = R_k^*/R_k^* \cap k_\infty^*$. By the table above, we see that for each choice of σ_i, $h_\infty = 1$ for the algebra unramified at σ_i. Therefore, there are exactly four conjugacy classes of groups of signature $(1; 2, 2)$ arising from quaternion algebras defined over k. $\square$

2.3.3 Cubic Number Fields

Lemma 2.3.7. *The only possibly periods of elements of finite order that can arise in* $\Gamma^1_{\mathcal{O}}$ *defined over fields* k *with* $|k;\mathbb{Q}| = 3$ *are 2,3,7, and 9.*

Proof. Since k can contain no other proper subfield other than $\mathbb{Q}$, 2 and 3 are the only possibly periods than can arise from proper subfields of k. By Prop. 1.3.13, the prime 7 is the only prime for which $|k_p : \mathbb{Q}| = 3$. In fact, $k_7 = \mathbb{Q}(\cos(2\pi/7))$ is the totally real field with discriminant 49. For prime powers $m = p^k$, the only field $\mathbb{Q}(\zeta_m)$ with $|\mathbb{Q}(\zeta_m) : \mathbb{Q}| = 6$ is $m = 9$. This corresponds to the totally real field of discriminant 81. There are no composite m for which $|\mathbb{Q}(\zeta_m) : \mathbb{Q}| = 6$; this finishes the proof. □

If $[k : \mathbb{Q}] = 3$, we have $Ram_f(A) = \emptyset$ as a possibility. As in the case $[k : \mathbb{Q}] = 5$, this helps to simplify the process immensely, since this implies $d_k \leq 297$. If $Ram_f(A) \neq \emptyset$, then $d_k \leq 981$. On the lists [4], there are 25 number fields k with discriminants satisfying the latter inequality (see Appendix A). The cases $k = \cos(\frac{2\pi}{9}), d_k = 81$ and, $k = \cos(\frac{2\pi}{7}), d_k = 49$, where 9 and 7, respectively, are possible periods require special examination. We analyze the latter case in detail below.

Lemma 2.3.8. *There exist no derived arithmetic Fuchsian groups of genus two arising from a quaternion algebra defined over the cubic number field of discriminant 361.*

Proof. The field k has defining minimal polynomial $f(x) = x^3 - x^2 - 6x + 7$. Using Pari, we compute

$$\frac{8\pi 361^{3/2}\zeta_k(2)}{(4\pi^2)^3} = \pi.$$

By the preceding comments, if $Ram_f(A) \neq \emptyset$. Now the equation

$$4\pi = \mu(\Gamma) = M\mu(\Gamma^1_{\mathcal{O}}) = M\pi \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) \tag{2.11}$$

has no solutions, as 2, 3, and 5 are inert in $k|\mathbb{Q}$. Therefore, there are no derived arithmetic groups of genus two defined over k. □

Lemma 2.3.9. *For $k = \cos(\frac{2\pi}{7})$, the only possible $\Gamma^1_{\mathcal{O}}$ containing Γ are those listed in Theorem 2.2.1.*

Proof. Fix $f(x) = x^3 - x^2 - 2x + 1$ as the minimal polynomial for k. Again, using Pari, we get

$$\frac{8\pi 49^{3/2}\zeta_k(2)}{(4\pi^2)^3} = \frac{\pi}{21}.$$

Thus,

$$4\pi = \mu(\Gamma) = M\mu(\Gamma^1_{\mathcal{O}}) = M\frac{\pi \prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P}) - 1)}{21} \tag{2.12}$$

If we take $Ram_f(A) = \emptyset$, then M = 84. So $\mu(\Gamma^1_{\mathcal{O}}) = \frac{\pi}{21}$. Since $Ram_f(A) = \emptyset$, we have $a_2, a_3, a_7 \neq 0$. Therefore,

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{2\pi}{3} = 2\pi\left(2g - 2 + \frac{a_2}{2} + \frac{2a_3}{3}\right).$$

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{\pi}{21} = 2\pi\left(2g - 2 + \frac{a_2}{2} + \frac{2a_3}{3} + \frac{6a_7}{3}\right)$$

The only solution to this equation is $a_2 = a_3 = a_7 = 1$. Thus, $\Gamma^1_{\mathcal{O}}$ is a triangle group of signature $(0; 2, 3, 7)$ and since $2|84$, $\Gamma^1_{\mathcal{O}}$ has a torsion-free subgroup of index 84.

If $Ram_f(A) \neq \emptyset$, then $\prod_{\mathcal{P}|D(A)}(N(\mathcal{P}) - 1) \geq 42$ since the primes of smallest norm in k have norms 7 and 8, and $|Ram_f(A)| \geq 2$. This implies

$M \leq 2$. However, since $\Gamma^1_{\mathcal{O}}$ will not be torsion-free, 2.1.1 implies that $m \geq 2$. Thus, the only other possible solution to (2.12) occurs when $M = 2$.

If $M = 2$, and we take $Ram_f = \{\mathcal{P}_2, \mathcal{P}_7\}$, the equation is satisfied. Since $6 \nmid d_k$, Lemma 2.2.3 applies. $h = h(k(i)) = h(k(\omega)) = 1$, and since $\mathcal{P}_2$ ramifies and $\mathcal{P}_7$ is inert in $k(i)|k$, $a_2 = 2$. $\mathcal{P}_7$ splits in $k(\omega)|k$, therefore $a_3 = 0$. But

$$\mu(\Gamma^1_{\mathcal{O}}) = 42\frac{\pi}{21} = 2\pi\left(2g - 2 + 1 + \frac{6e_7}{7}\right)$$

and $g = 1, e_7 = 0$ is the only solution. Thus, $\Gamma^1_{\mathcal{O}}$ has signature $(1; 2, 2)$ and, again by Theorem 2.1.1, it has a torsion-free subgroup of genus two and of index 2. Since $k|\mathbb{Q}$ is Galois, there is only one conjugacy class of groups $\Gamma^1_{\mathcal{O}}$ of this signature. □

Chapter 3

Fundamental Domains and Generators for Arithmetic Fuchsian Groups

The group $SU(1,1)$ is the group of orientation-preserving isometries of the unit disk $\mathcal{U} = \{z \in \mathbb{C} | |z| \leq 1\}$. By embedding a cocompact arithmetic Fuchsian group Γ into $SU(1,1)$, one can determine a fundamental domain for its image, Γ', using a theorem of Ford. The elements of Γ' which give the side-pairings of the fundamental domain are generators for Γ'. This technique is described in [21] and [10], but only for arithmetic groups defined over rational or quadratic fields. In [9], Johansson gives a more general description for this technique and gives explicit bounds for the entries of an element of Γ in the quadratic number fields. In this chapter, we give the necessary background for this technique and describe its implementation for number fields of arbitrary degree. In order to find a fundamental domain for Γ, one must have a maximal order written explicitly as an R_k-module, where R_k is the ring of integers of the number field k. We state and prove some results on the existence and form of maximal orders given a Hilbert symbol for a quaternion algebra A. These will be used in the final chapter to obtain generators for the all derived arithmetic groups of signatures (2;0),(1;2,2), and (0;2,2,2,2,2,2) given in Theorem 2.2.1.

3.1 Quaternion Algebras and Maximal Orders

Using a Hilbert symbol for the invariant quaternion algebra A of a derived arithmetic group, one can determine a maximal order $\mathcal{O}$ in A. This in turn can be used to find a fundamental domain for the corresponding unit group $\Gamma^1_{\mathcal{O}}$. Recall that for any quaternion algebra A, one has the associated *Hilbert symbol*

$$\left(\frac{a,b}{k}\right)$$

where $i^2 = a, j^2 = b, ij = -ji = k$ for some a, b in k^*. The basis $\{1, i, j, ij\}$ is referred to as the *standard basis* of A.

We can embed A in $M_2(k(\sqrt{a}))$ (or $M_2(k(\sqrt{b}))$ via a homomorphism ρ; for example, we will take

$$i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix}$$

where $b_1 b_2 = b$. The conjugate of an element $x = x_0 + x_1 i + x_2 j + x_3 ij \in A$ is $\bar{x} = x_0 - x_1 i - x_2 j - x_3 ij$; furthermore, conjugation defines an involution on A.

Recall the definition of the (reduced) norm and (reduced) trace of an element $x \in A$:

For $x \in A$ the *(reduced) norm* and *(reduced) trace* of x lie in F and are defined by $n(x) = x\bar{x}$ and $\mathrm{tr}(x) = x + \bar{x}$, respectively.

Furthermore, one sees that the reduced norm agrees with the determinant under the embedding given above:

$$\mathrm{n}(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$$

as well as the trace, $\mathrm{tr}(x) = 2x_0$.

Let R denote the ring of integers of k. Recall that an order $\mathcal{O}$ of A is a complete R-lattice with 1. It is also useful to think of orders in terms of integers of A:

An element $x \in A$ is an *integer* (over R) if $R[x]$ is an R-lattice in R.

The following facts relating orders to integral elements of A will be useful for us (cf. [13] Ch. 2):

Fact 3.1.1. *An element $x \in A$ is an integer if and only if the reduced norm $n(x)$ and the reduced trace $tr(x)$ lie in R.*

Fact 3.1.2. *$\mathcal{O}$ is an order in A if and only if $\mathcal{O}$ is a ring of integers in A containing R and such that $k\mathcal{O} = A$.*

Recall that the discriminant $\Delta(A)$ of a quaternion algebra A is defined to be the product of the prime ideals at which A is ramified. For the remainder of this section, we will denote the ring of integers in the field k by R. For any R-order $\mathcal{O}$ in A, the discriminant $d(\mathcal{O})$ is defined to be the square root of the R-ideal generated by the set $\{\det(\mathrm{tr}(x_i x_j)), 1 \leq i, j \leq 4\}$, where $x_i \in \mathcal{O}$. The following results on orders appear in [13].

Theorem 3.1.3. *Let $\Delta(A)$ be the discriminant of the quaternion algebra A over a number field k and let $\mathcal{O}$ be a order in A. Then $\mathcal{O}$ is a maximal order if and only if $\Delta(A) = d(\mathcal{O})$. In particular, all maximal orders have the same discriminant.*

Furthermore, we can compute the discriminant of an order, provided it has a free R-basis, via the following theorem:

Theorem 3.1.4. *If $\mathcal{O}$ has free R-basis $\{e_1, e_2, e_3, e_4\}$, then $d(\mathcal{O})$ is the principal ideal $\sqrt{det(tr(e_i e_j))}R$.*

The following two theorems give simple criteria for the ramification set of a quaternion algebra via its Hilbert symbol. We will use these to find appropriate Hilbert symbols for each invariant quaternion algebra on our list.

Theorem 3.1.5. *The quaternion algebra $\left(\frac{a,b}{\mathbb{R}}\right)$ is isomorphic to exactly one of $\mathcal{H}$ or $M_2(\mathbb{R})$, according to whether both a and b are negative or not, respectively.*

Theorem 3.1.6. *Let K by a non-dyadic $\mathcal{P}$-adic field, with integers R and maximal ideal $\mathcal{P}$. Let*

$$A = \left(\frac{a,b}{K}\right)$$

where $a, b \in R$.

1. *If $a, b \notin \mathcal{P}$, then A splits.*
2. *If $a \notin \mathcal{P}$ and $b \in \mathcal{P}/\mathcal{P}^2$, then A splits if and only if a is a square* mod $\mathcal{P}$.

Once we obtain an appropriate Hilbert symbol for our quaternion algebra A, we find its maximal order using the standard order $\mathcal{O}' = R[1, i, j, ij]$. In general, this process involves two main steps and depends primarily on the Hilbert symbol of A. The standard order $\mathcal{O}' = R[1, i, j, ij]$ is always contained in a maximal order $\mathcal{O}$. Now, in all our cases, there will always exist an $r \in R$ such that $\mathcal{O}' \subsetneq \mathcal{O} \subset \frac{1}{r}\mathcal{O}'$. We state a proposition characterizing this denominator r. But, in general, the determination of $\mathcal{O}$ depends mainly on finding an integral element $\beta \in \mathcal{O} \setminus \mathcal{O}'$. We use a computer program to determine β. Then we verify that either $R[1, i, j, \beta]$ or $R[1, i, \beta, i\beta]$ is a maximal order by checking discriminants. In certain cases the Hilbert symbol is "nice" and $r = 2$. Below we state a theorem for these "nice" cases, which states that for a suitable element β, the order $R[1, i, \beta, i\beta]$ is always maximal.

But before we get to the result on these "nice" cases, we state and prove some lemmas for the general case. In the discussion that follows and throughout the remainder of the text, the number field k will be a principal ideal domain, i.e., the class number h of k equals 1.

Lemma 3.1.7. *Let $A = \left(\frac{a,b}{k}\right)$ be a a quaternion algebra over a number field k where $\Delta(A)$ divides abR. Then the standard order $\mathcal{O}'=R[1, i, j, ij]$ has discriminant $d(\mathcal{O}') = 2^2 abR$. In particular, if $a, b \in R$, then $\mathcal{O}'$ is not maximal.*

Proof. Since $i^2 = a, j^2 = b$, by Theorem 3.1.4

$$d(\mathcal{O}')^2 = \det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix} = 2^4 a^2 b^2.$$

Taking the square root gives $d(\mathcal{O}')$. Any maximal order $\mathcal{O}$ of A has discriminant $d(\mathcal{O}) = \Delta(A)$ which divides abR. If $\mathcal{O}$ is a maximal order containing $\mathcal{O}'$, then $d(\mathcal{O}') = 2^2 ab \neq \Delta(A) = d(\mathcal{O})$ implies $\mathcal{O}' \subsetneq \mathcal{O}$. □

Although the standard order is not maximal, the following proposition allows us to use it to find a maximal order of $A = \left(\frac{a,b}{k}\right)$.

Proposition 3.1.8. *Suppose k has class number 1 and $a, b \in R$ are square-free. Let $A = \left(\frac{a,b}{k}\right)$ be a quaternion algebra over a number field k. Suppose, in addition, that $\Delta(A)$ divides abR. Let $\pi_i R = \mathcal{P}_i$ for each $\mathcal{P}_i \notin Ram_f(A)$ and*

$$r_1 = \begin{cases} 1 & \Delta(A) = abR \\ \displaystyle\prod_{\substack{\mathcal{P} | abR \\ \mathcal{P} \nmid \Delta(A)}} \pi_i & \Delta(A) \neq abR \end{cases}.$$

If $\mathcal{O}$ is a maximal order of A containing $\mathcal{O}' = R[1, i, j, ij]$, then

$$\mathcal{O}' \subsetneq \mathcal{O} \subsetneq \frac{1}{r}\mathcal{O}'$$

where $r = 2r_1$.

Proof. The first containment follows from the preceding lemma. Now, since a and b are square-free, $abR = r_1\Delta(A)$, up to multiplication by a unit. Any maximal order of A has discriminant $\Delta(A)$. If $\mathcal{O}$ is a maximal order containing $\mathcal{O}'$, then there exists $\beta \in \mathcal{O} \setminus \mathcal{O}'$. Since $d(\mathcal{O}') = r_1\Delta(A)$ and $d(\mathcal{O}) = \Delta(A)$, by the definition of discriminant, there exists a β in $\mathcal{O} \cap (\frac{1}{2r_1}\mathcal{O}' \setminus \mathcal{O}')$. This implies $\mathcal{O}'[\beta] \subset \mathcal{O} \subset \frac{1}{2r_1}\mathcal{O}'$. Now, the ideal $\frac{1}{2r_1}\mathcal{O}'$ has discriminant

$$d(\frac{1}{2r_1}\mathcal{O}') = \frac{1}{2^4 r_1^4} d(\mathcal{O}') = \frac{1}{2^4 r_1^4} 2^2 abR = \frac{1}{4r_1^4} abR;$$

$\frac{1}{2r_1}\mathcal{O}'$ is clearly not an order, since it contains nonintegral elements, e.g., $\frac{1}{2r_1}$. This implies $\mathcal{O} \subsetneq \frac{1}{2r_1}\mathcal{O}' = \frac{1}{r}\mathcal{O}'$ which completes the proof. □

Lemma 3.1.9. *Let $A = \left(\frac{a,b}{k}\right)$ be a quaternion algebra over a number field k and ring of integers R with $a, b \in R$ satisfying the following conditions*

(i) $(a, b) = 1$,

(ii) $\exists\, \tilde{a}, \tilde{b} \in R$ *such that* $\tilde{a}^2 \equiv a \bmod 4R$ *and* $\tilde{b}^2 \equiv b \bmod 4R$.

Then there exists a nonzero solution $(x, y) \in R \times R$ to the equation $x^2 - ay^2 \equiv b \bmod 4R$.

Proof. We need to show that, under the hypotheses, there always exist $x, y \in R$ such that $x^2 - ay^2 \equiv b \bmod 4R$ or, equivalently, such that $x^2 - ay^2 - b \in 4R$.

By assumption (ii), $x_0^2 - ax_1^2 - bx_2^2 \equiv 0 \bmod 4R$ is equivalent to $x^2 - \tilde{a}^2y^2 \equiv \tilde{b}^2 \bmod 4R$. Now, the equation

$$x - \tilde{a}y \equiv \tilde{b} \bmod 2R \tag{3.1}$$

will have a solution $(x, y) \in R \times R$ provided

$$x - \tilde{a}_{\mathcal{P}}y \equiv \tilde{b}_{\mathcal{P}} \bmod R_{\mathcal{P}} \tag{3.2}$$

has a nonzero solution $(\tilde{a}_{\mathcal{P}}, \tilde{b}_{\mathcal{P}})$ for every prime $\mathcal{P}$ dividing 2 in R (by the Chinese Remainder Theorem). Since $(a, b) = 1$ implies $(\tilde{a}_{\mathcal{P}}, \tilde{b}_{\mathcal{P}}) = 1$, equation (3.2) clearly has a nonzero solution $(\tilde{x}_{\mathcal{P}}, \tilde{y}_{\mathcal{P}})$ for each prime $\mathcal{P}$ dividing 2. Therefore, (3.1) has a nonzero solution $(x, y) \in R$. Since $x - \tilde{a}y \equiv \tilde{b} \bmod 2R \Leftrightarrow x + \tilde{a}y \equiv \tilde{b} \bmod 2R$, (x, y) satisfies

$$(x - \tilde{a}y)(x - \tilde{a}y) \equiv x^2 + \tilde{a}^2y^2 \equiv \tilde{b}^2 \bmod 4R.$$

□

Lemma 3.1.10. *Let* $A = \left(\frac{a,b}{k}\right)$ *be a quaternion algebra with* $a, b \in R$ *and let* $\mathcal{O}' = R[1, i, j, ij]$ *be the standard order in* A*. Suppose further that* $abR = \Delta(A)$*. If* $\beta = \frac{1}{2}\mathcal{O}' \setminus \mathcal{O}'$ *is integral, then* $\mathcal{O} = R[1, i, \beta, i\beta]$ *is an integral ideal. Furthermore, if* $\beta = \frac{1}{2}(x_0 + x_1 i + x_2 j)$*, where* $x_0, x_1 \in R$ *and* $x_2 \in R^*$*, then* $\mathcal{O} \supset \mathcal{O}'$ *is a maximal order of* A*.*

Proof. Let $e_0 = 1, e_1 = i, e_2 = \beta$, and $e_3 = i\beta$. Now $\mathcal{O} = R[1, i, \beta, i\beta]$ is an order if and only if the following conditions are satisfied:

1. $e_k e_l$ is integral for $0 \leq k, l \leq 3$

2. $e_k + e_l$ is integral for $0 \leq k, l \leq 3$

The simple structure of this order makes many of these conditions redundant. Conditions (1) and (2) are conditions that the norms and traces of these elements belong to R. We list the norms and traces of the elements in Tables 3.1 and 3.2 below. Note that the elements $e_k e_l$ and $e_l e_k$, where $k \neq l$ are certainly not equal. However, their traces and norms are equal and therefore both tables are symmetric. We have also omitted the obvious cases, e.g., 1 and i, for brevity.

$\times$	1	i	β	$i\beta$
1	*	*	n=$\frac{(x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= x_0$	n=$-\frac{a(x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= ax_1$
i	*	*	*	n=$\frac{a^2(x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= ax_0$
β	*	*	n=$\frac{(x_0^2-ax_1^2-bx_2^2)^2}{16}$ tr $= \frac{(x_0^2+ax_1^2+bx_2^2)}{2}$	n=$\frac{a(x_0^2-ax_1^2-bx_2^2)^2}{16}$ tr $= ax_0x_1$
$i\beta$	*	*	*	n=$-a(x_0^2-ax_1^2-bx_2^2)$ tr $= 2ax_1$

TABLE 3.1: Norms and traces of products of $\mathcal{O}$ in Lemma 3.1.10

$+$	1	i	β	$i\beta$
1	*	*	n=$\frac{(4+4x_0-x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= 2+x_0$	n=$\frac{(4+4ax_1-a(x_0^2-ax_1^2-bx_2^2))}{4}$ tr $= 2+ax_1$
i	*	*	n=$\frac{(-4a+4ax_1+x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= x_0$	n=$-\frac{a(4+4x_0+x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= ax_1$
β	*	*	n=$(x_0^2-ax_1^2-bx_2^2)$ tr $= 2x_0$	n=$\frac{(a-1)(x_0^2-ax_1^2-bx_2^2)}{4}$ tr $= x_0+ax_1$
$i\beta$	*	*	*	n=$-a(x_0^2-ax_1^2-bx_2^2)$ tr $= 2ax_1$

TABLE 3.2: Norms and sums of products of $\mathcal{O}$ in Lemma 3.1.10

Since $a, b, x_k \in R$, for $0 \leq k \leq 2$, all the conditions on integrality reduce to the following conditions:

1. $x_0^2 - ax_1^2 - bx_2^2 \in 4R$
2. $a(x_0^2 - ax_1^2 - bx_2^2) \in 4R$
3. $a^2(x_0^2 - ax_1^2 - bx_2^2) \in 4R$
4. $(x_0^2 - ax_1^2 - bx_2^2)^2 \in 16R$
5. $a(x_0^2 - ax_1^2 - bx_2^2)^2 \in 16R$
6. $x_0^2 + ax_1^2 + bx_2^2 \in 2R$
7. $a(4 + 4x_0 - x_0^2 - ax_1^2 - bx_2^2) \in 4R \iff a(x_0^2 - ax_1^2 - bx_2^2) \in 4R$
8. $4 + 4ax_1 - a(x_0^2 - ax_1^2 - bx_2^2) \in 4R \iff a(x_0^2 - ax_1^2 - bx_2^2) \in 4R$
9. $-4a + 4ax_1 + x_0^2 - ax_1^2 - bx_2^2 \in 4R \iff x_0^2 - ax_1^2 - bx_2^2 \in 4R$
10. $(a - 1)(x_0^2 - ax_1^2 - bx_2^2) \in 4R.$

Condition (1),

$$x_0^2 - ax_1^2 - bx_2^2 \in 4R,$$

implies all the others. We will show (1) implies (6), as the others follow immediately from basic properties of ideals. $x_0^2 - ax_1^2 - bx_2^2 \in 4R \Rightarrow x_0^2 - ax_1^2 - bx_2^2 \in 2R$ since $4R \subset 2R$. But $x_0^2 - ax_1^2 - bx_2^2 \equiv x_0^2 - ax_1^2 - bx_2^2 \mod 2R$, so $x_0^2 - ax_1^2 - bx_2^2 \in 2R \Leftrightarrow x_0^2 + ax_1^2 + bx_2^2 \in 2R$. However, condition (1) is the equivalent to the integrality of β. This shows that integrality of β implies the integrality of all elements of $\mathcal{O} = R[1, i, \beta, i\beta]$.

In order to show that I is an order, we must show that $I = R[1, i, \beta, i\beta]$ is a complete R-lattice with 1. Since $1, i \in I$, it remains to show that $j \in I$.

Since $\beta = \frac{1}{2}(x_0 + x_1 i + x_2 j) \in I$, we have $j = x_2^{-1}(2\beta - x_1 - x_2 i) \in I$ and, hence, I is complete R-lattice with 1. Therefore, $R[1, i, \beta, i\beta]$ is an order. Using Theorem 3.1.4, the discriminant of the order $R[1, i, \beta, i, \beta]$ is $ab(x_2^2 - ax_3^2)R$. Since $x_3 = 0$ and $x_2 \in R^*$ the discriminant is equal to abR. Hence, $\mathcal{O} = I = R[1, i, \beta, i\beta] \supset \mathcal{O}'$ is a maximal order. $\square$

Remark 3.1.11. *There is an analogous statement of the above lemma to an order of the form $R[1, j, \beta, j\beta]$ due to the anti-symmetry of the algebra A.*

Proposition 3.1.12. *Let $A = \left(\frac{a,b}{k}\right)$ be a quaternion algebra over a number field k with finite ramification set $Ram_f(A)$ and denote the standard order of A by $\mathcal{O}' = R[1, i, j, ij]$. Suppose that $a, b \in R_k$ satisfy the hypotheses of Lemma 3.1.9 and, in addition, that $\Delta(A) = abR$. Then there exists $\beta \in \frac{1}{2}\mathcal{O}'$ such that $\mathcal{O}' \subset \mathcal{O}$ and $\mathcal{O} = R[1, i, \beta, i\beta]$ is a maximal order of A.*

Proof. By Lemma 3.1.7, $\mathcal{O}' = R[1, i, j, k]$ has $d(\mathcal{O}') = 2^2abR$ and, hence, is not maximal. Since any order is contained in a maximal order, $\mathcal{O}' \subset \mathcal{O}$ where $\mathcal{O}$ is a maximal order. In particular, $d(\mathcal{O}) = abR = \Delta(A)$. The ideal $I = \frac{1}{2}\mathcal{O}' \supset \mathcal{O}'$ is not an order since its elements, e.g., $1/2$, are not all integral. But the discriminant of I is equal to abR. Therefore, $\mathcal{O}' \subsetneq \mathcal{O} \subsetneq \frac{1}{2}\mathcal{O}'$. This implies there exists some $\beta \in \frac{1}{2}\mathcal{O}'$ such that $\beta \in \mathcal{O}$.

Since a, b satisfy the hypothesis of Lemma 3.1.9, there exist integers $x_0, x_1 \in R$ such that $x_0^2 - ax_1^2 - b \in 4R$. Therefore, if we take $\beta = \frac{1}{2}(x_0 + x_1 i + j) \in \frac{1}{2}\mathcal{O}'$, then β is integral. Furthermore, by Lemma 3.1.10, $I = R[1, i, \beta, i\beta]$ is a maximal order. This finishes the proof. $\square$

If the Hilbert symbol of A does not satisfy the conditions of the previous proposition, we can still use Lemma 3.1.8 as a starting point, but the process of finding a free-basis for $\mathcal{O}$ becomes more ad hoc. For our examples, we use an intermediate order $\mathcal{O}''$ where $\mathcal{O}' \subsetneq \mathcal{O}'' \subsetneq \frac{1}{2}\mathcal{O}'$ with $d(\mathcal{O}'') = abR$. Then we search for integral elements in the ideal $\frac{1}{r_1}\mathcal{O}''$ where $r_1 \in R$ is as stated in the proof of Lemma 3.1.8. We test these integral elements β as part of a free R-basis of the orders $R[1, i, \beta, i\beta]$ and $R[1, j, \beta, j\beta]$ and compute the discriminants of these orders to detect maximality.

3.2 Fundamental Domain

Let A be the invariant quaternion algebra corresponding to arithmetic Fuchsian group $\Gamma^1_{\mathcal{O}}$. For any maximal order $\mathcal{O}$ in a quaternion algebra A, fix an embedding ρ of $\mathcal{O}^1$ in $PSL_2(\mathbb{R})$ and denote the image by $\Gamma^1_{\mathcal{O}}$. Choose ρ so that $i \in \mathbf{H}^2$ is not the fixed point of any nontrivial element in $\Gamma^1_{\mathcal{O}}$. The Mobius transformation

$$\varphi = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

maps $\mathbf{H}^2$ to the unit disk $\mathcal{U}$. Furthermore, the action of $SL_2(\mathbb{R})$ on $\mathbf{H}^2$ is conjugate to the action of $SU(1,1)$ on $\mathcal{U}$ since

$$SU(1,1) = \varphi SL_2(\mathbb{R})\varphi^{-1}.$$

This defines an embedding of $\Gamma^1_{\mathcal{O}}$ in $SU(1,1)$.

For any $g \in SU(1,1)$ or $SL_2(\mathbb{R})$,

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $c \neq 0$, the isometric circle C_g of g is defined to be the set of points on which g acts as a Euclidean isometry. By taking the derivative of g, one can verify that the circle $\{z \in \mathbb{C} | |cz + d| = 1\} = \{z \in \mathbb{C} | |z + \frac{d}{c}| = \frac{1}{|c|}\}$ is the isometric circle of g.

The following theorem of Ford (cf. [10]) gives a characterization of the fundamental domain of Γ via the isometric circles of a $\Gamma \subset SU(1,1)$:

Theorem 3.2.1. *Let Γ be a discrete subgroup of $SU(1,1)$ such that the origin is not a fixed point of any nontrivial element of Γ. Let C_g be the isometric circle of g. If C_g^o is the set of all points outside C_g, then*

$$\mathcal{F} = \mathcal{U} \cap \bigcap_{g \in \Gamma} C_g^o$$

is a fundamental domain of Γ.

Clearly, $\varphi^{-1}(\mathcal{F})$ is a fundamental domain for $\varphi^{-1}(\Gamma)$. Let r_g be the radius of the isometric circle C_g where $g \in \Gamma$ for a discrete subgroups Γ of $SU(1,1)$. Since

$$SU(1,1) = \left\{ \left(\begin{array}{cc} a & c \\ \bar{c} & \bar{a} \end{array} \right) \Big| a, c \in \mathbb{C},\, a\bar{a} - c\bar{c} = 1 \right\},$$

the radius $r_g = \frac{1}{|c|}$. From the discreteness of Γ and the additional relation $a\bar{a} - c\bar{c} = 1$, it follows that

$$\Gamma_\epsilon = \{g \in \Gamma | r_g > \epsilon\}$$

is finite for every ϵ, $0 < \epsilon < 1$.

$$\mathcal{F}_\epsilon = \mathcal{U} \cap \bigcap_{g \in \Gamma_\epsilon} C_g^o, \quad \mathcal{U}\epsilon = \{z \in \mathbb{C} | |z| < 1 - \epsilon\}, \quad \mathcal{F}_\epsilon \subset \mathcal{U}_\epsilon,$$

then $\mathcal{F}_\epsilon$ is a fundamental domain for Γ for some $\epsilon > 0$ since Γ has finite coarea and no parabolic elements.

Let r_g denote the radius of the isometric circle $\varphi g \varphi^{-1}$, where $g \in \Gamma \subset PSL_2(\mathbb{R})$. If

$$g = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right),$$

then

$$\varphi g \varphi^{-1} = \frac{1}{2}\begin{pmatrix} (a+d)+i(b-c) & (b+c)+i(a-d) \\ (b+c)-i(a-d) & (a+d)-i(b-c) \end{pmatrix}.$$

Therefore,

$$r_g = \frac{2}{|(b+c)-i(a-d)|} = \frac{2}{\sqrt{(a-d)^2+(b+c)^2}} = \frac{2}{\sqrt{a^2+b^2+c^2+d^2-2}}. \tag{3.3}$$

Hence, the restriction $r_g > \epsilon$ gives an upper bound on the entries of g. Furthermore, using the fact that the norm is positive definite in all other $n-1$ embeddings of $\sigma_i : k \hookrightarrow \mathbb{Q}$, one obtains upper bounds on the absolute values of $\sigma_i(a), \sigma_i(b), \sigma_i(c), \sigma_i(d)$ for $2 \le i \le n$.

If we write $\mathcal{O}$ as a $\mathbb{Z}$-module, then we use the bounds on the σ_i to get bounds on the integral coefficients of the elements of Γ.

Suppose $|k : \mathbb{Q}| = n$ and suppose k has integral basis of the form $\{1, \omega, \dots, \omega^{n-1}\}$. W.l.o.g, suppose $A = \left(\frac{a,b}{k}\right)$, where $a > 0$ and $b < 0$. Fix an embedding $\rho : A \hookrightarrow M_2(k\sqrt{a})$. Then the standard order $R[1,i,j,ij]$ is the set of elements

$$\begin{pmatrix} x+y\sqrt{a} & b_1(u+v\sqrt{a}) \\ b_2(u-v\sqrt{a}) & x-y\sqrt{a} \end{pmatrix}$$

where $b_1, b_2 \in R$ satisfy $b_1 b_2 = b$. Now, by Lemma 3.1.8 a maximal order $\mathcal{O}$ of A is contained in $\frac{1}{r}R[1,i,j,ij]$, for some $r \in R \setminus \{0\}$. Therefore, $\mathcal{O}$ will be a subset of the set of elements of the form

$$g = \frac{1}{r}\begin{pmatrix} (\sum x_i\alpha^i)+(\sum y_i\alpha^i)\sqrt{a} & b_1((\sum u_i\alpha^i)+(\sum v_i\alpha^i)\sqrt{a}) \\ b_2((\sum u_i\alpha^i)-(\sum v_i\alpha^i)\sqrt{a}) & (\sum x_i\alpha^i)-(\sum y_i\alpha^i)\sqrt{a} \end{pmatrix}, \tag{3.4}$$

where $r \in R \setminus \{0\}$ and the integers $x_i, y_i, u_i, v_i \in \mathbb{Z}$, $0 \le i \le n-1$. The integrality of the elements in $\mathcal{O}$ translate to certain congruence relations on the $x_i, y_i, u_i, v_i \in \mathbb{Z}$, $0 \le i \le n-1$. The norm of g is $\mathrm{n}(g) = \frac{1}{r^2}(x^2 - ay^2 - bu^2 + abv^2)$.

Since norm is invariant under the embedding σ_i of the number field, $\mathrm{n}(g) = 1$ implies $\mathrm{n}(\sigma_i(g)) = 1$, for $1 \leq i \leq n$. Therefore, for each $g \in \Gamma^1_{\mathcal{O}}$, we have

$$\sigma(r^2) = \sigma(x)^2 - \sigma(a)\sigma(y)^2 - \sigma(b)\sigma(u)^2 + \sigma(a)\sigma(b)\sigma(v)^2.$$

Since A is a quaternion algebra ramified at all but one finite place, we may assume that $\sigma_1(a) > 0$,$\sigma_1(b) < 0$, and $\sigma_i(a) < 0$ and $\sigma_i(b) < 0$ for $2 \leq i \leq n$. Therefore, for each i, $2 \leq i \leq n$,

$$\begin{array}{rcl} |\sigma_i(x)| & \leq & r, \\ |\sigma_i(y)| & \leq & \sqrt{\frac{r^2-\sigma_i(x)^2}{-\sigma_i(a)}}, \\ |\sigma_i(v)| & \leq & \sqrt{\frac{r^2-\sigma_i(x)^2+\sigma_i(a)\sigma_i(y)^2}{\sigma_i(a)\sigma_i(b)}}, \\ |\sigma_i(u)| & \leq & \sqrt{\frac{r^2-\sigma_i(x)^2+\sigma_i(a)\sigma_i(y)^2-\sigma_i(a)\sigma_i(b)\sigma_i(v)^2}{-\sigma_i(b)}}. \end{array} \tag{3.5}$$

Substituting into (3.3), we get that $r_g = \frac{2}{\sqrt{q-2}}$, where

$$q = \frac{1}{r^2}\left(2x^2 + 2y^2 + \frac{4ab^2}{b_1^2+b_2^2}v^2 + (b_1^2+b_2^2)(u + v\frac{b_1^2-b_2^2}{b_1^2+b_2^2}\sqrt{a})^2\right).$$

The condition that $r_g > \epsilon$ is equivalent to $g < M_\epsilon := 2 + \frac{4}{\epsilon^2}$, and this condition implies the following set of bounds for $\sigma_1 = \mathrm{Id}$:

$$\begin{array}{rcl} |x| & < & r\sqrt{\frac{M_\epsilon}{2}}, \\ |y| & < & \sqrt{\frac{1}{2a}(r^2M_\epsilon - 2x^2)}, \\ |v| & < & \sqrt{\frac{b_1^2+b_2^2}{4ab^2}(r^2M_\epsilon - 2x^2 - 2ay^2)}, \\ |u| & < & \sqrt{\frac{1}{b_1^2+b_2^2}(r^2M_\epsilon - 2x^2 - 2ay^2 - \frac{4ab^2}{b_1^2+b_2^2}v^2)} + \frac{b_1^2-b_2^2}{b_1^2+b_2^2}\sqrt{a}|v|. \end{array} \tag{3.6}$$

By taking linear combinations of these inequalities, we obtain bounds on the integers $x_i, y_i, u_i, v_i \in \mathbb{Z}$, $0 \leq i \leq n-1$. This, of course, depends on n and increases in difficulty with n. These bounds are explicitly stated in the programs. We take the best bounds on each integer from the various inequalities obtained. The programs used to obtain the lists for each $\Gamma^1_{\mathcal{O}}$ are given in the appendix, and our examples cover cases in the range $1 \leq n \leq 4$. We will focus mainly on the cases $3 \leq n \leq 4$, since these are not in the literature.

Lastly, we remark that we obtain the most efficient bounds by taking $b_1 = \pm b_2 = \pm\sqrt{b}$. However, Theorem 3.2.1 requires that the origin is not a fixed point of Γ or, equivalently, that i is not a fixed point of $\varphi\Gamma\varphi^{-1}$. If we take $b_1 \neq \pm b_2$, then i will not be a fixed point of $\varphi\Gamma\varphi^{-1}$, and we will do this in the examples in which Γ has torsion.

Chapter 4

The Examples

In this chapter, we use the results of the previous chapter to find generators for a few examples of the derived arithmetic groups $\Gamma^1_{\mathcal{O}}$ in Theorem 2.2.1 containing genus two surface groups using programs written in Mathematica. Example programs for number fields of degrees 2 and 3 are given in the appendix. We will give examples in which the Hilbert symbol of A satisfies the hypotheses of Proposition 3.1.12 and examples in which it does not. We will work in the context described in the previous chapter; as such, the generators will be given as a vector of integers using an integral power basis of R with a specified denominator r. (cf. (3.4)). In the cases the group has signature $(1; 2, 2)$ and $(0; 2, 2, 2, 2, 2, 2)$, we use a standard presentation of the group $\Gamma^1_{\mathcal{O}}$ and Magma to explicitly determine generators for the genus two subgroups.

4.1 Quadratic Number Fields

We begin with an example in which the Hilbert symbol of the quaternion algebra A does not satisfy the hypotheses of Proposition 3.1.12.

Proposition 4.1.1. *Let A be the quaternion algebra A over $\mathbb{Q}(\sqrt{2})$ with $Ram_f(A) = \{\mathcal{P}_5\}$. Then a Hilbert symbol for A is $\left(\frac{\sqrt{2}, -5}{\mathbb{Q}(\sqrt{2})}\right)$ and, if $\mathcal{O} \subset A$ is a maximal order, then a set of generators for $\Gamma^1_{\mathcal{O}}$ are:*

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	2	2	-4	-1	-2	-2	-2	-1
h_2	2	2	-4	-1	2	2	-2	-1
h_3	4	2	-2	-1	0	0	0	-1
h_4	6	2	-4	-3	-2	-2	2	1
h_5	6	2	-4	-3	2	2	2	1
h_6	8	4	-2	0	0	0	-2	-2
h_7	8	4	-2	0	0	0	2	2
h_8	8	6	-4	-5	0	0	2	1
h_9	8	8	-6	-4	0	0	2	2

.

Proof. The ring of integers R_k is equal to $\mathbb{Z}[1, \sqrt{2}]$. Since $\binom{2}{5} = \binom{5}{2} = -1$, $\mathcal{P}_5 = 5R$ and $R_k/\mathcal{P}_5 \cong \mathbb{F}_{5^2}$. Furthermore, $\{1, 1+\sqrt{2}\}$ is a fundamental set of generators for R_k^*, and since both -1 and $1+\sqrt{2}$ are squares mod$\mathcal{P}_5$, there exists no unit $u \in R^*$ such that $\left(\frac{u,-5}{\mathbb{Q}(\sqrt{2})}\right)$ is a Hilbert symbol for A. However, $\sqrt{2}$ is not a square mod$\mathcal{P}_5$, therefore

$$A = \left(\frac{\sqrt{2}, -5}{\mathbb{Q}(\sqrt{2})}\right).$$

satisfies $\mathcal{P}_5 \in Ram_f(A)$ by Theorem 3.1.6. In this case, there is a unique prime $\mathcal{P}_2 = \sqrt{2}R$ over 2. Furthermore, $\mathcal{P}_2$ divides ab. This shows that the Hilbert symbol in this case violates the hypotheses of Proposition 3.1.12. However, since $\mathcal{P}_2$ is the only other prime dividing ab, $\{\mathcal{P}_5\} = Ram_f(A)$ by Theorems 1.3.1 and 3.1.6. The order $\mathcal{O}' = R[1, i, \beta', i\beta']$, where $\beta' = \frac{1}{2}(1+\sqrt{2}i+j)$, has discriminant $d(\mathcal{O}') = \mathcal{P}_2\mathcal{P}_5 = 5\sqrt{2}$. Therefore, $\mathcal{O}'$ is not a maximal order. Let $\mathcal{O}$ be the maximal order containing $\mathcal{O}'$. There exists $\beta \in \mathcal{O}/\mathcal{O}'$ since $\mathcal{O}'$ is not maximal. In fact, $\mathcal{O} \subset \frac{1}{2}\mathcal{O}'$. We determine β as follows. First we determine the congruence relations for the $\mathbb{Z}$-order $\mathcal{O}'$ written as a $\mathbb{Z}$-module:

$$\begin{aligned} x_0 + u_0 &\equiv 0 \bmod 2 & y_0 + v_0 &\equiv 0 \bmod 2 \\ x_1 + u_0 + u_1 &\equiv 0 \bmod 2 & y_1 + u_0 + v_0 + v_1 &\equiv 0 \bmod 2 \end{aligned} \tag{4.1}$$

Secondly, we determine the necessary and sufficient conditions for $\beta = \frac{1}{2}\gamma$, $\gamma \in \mathcal{O}'$. Therefore,

$$\beta = \frac{1}{4}(x_0 + x_1\sqrt{2} + (y_0 + y_1\sqrt{2})i + (u_0 + u_1\sqrt{2})j + (v_0 + v_1\sqrt{2})ij),$$

where the x_i, y_i, u_i, v_i are subject to the congruence relations (4.1). Now, β will be integral provided $\mathrm{tr}(\beta) = \frac{2}{4}(x_0 + x_1\sqrt{2}) = \frac{1}{2}(x_0 + x_1\sqrt{2}) \in R = \mathbb{Z}[1, \sqrt{2}]$ and $\det(\beta) \in R$. The first condition is equivalent to $\mathrm{mod} x_i \equiv 0$ for $i = 0, 1$. The second condition gives two more congruence relations on the integral coefficients of β in addition to those in (4.1). We determine β via these congruences. For each integral element β, we test the discriminant of the order $R[1, i, \beta, i\beta]$ to detect maximality and check that is indeed an order. In this case, we find that $\beta = \frac{1}{4}(2\sqrt{2} + (2 + \sqrt{2})i + \sqrt{2}ij)$ is integral and that $R[1, i, \beta, i\beta]$ is indeed an order. The products and sums of the free basis elements are integral and, since $i\beta = \frac{1}{4}((2\sqrt{2})i + (2 + 2\sqrt{2}) + 2j) = \frac{1}{2}((\sqrt{2})i + (1 + \sqrt{2}) + j)$, $j = 2i\beta - (1 + \sqrt{2}) - (\sqrt{2})i \in R[1, i, \beta, i\beta]$. Finally, $\mathcal{O} = R[1, i, \beta, i\beta]$ since $d(\mathcal{O}) = 5 = \Delta(A)$.

Therefore, $r = 4$ here and $\mathcal{O}$ is the subset of $\frac{1}{4}R[1, i, j, ij]$ satisfying the following congruence relations:

$$\begin{aligned} x_0 - u_0 - 2u_1 - 2v_0 &\equiv 0 \bmod 4 & u_0 &\equiv 0 \bmod 2 \\ x_1 - u_0 - u_1 - 2v_1 &\equiv 0 \bmod 4 & u_1 &\equiv 0 \bmod 2 \\ y_0 - 2u_1 - v_0 - 2v_1 &\equiv 0 \bmod 4 & v_0 &\equiv 0 \bmod 2 \\ y_1 - u_0 - v_0 - v_1 &\equiv 0 \bmod 4 \end{aligned}$$

Since $\Gamma^1_{\mathcal{O}}$ is torsion free, we can apply the program for the quadratic case with $b1 = \sqrt{5}, b_2 = -\sqrt{5}$. We obtain a fundamental region for $\Gamma^1_{\mathcal{O}}$ shown in Figure 4.3 by taking $\epsilon = 0.1$ in the quadratic program.

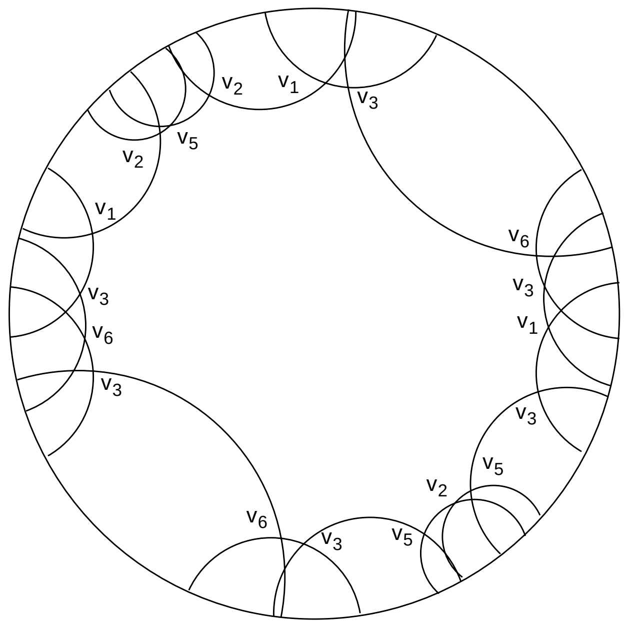

FIGURE 4.3: Fundamental region for $\Gamma^1_{\mathcal{O}}$ of Proposition 4.1.1

Using the identifications determined by the side pairings of the fundamental region, we verify that $\Gamma^1_{\mathcal{O}}$ has signature $(2; 0)$. The generators obtained via the side pairings of the fundamental region are those given in the proposition. □

4.2 Cubic Number Fields

Proposition 4.2.1. *Let A be the quaternion algebra A defined over the totally real cubic field $k = \mathbb{Q}(\alpha) = \mathbb{Q}(cos(2\pi/7))$ with $Ram_f(A) = \{\mathcal{P}_2, \mathcal{P}_7\}$. Then a Hilbert symbol for A is $\left(\frac{2(2\alpha-3),-1}{k}\right)$. Furthermore, if $\mathcal{O} \subset A$ is a maximal order, then a set of generators for $\Gamma^1_{\mathcal{O}}$ in the presentation $< A, B, X|([A, B]X)^2, X^2 >$ are*

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
A	0	2	2	-1	2	2	0	2	2	1	-2	-2
B	-3	2	3	1	-2	-2	1	-2	-3	-2	2	3
X	0	0	0	0	0	0	2	0	0	0	0	0

where $r = 2$.

Proof. The cubic field $k = \mathbb{Q}(cos(\pi/7))$ has minimal polynomial $f(x) = x^3 - x^2 - 2x + 1$ and discriminant 49. Since the extension $k|\mathbb{Q}$ is Galois, there is only one conjugacy classes of groups $\Gamma^1_{\mathcal{O}}$ of signature $(1; 2, 2)$. Denote the three roots of $f(x)$ by α_1, α_2 and α_3 where $\alpha_1 < 0 < \alpha_2 < \alpha_3$. By Pari, there is one unique prime lying over 2 and one unique prime lying over 7 with $\mathcal{P}_7 = (7, \alpha + 2)R = (2\alpha - 3)R$ and $\mathcal{P}_2 = 2R$. We will first show that the quaternion algebra A is given by the Hilbert symbol

$$\left(\frac{2(2\alpha - 3), -1}{k}\right).$$

Since $2\alpha_1 - 3, 2\alpha_2 - 3 < 0$ and $2\alpha_3 - 3 > 0$, A is ramified at the two real places corresponding to α_1 and α_2. Furthermore, $-1 \equiv 6 \bmod \mathcal{P}_7$ and 6 is not a square mod7, so $\mathcal{P}_7 \in Ram_f(A)$ by Theorem 3.1.6. By Theorems 3.1.6 and 1.3.1, A cannot be ramified at any nondyadic prime other than $\mathcal{P}_7$; therefore, $Ram_f(A) = \{\mathcal{P}_2, \mathcal{P}_7\}$. This shows that A has the correct ramification set.

In this case, $Ram_f(A)$ contains a prime dividing 2, and therefore A does not satisfy the hypotheses of Proposition 3.1.12. However, $ab = 2(2\alpha - 3) = \mathcal{P}_2\mathcal{P}_7 = \Delta(A)$, and since there is a unique dyadic prime in this case, a maximal order $\mathcal{O}$ of A will nonetheless be of the form $R[1, i, \beta, i\beta]$ where $\beta \in \frac{1}{2}\mathcal{O}/\mathcal{O}$. The element $\beta = \frac{1}{2}(1 + i + j)$ is integral since $\mathrm{tr}(\beta = 1)$ and $\mathrm{n}(\beta) = -w + 2$. We can write $\frac{1}{2}R[1, i, j, ij] = \frac{1}{2}(x + yi + uj + vij)$, where $x = x_0 + x_1 w + x_2 w^2, y = y_0 + y_1 w + y_2 w^2$, etc., $x_i, y_i, u_i, v_i \in \mathbb{Z}$. Similarly, we write $\mathcal{O} = m+ni+o\beta+pi\beta$, where $m = m_0+m_1w+m_2w^2$, etc., $m_i, n_i, o_i, p_i \in \mathbb{Z}$. Clearly, $\mathcal{O} \subset \frac{1}{2}R[1, i, j, ij]$. Setting the two $\mathbb{Z}$-modules equal yields a linear system of equations. Since the m_i, n_i, o_i, p_i are integers, solving the system for these variables gives congruence conditions on the x_i, y_i, u_i, v_i. These are necessary and sufficient conditions for an element $g \in \frac{1}{2}R[1, i, j, ij]$ to be an element of $\mathcal{O}$. In this particular case, $\mathcal{O}$ is the subgroup comprised of elements satisfying the following congruence relations:

$$\begin{array}{ll} x_0 + u_0 \equiv 0 \bmod 2 & y_0 + u_0 + v_0 \equiv 0 \bmod 2 \\ x_1 + u_1 \equiv 0 \bmod 2 & y_1 + u_1 + v_1 \equiv 0 \bmod 2 \\ x_2 + u_2 \equiv 0 \bmod 2 & y_2 + u_2 + v_2 \equiv 0 \bmod 2 \end{array}.$$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	0	2	2	1	-2	-2	0	2	2	1	-2	-2
h_2	0	2	2	1	-2	-2	0	-2	-2	-1	2	2
h_3	-1	0	1	0	0	0	-1	0	1	1	0	-1
h_4	-1	0	1	0	0	0	-1	4	5	3	-4	-5
g_1	0	0	0	0	0	0	2	0	0	0	0	0

TABLE 4.1: Generators for $\Gamma^1_{\mathcal{O}}$ of Example 4.2.1

In the setting of (3.4), we take $r = 2, b_1 = 2$, and $b_2 = -1/2$ in the program for the cubic case given in the Appendix. In this case, $\epsilon = .15$ is sufficient to obtain the Ford domain for $\Gamma^1_{\mathcal{O}}$.

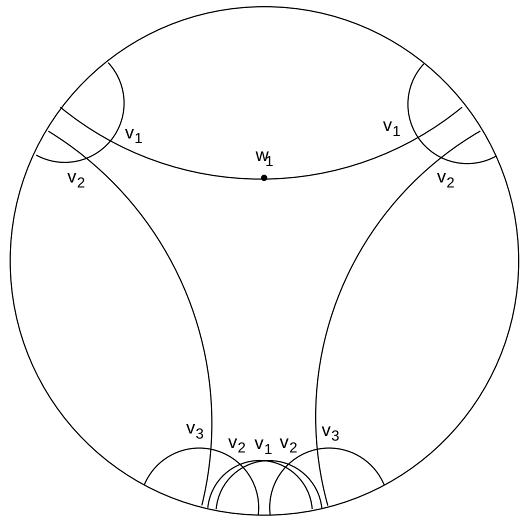

FIGURE 4.1: Fundamental region for $\Gamma^1_{\mathcal{O}}$ of Proposition 4.2.1

The identifications obtained by the side pairings are shown in Figure 4.1; furthermore, α_1 is the fixed point of the element g_1 and the vertex v_2 also has order two. This verifies that $\Gamma^1_{\mathcal{O}}$ has signature $(1; 2, 2)$. The elements listed in the Table 4.1 are the generators for $\Gamma^1_{\mathcal{O}}$ corresponding to the side pairings of the Ford domain.

The elements $A = h_2^{-1}$, $B = h_1 h_3^{-1}, X = g_1$ are noncommuting hyperbolic elements that satisfy the relation

$$([A, B]X)^2 = -Id.$$

Furthermore, no proper subrelation is trivial. Therefore, if we denote the group $< A, B, X|([A, B]X)^2, X^2 >$ by Γ', Γ' has signature $(1; 2, 2)$. The elements $h_1 = A^{-1}X$ and $h_4 = A^{-1}B^{-1}$ and therefore $< A, B, X > \subset \Gamma^1_{\mathcal{O}}$. But since Fuchsian groups are Hopfian, $\Gamma^1_{\mathcal{O}}$ cannot contain a proper isomophic subgroup. This implies $\Gamma^1_{\mathcal{O}} =< A, B, X|([A, B]X)^2, X^2 >$. The elements A, B, X are therefore generators for $\Gamma^1_{\mathcal{O}}$ in the required presentation. $\square$

Proposition 4.2.2. *The group $\Gamma^1_{\mathcal{O}}$ of Proposition 4.2.1 has four distinct subgroups Γ_i, $1 \leq i \leq 4$, of signature $(2;0)$ and index two. Furthermore, a list of generators for each subgroup Γ_i is given below in the standard presentation*

$$< a_1, b_1, a_2, b_2 | [a_1, b_1][a_2, b_2] > .$$

Γ_1	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
a_1	-14	20	24	-12	18	22	-12	20	24	12	-18	-22
b_1	-15	20	25	12	-18	-22	15	-20	-25	-13	18	23
a_2	0	2	2	-1	2	2	0	2	2	-1	2	2
b_2	30	-42	-52	-30	42	53	-32	46	58	-26	38	47

Γ_2	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
a_1	-3	2	3	1	-2	-2	1	-2	-3	-2	2	3
b_1	-14	20	24	-12	18	22	-12	20	24	12	-18	-22
a_2	30	-42	-52	-30	42	53	-32	46	58	-26	38	47
b_2	0	2	2	-1	2	2	0	2	2	-1	2	2

Γ_3	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
a_1	0	2	2	-1	2	2	0	2	2	1	-2	-2
b_1	-14	21	25	13	-18	-23	18	-25	-31	-15	23	28
a_2	1	-2	-3	-2	2	3	3	-2	-3	-1	2	2
b_2	-37	52	65	-33	47	59	-3	2	3	2	-3	-4

Γ_4	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
a_1	0	2	2	-1	2	2	0	2	2	1	-2	-2
b_1	-3	2	3	1	-2	-2	1	-2	-3	-2	2	3
a_2	0	-2	-2	-1	2	2	0	-2	-2	1	-2	-2
b_2	3	-2	-3	1	-2	-2	-1	2	3	-2	2	3

Proof. Using the presentation $< A, B, X, Y | [[A, B]XY, X^2, Y^2] >$ for $\Gamma^1_{\mathcal{O}}$ obtained in Proposition 4.2.1, we use Magma to find generators for all the subgroups of $\Gamma^1_{\mathcal{O}}$ of index 2. Of these, there are four subgroups that are torsion free, which we will denote by Γ_i, $1 \le i \le 4$. The generators in each case are:

$$\begin{aligned} \Gamma_1 &= < BA^{-1}, XA^{-1}, YA^{-1}, A^{-2} > \\ \Gamma_2 &= < B, XA^{-1}, YA^{-1}, A^{-2} > \\ \Gamma_3 &= < A, XB^{-1}, YB^{-1}, B^{-2} > \\ \Gamma_4 &= < A, B, XAX, XBX > \end{aligned}$$

For each Γ_i, we determine the trivial relation in the group. We put each group in the standard presentation to obtain the list of generators for each Γ_i. □

4.3 Quartic Number Fields

Proposition 4.3.1. *Let A be the quaternion algebra A with $Ram_f(A) = \{\mathcal{P}_3\}$ and unramified at the infinite place corresponding to the root α_2, where $-1 < \alpha_2 < 0$, defined over the totally real quartic field of discriminant 3981. Then a Hilbert symbol for A is $\left(\frac{-\alpha(\alpha+1),-1}{k}\right)$. Furthermore, if $\mathcal{O} \subset A$ is a maximal order, then a set of generators for $\Gamma^1_{\mathcal{O}}$ in the presentation*

$$< c_1, c_2, c_3, c_4, c_5 | c_1^2, c_2^2, c_3^2, c_4^2, c_5^2, (c_1c_2c_3c_4c_5)^2 >$$

are

	x	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
c_1	0	-2	4	1	-1	2	-4	-1	1	-3	4	1	-1
c_2	0	0	0	0	2	0	0	0	0	0	0	0	0
c_3	0	-2	4	1	-1	-2	4	1	-1	3	-4	-1	1
c_4	0	-3	4	1	-1	-17	18	7	-5	36	-39	-15	11
c_5	0	0	0	0	0	20	-22	-8	6	-42	50	18	-14

Proof. In this case, $k = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $f(x) = x^4 - x^3 - 4x^2 + 2x + 1$. Let $\alpha_1 < -1 < \alpha_2 < 0 < \alpha_3 < 1 < \alpha_4$ denote the four roots of $f(x)$. In this case, there are four conjugacy classes of groups $\Gamma^1_{\mathcal{O}}$ defined over k. The algebra $A = \left(\frac{-\alpha(\alpha+1),-1}{k}\right)$ is unramified at the place σ_2 since $-\alpha_i(\alpha_i + 1) < 0$ for $i = 1, 3, 4$ and $-\alpha_2(\alpha_2 + 2) > 0$. Furthermore, $f(x) \equiv (x + 1)(x^2 + 1) \bmod 3$, so there are two primes dividing 3. Let $\mathcal{P}_3 = (3, \alpha + 1)R = (\alpha + 1)R$. Since $-1 \equiv 2 \bmod \mathcal{P}_3 \equiv 2 \bmod 3$ and 2 is not a square mod3, A is ramified at $\mathcal{P}_3$ by Theorem 3.1.6. Since no other prime divides ab and there is a unique prime above 2, by Theorems 3.1.6 and 1.3.1, $Ram_f(A) = \{\mathcal{P}_3\}$. This is another "nice" case, so Propostion 3.1.12 applies, and we find that $\mathcal{O} = R[1, i, \alpha, i\alpha]$ where $\alpha = \frac{1}{2}(1 + \alpha + \alpha^2 i = j)$ is a maximal order. The congruence relations in this case are:

$$
\begin{aligned}
x_0 + u_0 + u_3 + v_0 &\equiv 0 \bmod 2 & y_0 + u_2 + u_3 + v_0 + v_3 &\equiv 0 \bmod 2\\
x_1 + u_0 + v_1 &\equiv 0 \bmod 2 & y_1 + u_3 + v_0 + v_1 &\equiv 0 \bmod 2\\
x_2 + u_1 + u_2 + v_2 &\equiv 0 \bmod 2 & y_2 + u_0 + v_1 + v_2 &\equiv 0 \bmod 2\\
x_3 + u_2 + v_3 &\equiv 0 \bmod 2 & y_3 + u_1 + u_2 + u_3 + v_2 &\equiv 0 \bmod 2.
\end{aligned}
$$

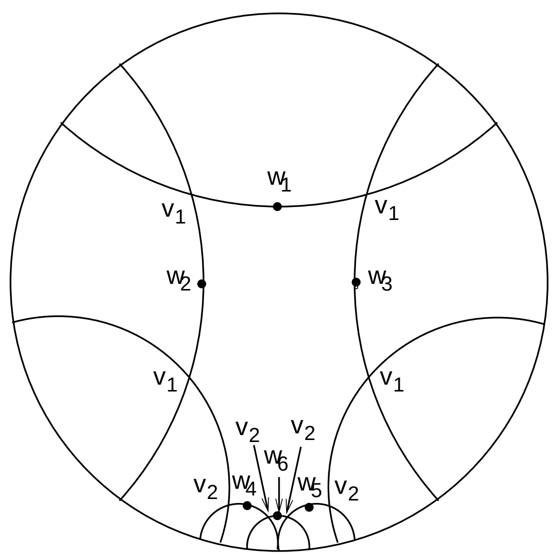

FIGURE 4.2: Fundamental region for $\Gamma^1_{\mathcal{O}}$ of Proposition 4.3.1

We apply the program for the quartic case with $r = 2, b_1 = 2, b_2 = -1/2$, and $\epsilon = .15$ to obtain the fundamental region shown in Figure 4.2; the corresponding generators are listed in Table 4.2. The points w_i are the fixed points of the g_i, $1 \leq i \leq 6$, which all have order two. The side pairings detemined by these generators verifies that $\Gamma^1_{\mathcal{O}}$ has signature (0;2,2,2,2,2,2).

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
g_1	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0
g_2	0	0	0	0	-2	4	1	-1	-2	4	1	-1	3	-4	-1	1
g_3	0	0	0	0	-2	4	1	-1	2	-4	-1	1	-3	4	1	-1
g_4	0	0	0	0	-3	4	1	-1	-17	18	7	-5	36	-39	-15	11
g_5	0	0	0	0	-3	4	1	-1	17	-18	-7	5	-36	39	15	-11
g_6	0	0	0	0	0	0	0	0	20	-22	-8	6	-42	50	18	-14
h_1	2	-3	-1	1	0	0	0	0	5	-3	-2	1	-10	11	4	-3

TABLE 4.2: Generators for $\Gamma^1_{\mathcal{O}}$ of Example 4.3.1

After putting the group in the required presentation, we obtain the list as stated in the Proposition. □

Proposition 4.3.2. *The group* $\Gamma^1_{\mathcal{O}}$ *of Proposition 4.3.1 has a unique subgroup* Γ *of genus two with the following generators:*

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4
a_1	*9*	*-11*	*-4*	*3*	*67*	*-75*	*-28*	*31*
b_1	*2*	*-4*	*-1*	*1*	*-10*	*11*	*4*	*-3*
a_2	*-12*	*14*	*5*	*-4*	*26*	*-28*	*-11*	*8*
b_2	*-2*	*4*	*1*	*-1*	*31*	*-36*	*-13*	*10*

	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
a_1	*-35*	*39*	*15*	*-11*	*39*	*-43*	*-16*	*12*
b_1	*7*	*-7*	*-3*	*2*	*-11*	*14*	*5*	*-4*
a_2	*-14*	*18*	*6*	*-5*	*31*	*-36*	*-13*	*10*
b_2	*-14*	*18*	*6*	*-5*	*3*	*-4*	*-1*	*1*

Proof. The group $\Gamma^1_{\mathcal{O}}$ of Proposition 4.3.1 has signature $(0; 2, 2, 2, 2, 2, 2)$ and hence, has a unique subgroup Γ of signature $(2; 0)$ by [7]. Using Magma, we find that, if $\Gamma^1_{\mathcal{O}}$ is presented in the form

$$< c_2c_1, c_3c_1, c_4c_1, c_5c_1 | c_1^{-1}c_2c_3^{-1}c_4c_1c_2^{-1}c_2c_4^{-1} >,$$

then the subgroup Γ is generated by $< c_2c_1, c_3c_1, c_4c_1, c_5c_1 >$. Putting the these generators in the standard form $< a_1, b_1, a_2, b_2 | [a_1, b_1][a_2, b_2] >$ yields the generators listed in the Proposition. □

The following example is an example of a quartic case in which the Hilbert symbol of A does not satisfy the hypotheses of Proposition 3.1.12. We will show in the proof that a "nice" symbol does not exist for A. We remark that the technique for finding a maximal order is exactly the same as in the previous example, except in this case we cannot take r to be a rational integer.

Proposition 4.3.3. *Let A be the quaternion algebra A with $Ram_f(A) = \{\mathcal{P}_2\}$ and unramified at the infinite place corresponding to the root α_1, where $-2 < \alpha_1 < -1$, defined over the totally real quartic field of discriminant 4752. Then a Hilbert symbol for A is $\left(\frac{1+\alpha, -(-1+\alpha)(-1+\alpha+\alpha^2)}{\mathbb{Q}(\alpha)}\right)$ and, if $\mathcal{O} \subset A$ is a maximal order, then $\Gamma^1_{\mathcal{O}}$ has the following list of generators:*

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	0	-1	0	-1	0	0	0	0	0	0	0	0	4	1	-1
h_2	0	-2	-1	1	-1	3	1	-1	0	0	0	0	-1	-2	1	0
h_3	0	-4	0	1	1	-1	0	0	1	3	1	-1	1	2	-1	0
h_4	0	-4	0	1	1	-1	0	0	-1	-3	-1	1	1	2	-1	0
h_5	1	0	-1	0	0	3	-1	0	1	1	2	-1	0	-1	-2	1
h_6	1	0	-1	0	0	3	-1	0	-1	-1	-2	1	0	-1	-2	1
h_7	1	2	-2	0	2	2	-1	0	0	0	0	0	-1	-1	3	-1
h_8	0	-1	-3	1	-1	3	-1	0	0	0	0	0	0	-1	3	-1
h_9	1	1	-2	1	0	3	-1	0	0	0	0	0	0	-5	2	0

Proof. The totally real number field of degree 4 with discriminant 4752 is equal to $k = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^4 - 2x^3 - 3x^2 + 4x + 1$. Let

$\alpha_1 < -1 < \alpha_2 < 0 < 1 < \alpha_3 < 2 < \alpha_4$ denote the four real roots of $f(x)$. Since $f(x) \equiv (x^2+x+1)^2$, there is a unique prime $\mathcal{P}_2$ of norm 4 dividing 2; furthermore, $\mathcal{P}_2 = (2, \alpha^2+\alpha+1) = (\alpha^2+\alpha-1) = (\pi)$. A fundamental system for R^* is $< \alpha, \alpha-1, \alpha^2-2 >$. The signs of the generators of R^* and of the uniformizer π for $\mathcal{P}_2$ under the different embeddings corresponding to the α_i are shown in the below:

	α	$-1+\alpha$	$-2+\alpha^2$	π
$\alpha_1 \sim -1.4955$	$-$	$-$	$+$	$-$
$\alpha_2 \sim -0.21968$	$-$	$-$	$-$	$-$
$\alpha_3 \sim 1.2196$	$+$	$+$	$-$	$+$
$\alpha_4 \sim 2.4955$	$+$	$+$	$+$	$+$

From the table of embeddings, it is evident that we there does not exist a Hilbert symbol for A such that the only primes dividing ab are in $Ram_f(A)$. However, the algebra given by

$$\left(\frac{1+\alpha, (1-\alpha)(-1+\alpha+\alpha^2)}{\mathbb{Q}(\alpha)}\right).$$

is unramified at the place σ_1. The element $1+\alpha$ is a uniformizer for $\mathcal{P}_3$ in R (since $f(x) \equiv (x+1)^4$, $\mathcal{P}_3$ is the unique prime of norm 3 lying over 3.) But A is unramified at $\mathcal{P}_3$ since $(1-\alpha)(-1+\alpha+\alpha^2) \equiv 1 \bmod \mathcal{P}_3$ which is a square mod3. Thus, A correponds to one of the two conjugacy classes of $\Gamma^1_{\mathcal{O}}$ defined over k.

As in the previous example, we use an intermediate order to find a maximal order $\mathcal{O}$. The order $\mathcal{O}' = R[1, i, \beta, i\beta]$, where $\beta = \frac{1}{2}((1+\alpha) + (1+\alpha^2)i + j)$ has discriminant $d(\mathcal{O}') = (1+\alpha)(-1+\alpha)(-1+\alpha+\alpha^2)R = \mathcal{P}_3\mathcal{P}_2R$. Therefore, a maximal order $\mathcal{O}$ will be contained in the ideal $\frac{1}{\alpha+1}\mathcal{O}'$. Again, this implies there exists an element $\beta \in \frac{1}{\alpha+1}\mathcal{O}'/\mathcal{O}'$. An element in $\mathcal{O}'$ written as in integral vector satisfies the following congruence relations:

$$\begin{aligned}
x_0 + u_0 + u_3 + v_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2\\
x_1 + u_0 + v_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2\\
x_2 + u_1 - u_2 + u_3 + v_0 + v_3 &\equiv 0 \bmod 2\\
x_3 + u_2 + u_3 + v_0 + v_1 &\equiv 0 \bmod 2\\
y_0 - u_0 + u_2 + v_0 + v_3 &\equiv 0 \bmod 2\\
y_1 + u_1 + u_3 + v_0 + v_1 &\equiv 0 \bmod 2\\
y_2 + u_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2\\
y_3 + u_1 + v_2 + v_3 &\equiv 0 \bmod 2.
\end{aligned} \tag{4.2}$$

Consider an element of the form $\beta = \frac{1}{2(\alpha+1)}(x+yi+uj+vij) \in I = \frac{1}{\alpha+1}\mathcal{O}'/\mathcal{O}'$. Now, β is integral if and only if

$$\begin{aligned}
\operatorname{tr}(\beta) &= \frac{x}{1+\alpha} \in R\\
\det(\beta) &= \frac{1}{4(1+\alpha)^2}\big(x^2 + (1+\alpha)y^2 + (-1+\alpha)(-1+\alpha+\alpha^2)u^2\\
&\quad +(1+\alpha)(-1+\alpha)(-1+\alpha+\alpha^2)v^2\big)\\
&= \frac{d(x,y,u,v)}{4(1+\alpha)^2} = \frac{d}{4(1+\alpha)^2}
\end{aligned}$$

	r_0	r_1	r_2	r_3	s_0	s_1	s_2	s_3
β	1	0	1	0	1	0	0	2
$i\beta$	-1	-1	-2	0	-1	-7	6	6
β^2	-2	-4	5	-2	-27	-120	48	68
$(i\beta)^2$	-1	0	5	0	-247	-1522	469	888
$1+\beta$	3	0	1	0	3	0	1	2
$1+i\beta$	1	-1	-2	0	-1	-8	4	6
$i+\beta$	1	0	1	0	3	2	2	2
$i+i\beta$	-1	-1	-2	0	1	-5	7	7
$\beta+i\beta$	0	-1	-1	0	0	-7	6	8

TABLE 4.6

If we write each of x, y, u, v in an integral power basis of R, these conditions are equivalent to the existence of solutions $(r_0, r_1, r_2, r_3), (s_0, s_1, s_2, s_3) \in \mathbb{Z}^4$ to the equations

$$\begin{array}{rcl} x & = & (1+\alpha)(r_0 + r_1\alpha + r_2\alpha^2 + r_3\alpha^3) \\ & = & (r_0 - r_3) + (r_0 + r_1 - 4r_3)\alpha + (r_1 + r_2 + 3r_3)\alpha^2 + (r_2 + 3r_3)\alpha^3 \\ d & = & 4(1+\alpha)^2(s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3) \\ & = & 4(s_0 - s_2 - 4s_3) + 4(2s_0 + s_1 - 4s_2 - 17s_3)\alpha \\ & & \quad +4(s_0 + 2s_1 + 4s_2 + 8s_3)\alpha^2 + 4(s_1 + 4s_2 + 12s_3)\alpha^3 \end{array} \tag{4.3}$$

where $d = d(x_0, \ldots x_4, y_0, \ldots y_4, u_0, \ldots u_4, v_0, \ldots v_4) \in R$. The expressions for x and d are simplified by the relation $\alpha^4 = 2\alpha^3 + 3\alpha^2 - 4\alpha - 1$. The existence of solutions to these equations yields another set of congruences on the x_i, y_i, u_i, v_i. Using these in addition to the congruence relations (4.2), we find that

$$\beta = \frac{1}{2(\alpha+1)}\left((1 + \alpha + \alpha^2 + \alpha^3) + (1 + \alpha + 2\alpha^2)i + ij\right)$$

is integral; $\mathrm{tr}(\beta) = 1 + \alpha^2 \in R$ and $\det(\beta) = 2\alpha^3 + 1$. Furthermore,

$$\begin{array}{rcl} i\beta & = & \frac{1}{2(\alpha+1)}\left((1 + \alpha + 2\alpha^2)(\alpha+1) + (1 + \alpha + \alpha^2 + \alpha^3)i + (\alpha+1)j\right) \\ & = & \frac{1}{2}\left((1 + \alpha + 2\alpha^2) + (1 + \alpha^2)i + j\right) \end{array};$$

this implies $j = 2i\beta - (1 + \alpha + 2\alpha^2) - (1 + \alpha^2)i \in I$. The integrality of the elements of I are verified using 4.3 and the traces and products of the R-basis are listed in Tables 4.4 and 4.5. The solutions $(r_0, r_1, r_2, r_3), (s_0, s_1, s_2, s_3)$ to (4.3) are also given in Table 4.6 for completeness.

$\times$	1	i	β	$i\beta$
1	*	*	n=$3+\alpha^2+2\alpha^3$ tr $=3+\alpha^2$	n=$-1-8\alpha+4\alpha^2+6\alpha^3$ tr $=1-\alpha-2\alpha^2$
i	*	*	*	n=$1-5\alpha+7\alpha^2+7\alpha^3$ tr $=-1-\alpha-2\alpha^2$
β	*	*	n=$4(1+2\alpha^3)$ tr $=2(1+\alpha^2)$	n=$-7\alpha+6\alpha^2+8\alpha^3$ tr $=-\alpha-\alpha^2$
$i\beta$	*	*	*	n=$-4(1+7\alpha-6\alpha^2-6\alpha^3)$ tr $=-2(1+\alpha+2\alpha^2)$

TABLE 4.4: Norms and traces of sums of the R-basis of $\mathcal{O}$

$+$	1	i	β	$i\beta$
1	*	*	n=$1+2\alpha^3$ tr $=1+\alpha^2$	n=$-1-7\alpha+6\alpha^2+6\alpha^3$ tr $=1+\alpha^2$
i	*	*	n=$-1-7\alpha+6\alpha^2+6\alpha^3$ tr $=-1-\alpha-2\alpha^2$	n=$1-3\alpha+10\alpha^2+8\alpha^3$ tr $=-3-3\alpha-2\alpha^2$
β	*	*	n=$(1+2\alpha^3)^2$ tr $=-2-4\alpha+5\alpha^2-2\alpha^3$	n=$-37-170\alpha+70\alpha^2+108\alpha^3$ tr $=-3-5\alpha+3\alpha^2-2\alpha^3$
$i\beta$	*	*	*	n=$(-1-7\alpha+6\alpha^2+6\alpha^3)^2$ tr $=2(-1+5\alpha^2)$

TABLE 4.5: Norms and traces of products of the R-basis of $\mathcal{O}$

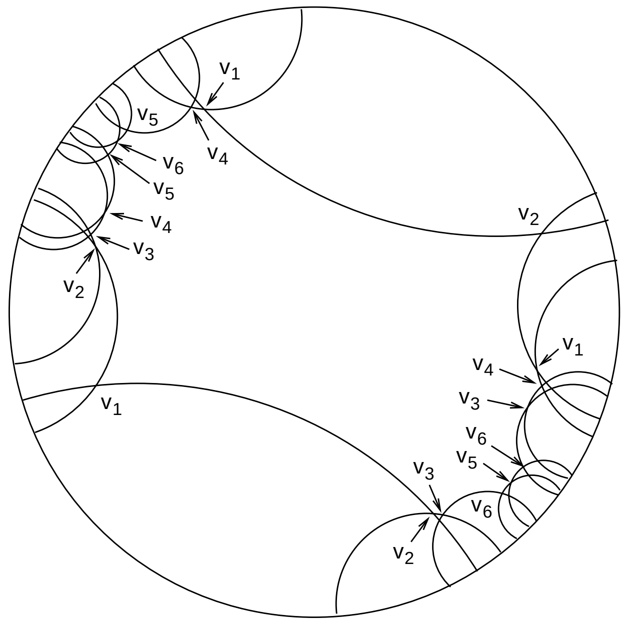

FIGURE 4.4: Fundamental region for $\Gamma^1_{\mathcal{O}}$ of Proposition 4.3.3

Since $R[1, i, \beta, i\beta]$ has discriminant $\mathcal{P}_2 = \Delta(A)$, it is a maximal order. Finally, we determine the congruence relations for $\mathcal{O}$ written as a $\mathbb{Z}$-module:

$$\begin{aligned}
4x_0 - x_1 + x_2 - x_3 + u_0 + 2u_1 - 2u_2 + 2u_3 - 3v_0 + 3v_2 &\equiv 0 \bmod 6 \\
x_0 - x_1 + x_2 - x_3 - 2u_0 + 2u_1 - 8u_2 - 7u_3 - v_1 + v_1 &\equiv 0 \bmod 6 \\
4y_0 - y_1 + y_2 - y_3 - u_0 - 2u_1 + 2u_2 + u_3 + v_0 + 2v_1 - 2v_2 + 2v_3 &\equiv 0 \bmod 6 \\
y_0 - y_1 + y_2 - y_3 + 2u_0 - 2u_1 - u_2 + u_3 - 2v_0 + 2v_1 - 2v_2 - v_3 &\equiv 0 \bmod 6 \\
-u_0 + u_1 - u_2 + u_3 &\equiv 0 \bmod 3 \ . \\
x_2 + x_3 + u_1 + v_1 + v_3 &\equiv 0 \bmod 2 \\
x_0 + x_1 + x_2 + u_2 + v_0 &\equiv 0 \bmod 2 \\
y_2 + y_3 + u_0 + u_1 + v_1 &\equiv 0 \bmod 2 \\
y_0 + y_1 + y_2 + u_1 + u_2 + u_3 + v_2 &\equiv 0 \bmod 2
\end{aligned} \tag{4.4}$$

Running the quartic program with $b_1 = \pm b_2 = \pm\sqrt{(\alpha - 1)(\alpha^2 - \alpha + 1)}$ and $\epsilon = 0.1$ yields the fundamental region in Figure 4.4 and the generators in the proposition. $\square$

Chapter 5

Generators of Derived Arithmetic Groups

Here we list all generators for the all derived arithmetic groups $\Gamma^1_{\mathcal{O}}$ of signatures (2;0),(1;2,2) and (0;2,2,2,2,2,2) listed in Proposition 2.2.1. The generators are given as a $\mathbb{Z}$-vector with denominator r (cf. (3.4)) for ease of notation; the Hilbert symbol for the corresponding quaternion algebra is also given. In the cases for which $\Gamma^1_{\mathcal{O}}$ has more than one conjugacy class, $f(x)$ is the minimal polynomial for the field k and the number α corresponds to the embedding of A.

5.1 Groups $\Gamma^1_{\mathcal{O}}$ with Signature (1;2,2)

The generators are those obtained from the Ford fundamental region. Hyperbolic elements are labelled by h_i and elliptic elements by g_i.

$|k : \mathbb{Q}| = 1$

$\Delta(A) = \{2, 7\}, A = \left(\frac{5,14}{\mathbb{Q}}\right), r = 10$

	x	y	u	v
h_1	3	-9	0	-2
h_2	3	-5	0	0
h_3	4	-2	-1	-1
h_4	4	-2	1	-1
g_1	0	-6	0	2

$|k:\mathbb{Q}|=2$

$\mathbf{d_k=5}$

$\Delta(A)=\mathcal{P}_{31}, A=\left(\frac{\frac{1+\sqrt{5}}{2},-6-\sqrt{5}}{\mathbb{Q}(\sqrt{5})}\right), r=4$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	2	2	-4	0	0	0	0	0
h_2	5	3	-2	-2	0	0	-2	0
h_3	5	3	-2	-2	0	0	2	0
g_1	0	0	-1	-1	-2	0	0	0
g_2	0	0	-1	-1	2	0	0	0

$\Delta(A)=\mathcal{P}'_{31}, A=\left(\frac{\frac{3(1+\sqrt{5})}{2},-6+\sqrt{5}}{\mathbb{Q}(\sqrt{5})}\right), r=12$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	9	3	-2	2	0	0	2	0
h_2	12	6	-8	0	0	0	1	1
h_3	12	6	-5	-3	-3	-3	1	1
h_4	12	6	-5	-3	3	3	1	1
h_5	18	6	-4	0	0	0	2	2
g_1	0	0	-2	0	-9	-3	-2	-2
g_2	0	0	-2	0	9	3	-2	-2

$|k:\mathbb{Q}|=3$

$\mathbf{d_k=49}, f(x)=x^3-x^2-2x+1$

$\Delta(A)=\mathcal{P}_2\mathcal{P}_7, A=\left(\frac{2(-3+2\alpha),-1}{k}\right), r=2$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	0	2	2	1	-2	-2	0	2	2	1	-2	-2
h_2	0	2	2	1	-2	-2	0	-2	-2	-1	2	2
h_3	-1	0	1	0	0	0	-1	0	1	1	0	-1
h_4	-1	0	1	0	0	0	-1	4	5	3	-4	-5
g_1	0	0	0	0	0	0	2	0	0	0	0	0

$\mathbf{d_k = 229}, f(x) = x^3 - 4x + 1$

$\sigma_1 \sim -2.1149,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_2', A = \left(\frac{-\alpha,-2}{k}\right), r = 2$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	0	-1	0	4	0	-1	0	0	0	0	0	0
h_2	0	-2	1	-1	0	0	-1	0	0	2	-1	0
h_3	0	-2	1	-1	0	0	-1	1	0	-2	-1	1
h_4	0	-2	1	-1	0	0	1	0	0	-2	1	0
h_5	0	-2	1	-1	0	0	1	-1	0	2	1	-1
h_6	0	0	0	4	-2	0	1	-2	1	-1	1	0
h_7	0	0	0	4	-2	0	-1	2	-1	1	-1	0

$\sigma_2 \sim 0.2541,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_2', A = \left(\frac{-2\alpha(-3+2\alpha),-1}{k}\right), r = 2(-3+2\alpha)$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	-7	-2	3	3	0	-1	-13	2	3	12	-1	-3
h_2	-10	0	3	8	-1	-2	10	0	-3	-9	1	2
h_3	-10	0	3	9	-1	-2	-10	0	3	8	-1	-2
h_4	-10	0	3	4	0	-1	10	0	-3	-11	0	3
h_5	-13	2	3	3	0	-1	-7	-2	3	12	-1	-3
g_1	0	0	0	9	-1	-2	20	0	-6	-15	1	4
g_2	0	0	0	0	0	0	6	-4	0	0	0	0

$\sigma_3 \sim 1.8608,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_2', A = \left(\frac{-7+4\alpha,-2}{k}\right), r = 2(-7+4\alpha)$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	-3	-5	3	3	-1	-1	-7	4	0	1	0	0
h_2	-7	-3	4	1	-1	0	7	-4	0	-1	0	0
h_3	-7	-3	4	1	-1	0	-7	4	0	-1	0	0
h_4	10	-6	1	4	-2	-1	0	0	0	0	0	0
h_5	-3	-5	3	3	-1	-1	7	-4	0	1	0	0
g_1	0	0	0	-2	0	0	3	5	-3	3	-1	-1
g_2	0	0	0	-2	0	0	7	3	-4	-1	1	0

$|k:\mathbb{Q}|=4$

$\mathbf{d_k = 725}$, $f(x) = x^4 - x^3 - 3x^2 + x + 1$

$\alpha_1 \sim -1.3557$, $\Delta(A) = \mathcal{P}_{31}, A = \left(\frac{-\alpha(1+\alpha)(1+3\alpha),-1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	0	-3	-1	1	0	0	0	0	0	0	0	0	-1	3	1	-1
h_2	-1	-6	-1	2	1	6	1	-2	7	17	1	-5	-7	-19	-2	6
h_3	2	1	-1	0	0	0	0	0	-4	-6	0	2	4	7	0	-2
h_4	-1	-6	-1	2	1	6	1	-2	-7	-17	-1	5	7	19	2	-6
g_1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
g_2	0	0	0	0	-1	3	1	-1	0	3	1	-1	0	0	0	0
g_3	0	0	0	0	-1	3	1	-1	0	-3	-1	1	0	0	0	0

$\alpha_4 \sim 2.0952$, $\Delta(A) = \mathcal{P}_{31}, A = \left(\frac{\alpha(-1+\alpha)(1+3\alpha),-1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	-1	-2	0	2	0	-1	0	-1	1	2	0	2	0	-1	0
h_2	1	-1	-2	0	2	0	-1	0	1	-1	-2	0	-2	0	1	0
h_3	-1	-1	0	0	0	0	0	0	0	-1	0	0	-3	2	2	-1
h_4	0	-1	0	0	0	0	0	0	-1	2	0	-1	0	3	1	-1
g_1	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0
g_2	0	0	0	0	-3	2	2	-1	0	1	0	-1	0	3	1	-1
g_3	0	0	0	0	-3	2	2	-1	0	-1	0	1	0	-3	-1	1

$\alpha_1 \sim -1.3557$, $\Delta(A) = \mathcal{P}'_{31}, A = \left(\frac{-(1+\alpha),-3+\alpha}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	-1	0	0	0	0	0	0	0	0	0	0	-1	0	0	0
h_2	1	1	-1	0	-1	1	2	-1	-1	1	2	-1	0	0	-2	1
h_3	1	1	-1	0	-1	1	2	-1	1	-1	-2	1	0	0	2	-1
h_4	1	0	-2	1	-1	3	1	-1	1	1	-3	1	-1	-1	5	-2
h_5	1	0	-2	1	-1	3	1	-1	-1	-1	3	-1	1	1	-5	2
g_1	0	0	0	0	-1	0	0	0	-1	0	0	0	0	0	0	0
g_2	0	0	0	0	-1	0	0	0	1	0	0	0	0	0	0	0

$\mathbf{d_k = 725}$, $f(x) = x^4 - x^3 - 3x^2 + x + 1$

$\alpha_4 \sim 2.0952$, $\Delta(A) = \mathcal{P}'_{31}$, $A = \left(\frac{(1-\alpha)(-3+\alpha)}{\mathbb{Q}(\alpha)}\right)$, $r = 2$

t	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	0	-1	0	-1	-1	0	0	-1	0	1	0	-1	-1	0	0
h_2	1	0	-1	0	-1	-1	0	0	1	0	-1	0	1	1	0	0
h_3	0	0	-1	0	0	0	0	0	1	1	0	0	0	2	0	-1
h_4	-1	-1	0	0	0	0	0	0	1	-2	0	1	0	-1	-1	0
h_5	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0
h_6	0	0	0	0	-3	2	2	-1	0	-1	0	1	0	3	1	-1
h_7	0	0	0	0	-3	2	2	-1	0	1	0	-1	0	-3	-1	1

$\mathbf{d_k = 1125}$, $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$

$\Delta(A) = \mathcal{P}_2$, $A = \left(\frac{-1-\alpha,-1}{\mathbb{Q}(\alpha)}\right)$, $r = 2(1+\alpha)$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	-1	0	0	0	0	0	0	0	0	0	0	-1	0	0	0
h_2	1	1	-1	0	-1	1	2	-1	-1	1	2	-1	0	0	-2	1
h_3	1	1	-1	0	-1	1	2	-1	1	-1	-2	1	0	0	2	-1
h_4	1	0	-2	1	-1	3	1	-1	1	1	-3	1	-1	-1	5	-2
h_5	1	0	-2	1	-1	3	1	-1	-1	-1	3	-1	1	1	-5	2
h_6	0	0	0	0	-1	0	0	0	-1	0	0	0	0	0	0	0
h_7	0	0	0	0	-1	0	0	0	1	0	0	0	0	0	0	0

$\mathbf{d_k = 1957}$, $f(x) = x^4 - 4x^2 - x + 1$

$\alpha_1 \sim -1.7640$, $\Delta(A) = \mathcal{P}_7$, $A = \left(\frac{-\alpha(1+\alpha)(2+3\alpha),-1}{\mathbb{Q}(\alpha)}\right)$, $r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	1	-1	0	-5	11	2	-3	1	1	-1	0	5	-11	-2	3
h_2	-1	-2	-1	1	0	0	0	0	1	-1	0	0	-3	8	1	-2
h_3	1	-1	0	0	0	0	0	0	1	1	-1	0	-3	10	2	-3
h_4	1	1	-1	0	-5	11	2	-3	-1	-1	1	0	-5	11	2	-3
g_1	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0

$\mathbf{d_k = 1957}$, $f(x) = x^4 - 4x^2 - x + 1$

$\alpha_2 \sim -0.6938$, $\Delta(A) = \mathcal{P}_7, A = \left(\frac{(1+\alpha)(2+3\alpha),-1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	2	-3	-1	1	-8	21	4	-6	2	-3	-1	1	-8	21	4	-6
h_2	2	-3	-1	1	-8	21	4	-6	-2	3	1	-1	8	-21	-4	6
h_3	2	-3	-1	1	0	0	0	0	3	-7	-1	2	-21	49	10	-14
h_4	3	-3	-1	1	0	0	0	0	2	-3	-1	1	-14	35	7	-10
h_5	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0

$\alpha_3 \sim 0.3963$, $\Delta(A) = \mathcal{P}_7, A = \left(\frac{(2-\alpha)(2+3\alpha),-1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	-1	-3	0	1	0	0	0	0	0	0	0	0	-2	4	1	-1
h_2	-1	-4	0	1	0	3	0	-1	9	15	-1	-4	-5	-4	1	1
h_3	-2	-4	0	1	-2	4	1	-1	-13	-19	2	5	6	8	-1	-2
h_4	-2	-4	0	1	-2	4	1	-1	13	19	-2	-5	-6	-8	1	2
h_5	-1	-4	0	1	0	3	0	-1	-9	-15	1	4	5	4	-1	-1
h_6	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0

$\alpha_4 \sim 2.0614$, $\Delta(A) = \mathcal{P}_7, A = \left(\frac{\alpha(-2+\alpha)(2+3\alpha),-1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	0	1	1	1	-3	-2	0	-1	0	-1	-1	-1	3	2	0
h_2	-1	-2	-1	0	0	0	0	0	0	1	0	0	-2	5	0	-2
h_3	0	-1	0	0	0	0	0	0	0	-3	0	1	0	3	0	-1
h_4	1	0	1	1	1	-3	-2	0	1	0	1	1	1	-3	-2	0
g_1	0	0	0	0	0	0	0	0	-2	0	0	0	0	0	0	0

5.2 Groups $\Gamma_{\mathcal{O}}^1$ with Signature (0;2,2,2,2,2,2)

The generators are given in the presentation $< c_1, c_2, c_3, c_4, c_5 | (c_1c_2c_3c_4c_5)^2 >$

$|k:\mathbb{Q}| = 2$

$\mathbf{d_k = 24}$

$\Delta(A) = \mathcal{P}_3, A = \left(\frac{2+\sqrt{6}, -3-\sqrt{6}}{\mathbb{Q}(\sqrt{6})}\right), r = 4$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
c_1	0	0	-2	1	-2	0	2	-1
c_2	0	0	-4	-1	-2	-2	-4	1
c_3	0	0	-4	0	4	0	0	0
c_4	0	0	-2	1	2	0	2	-1
c_5	0	0	-4	-1	2	2	-4	1

$|k:\mathbb{Q}| = 4$

$\mathbf{d_k = 3981}, f(x) = x^4 - x^3 - 4x^2 + 2x + 1$

$\sigma_1,\ \Delta(A) = \mathcal{P}_3, A = \left(\frac{-(1+\alpha), -1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
c_1	0	0	2	-1	0	0	1	-3	1	-2	2	4	-2
c_2	0	-1	0	0	0	1	1	-3	1	-2	2	4	-2
c_3	0	-1	0	0	0	-1	-1	3	-1	2	-2	-4	2
c_4	0	0	2	-1	0	0	-1	3	-1	2	-2	-4	2
c_5	0	0	0	0	0	2	0	0	0	0	0	0	0

$\sigma_2,\ \Delta(A) = \mathcal{P}_3, A = \left(\frac{-\alpha(1+\alpha), -1}{\mathbb{Q}(\alpha)}\right), r = 2$

	x	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
c_1	0	-2	4	1	-1	2	-4	-1	1	-3	4	1	-1
c_2	0	0	0	0	2	0	0	0	0	0	0	0	0
c_3	0	-2	4	1	-1	-2	4	1	-1	3	-4	-1	1
c_4	0	-3	4	1	-1	-17	18	7	-5	36	-39	-15	11
c_5	0	0	0	0	0	20	-22	-8	6	-42	50	18	-14

$\mathbf{d_k = 3981}, f(x) = x^4 - x^3 - 4x^2 + 2x + 1$

$\sigma_3,\ \Delta(A) = \mathcal{P}_3, A = \left(\frac{\alpha(2-\alpha),-1}{\mathbb{Q}(\alpha)}\right), r \;=\; 2$

	x	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
c_1	0	1	4	0	-1	-2	-4	0	1	-1	4	2	-1
c_2	0	-1	4	1	-1	-2	-5	0	1	2	4	0	-1
c_3	0	0	0	0	0	-4	-8	0	2	4	8	0	-2
c_4	0	-1	4	1	-1	2	5	0	-1	-2	-4	0	1
c_5	0	0	0	0	2	0	0	0	0	0	0	0	0

$\sigma_4,\ \Delta(A) = \mathcal{P}_3, A = \left(\frac{(-2+\alpha),-1}{\mathbb{Q}(\alpha)}\right), r \;=\; 2$

	x	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
c_1	0	1	2	-1	-1	1	-1	-1	0	1	0	0	0
c_2	0	-1	0	0	0	1	2	-1	-1	-1	0	2	1
c_3	0	-1	0	0	0	-1	-2	1	1	1	0	-2	-1
c_4	0	1	2	-1	-1	-1	1	1	0	-1	0	0	0
c_5	0	0	0	0	2	0	0	0	0	0	0	0	0

5.3 Groups $\Gamma^1_{\mathcal{O}}$ with Signature (2;0)

The generators are those obtained from the Ford fundamental region.

$|k:\mathbb{Q}| = 1$

$$\Delta(A) = \{2, 13\}, A = \left(\frac{2,13}{\mathbb{Q}}\right), r = 2$$

	x	y	u	v
h_1	3	-3	-1	-1
h_2	3	-3	-1	1
h_3	3	-3	1	-1
h_4	3	-3	1	1
h_5	5	-2	-1	0
h_6	5	-2	1	0
h_7	6	-4	0	0
h_8	7	-4	-1	0
h_9	7	-4	1	0

$|k:\mathbb{Q}| = 2$

$\mathbf{d_k = 5}$

$$\Delta(A) = \mathcal{P}_{61}, A = \left(\frac{\frac{1+\sqrt{5}}{2}, -9+2\sqrt{5}}{\mathbb{Q}(\sqrt{5})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	5	3	-3	-1	0	0	-1	-1
h_2	2	2	-4	0	0	0	0	0
h_3	5	3	-3	-1	0	0	1	1
h_4	5	1	-6	-4	-4	-2	0	0
h_5	6	4	-2	0	0	0	3	1
h_6	6	4	-2	0	0	0	-3	-1
h_7	5	1	-6	-4	4	2	0	0

$\mathbf{d_k = 5}$

$$\Delta(A) = \mathcal{P}'_{61}, A = \left(\frac{\frac{1+\sqrt{5}}{2}, -9-2\sqrt{5}}{\mathbb{Q}(\sqrt{5})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	2	2	-4	0	0	0	0	0
h_2	3	1	-3	-3	-1	-1	0	0
h_3	3	1	-3	-3	1	1	0	0
h_4	7	3	-5	-1	0	0	-2	0
h_5	7	3	-5	-1	0	0	2	0
h_6	9	3	-1	1	0	0	-1	-1
h_7	9	3	-1	1	0	0	1	1

$\mathbf{d_k = 8}$

$$\Delta(A) = \mathcal{P}_5, A = \left(\frac{\sqrt{2}, -5}{\mathbb{Q}(\sqrt{2})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	2	2	-4	-1	-2	-2	-2	-1
h_2	2	2	-4	-1	2	2	-2	-1
h_3	4	2	-2	-1	0	0	0	-1
h_4	6	2	-4	-3	-2	-2	2	1
h_5	6	2	-4	-3	2	2	2	1
h_6	8	4	-2	0	0	0	-2	-2
h_7	8	4	-2	0	0	0	2	2
h_8	8	6	-4	-5	0	0	2	1
h_9	8	8	-6	-4	0	0	2	2

$\mathbf{d_k = 12}$

$$\Delta(A) = \mathcal{P}_{13}, A = \left(\frac{1+\sqrt{3}, -4+\sqrt{3}}{\mathbb{Q}(\sqrt{3})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	4	2	-3	-1	2	2	1	1
h_2	6	2	-3	-1	4	2	3	1
h_3	2	2	-2	-2	2	2	0	0
h_4	2	2	-1	1	-4	-2	-3	-1
h_5	6	4	-1	-3	0	0	1	1
h_6	2	2	-2	-2	-2	-2	0	0
h_7	4	2	-3	-1	-2	-2	1	1
h_8	6	2	-3	-1	-4	-2	3	1
h_9	2	2	-1	1	4	2	-3	-1

$$\Delta(A) = \mathcal{P}'_{13}, A = \left(\frac{-1+\sqrt{3}, -4-\sqrt{3}}{\mathbb{Q}(\sqrt{3})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	2	2	-1	-1	-2	0	1	1
h_2	2	2	-1	-1	2	0	1	1
h_3	4	4	-4	-2	-2	-2	-4	-2
h_4	4	4	-4	-2	2	2	-4	-2
h_5	6	4	-9	-5	-2	-2	3	1
h_6	6	4	-9	-5	2	2	3	1
h_7	8	6	-9	-5	0	0	-3	-1

$\mathbf{d_k = 13}$

$$\Delta(A) = \mathcal{P}_{13}, A = \left(\frac{\frac{3+\sqrt{13}}{2}, \frac{-13+3\sqrt{13}}{2}}{\mathbb{Q}(\sqrt{13})}\right), r = 4$$

	x_1	x_2	y_1	y_2	u_1	u_2	v_1	v_2
h_1	1	1	-9	-1	-11	-3	0	0
h_2	1	1	-9	-1	11	3	0	0
h_3	3	1	-2	0	0	0	-2	0
h_4	3	1	-2	0	0	0	2	0
h_5	10	2	-2	-2	0	0	0	0
h_6	20	6	-3	1	0	0	-11	-3
h_7	20	6	-3	1	0	0	11	3

$|k:\mathbb{Q}| = 3$

$\mathbf{d_k = 148}, f(x) = x^3 - x^2 - 3x + 1$

$\alpha_1 \sim -1.1481,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_{13}, A = \left(\frac{1-4\alpha, -\alpha(1+\alpha)}{k}\right), r = 2$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	-1	-1	1	3	1	-1	0	0	0	0	0	0
h_2	1	-3	1	3	1	-1	-2	1	0	2	-1	0
h_3	1	-3	1	3	1	-1	2	-1	0	-2	1	0
h_4	1	-3	1	3	1	-1	2	-1	0	2	-1	0
h_5	1	-3	1	3	1	-1	-2	1	0	-2	1	0
h_6	2	-1	0	2	-1	0	0	4	-2	0	0	0
h_7	2	-1	0	2	-1	0	0	-4	2	0	0	0

$\alpha_2 \sim 0.3111,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_{13}, A = \left(\frac{2-\alpha^2, (1-4\alpha)(1+\alpha)}{k}\right), r = 2$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	-13	-2	4	3	1	-1	0	0	0	15	4	-5
h_2	-2	-1	1	1	-1	0	0	0	0	0	0	0
h_3	-13	-2	4	3	1	-1	0	0	0	-15	-4	5
h_4	-4	0	1	12	3	-4	29	6	-9	0	0	0
h_5	-12	-3	4	-1	0	0	0	0	0	15	4	-5
h_6	-12	-3	4	-1	0	0	0	0	0	-15	-4	5
h_7	-4	0	1	12	3	-4	-29	-6	9	0	0	0

$\alpha_3 \sim 2.1700,\ \Delta(A) = \mathcal{P}_2\mathcal{P}_{13}, A = \left(\frac{-2+\alpha, -(-1+4\alpha)(1+\alpha)}{k}\right), r = 2$

	x_1	x_2	x_3	y_1	y_2	y_3	u_1	u_2	u_3	v_1	v_2	v_3
h_1	0	-1	0	1	-1	-1	3	1	-1	0	0	0
h_2	0	-1	0	1	-1	-1	-3	-1	1	0	0	0
h_3	-1	1	1	-1	0	0	0	0	0	2	0	-1
h_4	-1	1	1	-1	0	0	0	0	0	-2	0	1
h_5	0	4	2	2	-8	-6	0	0	0	0	0	0
h_6	-3	9	7	9	-20	-18	0	0	0	2	0	-1
h_7	-3	9	7	9	-20	-18	0	0	0	-2	0	1

$|k:\mathbb{Q}|=4$

$\mathbf{d_k = 725}$, $f(x) = x^4 - x^3 - 3x^2 + x + 1$

$\sigma_1 \sim -1.3556, \Delta(A) = \mathcal{P}_{61}, A = \left(\frac{-2(\alpha+1), -1+2\alpha-2\alpha^2}{\mathbb{Q}(\alpha)}\right), r \ = \ 4$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	2	2	-2	0	-1	3	1	-1	0	0	0	0	1	-3	-1	1
h_2	6	4	-20	8	11	1	-26	11	0	0	0	0	1	-1	-2	1
h_3	6	-2	-22	10	10	1	-26	11	0	0	0	0	2	-1	-2	1
h_4	0	4	-6	2	0	0	-6	3	0	0	0	0	0	0	-2	1
h_5	2	-2	-8	4	-2	1	8	-4	0	0	0	0	2	-1	0	0
h_6	2	-2	-8	4	-2	-3	8	-3	0	-4	-2	2	-2	1	2	-1
h_7	2	-2	-8	4	-2	-3	8	-3	0	4	2	-2	-2	1	2	-1
h_8	2	-2	0	0	-1	3	3	-2	0	0	-4	2	1	1	-5	2
h_9	2	-2	0	0	-1	3	3	-2	0	0	4	-2	1	1	-5	2

$\sigma_4 \sim 2.0952, \Delta(A) = \mathcal{P}_{61}, A = \left(\frac{\alpha-1, -1+2\alpha-2\alpha^2}{\mathbb{Q}(\alpha)}\right), r \ = \ 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	0	-1	-1	0	-1	1	1	0	0	0	0	0	-2	-3	0	1
h_2	2	0	-2	0	-2	-2	0	0	0	0	0	0	0	0	0	0
h_3	0	-1	-1	0	1	-1	-1	0	0	0	0	0	-2	-3	0	1
h_4	0	-1	0	0	1	0	-1	0	0	-3	-1	1	0	0	0	0
h_5	0	-1	1	1	-2	-1	1	0	0	0	0	0	-1	-4	-1	1
h_6	0	-1	1	1	2	1	-1	0	0	0	0	0	-1	-4	-1	1
h_7	0	-1	0	0	1	0	-1	0	0	3	1	-1	0	0	0	0

$\mathbf{d_k = 725}$, $f(x) = x^4 - x^3 - 3x^2 + x + 1$

$\sigma_1 \sim -1.3556, \Delta(A) = \mathcal{P}'_{61}, A = \left(\frac{-\alpha-1,-2-2\alpha-\alpha^2}{\mathbb{Q}(\alpha)}\right), r = 2$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	0	2	-1	0	0	0	2	-1	0	0	0	0	-2	1	2	-1
h_2	2	-2	-4	2	0	0	4	-2	0	0	0	0	0	0	0	0
h_3	0	2	-1	0	0	0	2	-1	0	0	0	0	2	-1	-2	1
h_4	1	-1	0	0	-1	-1	3	-1	0	-2	1	0	0	0	0	0
h_5	1	1	-3	1	-1	0	0	0	0	0	0	0	-3	2	6	-3
h_6	1	1	-3	1	-1	0	0	0	0	0	0	0	3	-2	-6	3
h_7	1	-1	0	0	-1	-1	3	-1	0	2	-1	0	0	0	0	0

$\sigma_4 \sim 2.0952, \Delta(A) = \mathcal{P}'_{61}, A = \left(\frac{2(\alpha-1),-2-2\alpha-\alpha^2}{\mathbb{Q}(\alpha)}\right), r = 4$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	2	0	-2	0	0	4	1	-1	0	0	0	0	-2	-1	1	0
h_2	2	0	-2	0	2	4	0	-2	-2	4	2	-2	0	0	0	0
h_3	0	-2	-2	0	2	2	0	-1	0	0	0	0	2	0	-1	0
h_4	2	0	-2	0	-2	-4	0	2	-2	4	2	-2	0	0	0	0
h_5	0	-2	0	0	0	2	0	-1	0	2	0	0	2	0	-1	0
h_6	0	0	-2	0	1	6	1	-2	0	0	0	0	1	-2	-1	1
h_7	0	-2	0	0	0	2	0	-1	0	-2	0	0	2	0	-1	0
h_8	-4	2	6	2	0	-1	2	2	0	0	0	0	-1	-2	0	0
h_9	-2	-4	4	4	-3	-4	2	3	0	0	0	0	1	-3	-2	1

$\mathbf{d_k = 2304}$, $f(x) = x^4 - 4x^2 + 1$

$\Delta(A) = \mathcal{P}_3, A = \left(\frac{-1+\alpha,-(-2+\alpha^2)(1-\alpha-\alpha^2)}{\mathbb{Q}(\alpha)}\right), r = 2(-1 + \alpha)$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	-2	-1	0	0	0	0	0	0	3	0	-1	1	0	-1	0
h_2	1	-2	-1	0	0	0	0	0	0	-3	0	1	1	0	-1	0
h_3	1	0	-1	0	0	-1	0	0	1	-1	0	0	-1	0	0	0
h_4	1	0	-1	0	0	-1	0	0	-1	1	0	0	-1	0	0	0
h_5	1	-2	0	1	0	-1	0	0	0	3	0	-1	0	1	0	0
h_6	1	-2	0	1	0	-1	0	0	0	-3	0	1	0	1	0	0
h_7	0	-1	0	1	1	-2	-1	0	0	3	0	-1	0	0	0	0
h_8	0	-1	0	1	1	-2	-1	0	0	-3	0	1	0	0	0	0

$\mathbf{d_k = 4752}, f(x) = x^4 - 2x^3 - 3x^2 + 4x + 1$

$\alpha_1 \sim -1.4955, \Delta(A) = \mathcal{P}_2, A = \left(\frac{-1-\alpha,(1-\alpha)(-1+\alpha+\alpha^2)}{\mathbb{Q}(\alpha)}\right), r = 2(1+\alpha)$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	1	0	-1	0	-1	0	0	0	0	0	0	0	0	4	1	-1
h_2	0	-2	-1	1	-1	3	1	-1	0	0	0	0	-1	-2	1	0
h_3	0	-4	0	1	1	-1	0	0	1	3	1	-1	1	2	-1	0
h_4	0	-4	0	1	1	-1	0	0	-1	-3	-1	1	1	2	-1	0
h_5	1	0	-1	0	0	3	-1	0	1	1	2	-1	0	-1	-2	1
h_6	1	0	-1	0	0	3	-1	0	-1	-1	-2	1	0	-1	-2	1
h_7	1	2	-2	0	2	2	-1	0	0	0	0	0	-1	-1	3	-1
h_8	0	-1	-3	1	-1	3	-1	0	0	0	0	0	0	-1	3	-1
h_9	1	1	-2	1	0	3	-1	0	0	0	0	0	0	-5	2	0

$\alpha_2 \sim -0.2197, \Delta(A) = \mathcal{P}_2, A = \left(\frac{-\alpha(1+\alpha),(1-\alpha)(-1+\alpha+\alpha^2)}{\mathbb{Q}(\alpha)}\right), r = 2(1+\alpha)$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4
h_1	3	-3	-2	1	-11	4	5	-2	-3	3	2	-1	-4	3	2	-1
h_2	3	-3	-2	1	-11	4	5	-2	3	-3	-2	1	-4	3	2	-1
h_3	3	-3	-2	1	-8	5	4	-2	-4	7	3	-2	11	-8	-6	3
h_4	3	-3	-2	1	-8	5	4	-2	4	-7	-3	2	11	-8	-6	3
h_5	3	-3	-2	1	-6	2	3	-1	0	0	0	0	-4	-1	1	0
h_6	2	-4	-2	1	-1	0	0	0	0	0	0	0	4	-3	-2	1
h_7	6	-5	-3	2	-15	7	7	-3	0	0	0	0	1	-4	-1	1
h_8	6	-5	-3	2	-15	7	7	-3	0	0	0	0	-1	4	1	-1
h_9	4	-2	-2	1	-7	6	4	-2	0	0	0	0	4	-3	-2	1

Appendices

Appendix A

Lists of Number Fields

The following is a list of all the totally real number fields of degree less than or equal to six that are considered in the proof of Theorem 2.2.1. We list each field by its defining polynomial, and discriminant. This information is obtained from [4].

A.1 Degree Three

$x^3 - x^2 - 2x + 1, 49$

$x^3 - 3x - 1, 81$

$x^3 - x^2 - 3x + 1, 148$

$x^3 - x^2 - 4x - 1, 169$

$x^3 - 4x + 1, 229$

$x^3 - x^2 - 4x + 3, 257$

$x^3 - x^2 - 4x + 2, 316$

$x^3 - x^- 4x + 1, 321$

$x^3 - x^2 - 6x + 7, 361$

$x^3 - x^2 - 5x - 1, 404$

$x^3 - x^2 - 5x + 4, 469$

$x^3 - 5x - 1, 473$

$x^3 - x^2 - 5x + 3, 564$

$x^3 - x^2 - 6x - 2, 568$

$x^3 - 6x - 3, 621$

$x^3 - 7x - 5, 697$

$x^3 - x^2 - 7x + 8, 733$

$x^3 - 6x - 2, 756$

$x^3 - x^2 - 6x - 1, 761$

$x^3 - x^2 - 6x + 5, 785$

$x^3 - x^2 - 7x - 3, 788$

$x^3 - 6x - 1, 837$

$x^3 - x^2 - 8x + 10, 892$

$x^3 - 7x - 4, 940$

$x^3 - x^2 - 10x + 8, 961$

A.2 Degree Four

$x^4 - x^3 - 3x^2 + x + 1, 725$

$x^4 - x^3 - 4x^2 + 4x + 1, 1125$

$x^4 - 6x^2 + 4, 1600$

$x^4 - 4x^2 - x + 1, 1957$

$x^4 - 5x^2 + 5, 2000$

$x^4 - 4x^2 + 2, 2048$

$x^4 - x^3 - 5x^2 + 2x + 4, 2225$

$x^4 - 4x^2 + 1, 2304$

$x^4 - 2x^3 - 4x^2 + 5x + 5, 2525$

$x^4 - 2x^3 - 3x^2 + 2x + 1, 2624$

$x^4 - x^3 - 4x^2 + x + 2, 2777$

$x^4 - 2x^3 - 7x^2 + 8x + 1, 3600$

$x^4 - x^3 - 4x^2 + 2x + 1, 3981$

$x^4 - x^3 - 5x^2 - x + 1, 4205$

$x^4 - 9x^2 + 4, 4225$

$x^4 - 6x^2 - 4x + 2, 4352$

$x^4 - 7x^2 + 11, 4400$

$x^4 - x^3 - 7x^2 + 3x + 9, 4525$

$x^4 - 2x^3 - 3x^2 + 4x + 1, 4752$

$x^4 - x^3 - 6x^2 + x + 1, 4913$

$x^4 - 2x^3 - 6x^2 + 7x + 11, 5125$

$x^4 - x^3 - 8x^2 + x + 11, 5225$

$x^4 - x^3 - 8x^2 + 6x + 11, 5725$

$x^4 - 5x^2 - 2x + 1, 5744$

$x^4 - x^3 - 9x^2 + 9x + 11, 6125$

$x^4 - 6x^2 - 2x + 5, 6224$

$x^4 - 5x^2 - x + 1, 6809$

$x^4 - 2x^3 - 4x^2 + 3x + 3, 7053$

$x^4 - 5x^2 + 1, 7056$

$x^4 - 6x^2 + 7, 7168$

$x^4 - 11x^2 + 9, 7225$

$x^4 - 2x^3 - 5x^2 + 4x + 4, 7232$

$x^4 - 2x^3 - 4x^2 + 2x + 1, 7488$

$x^4 - x^3 - 5x^2 + 4x + 3, 7537$

$x^4 - 9x^2 + 19, 7600$

$x^4 - x^3 - 9x^2 + 4x + 16, 7625$

$x^4 - 10x^2 + 20, 8000$

$x^4 - x^3 - 5x^2 + 5x + 1, 8069$

$x^4 - 5x^2 + 3, 8112$

$x^4 - x^3 - 5x^2 + 3x + 4, 8468$

$x^4 - 2x^3 - 8x^2 + 9x + 19, 8525$

$x^4 - x^3 - 10x^2 + 2x + 19, 8725$

$x^4 - 2x^3 - 5x^2 + 6x + 7, 8768$

$x^4 - x^3 - 6x^2 - 2x + 1, 8789$

$x^4 - x^3 - 5x^2 + x + 1, 8957$

$x^4 - x^3 - 10x^2 + 7x + 19, 9225$

$x^4 - 5x^2 + 2, 9248$

$x^4 - x^3 - 5x^2 + x + 3, 9301$

A.3 Degree Five

$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1, 14641$

$x^5 - 5x^3 - x^2 + 3x + 1, 24217$

$x^5 - 2x^4 - 3x^3 + 5x^2 + x - 1, 36497$

$x^5 - 5x^3 + 4x - 1, 38569$

$x^5 - x^4 - 5x^3 + 2x^2 + 5x + 1, 65657$

$x^5 - x^4 - 5x^3 + 2x^2 + 3x - 1, 70601$

$x^5 - x^4 - 5x^3 + 3x^2 + 5x - 2, 81509$

$x^5 - 6x^3 + 8x - 1, 81589$

$x^5 - 6x^3 - x^2 + 8x + 3, 89417$

$x^5 - x^4 - 5x^3 + 5x^2 + 2x - 1, 101833$

$x^5 - 2x^4 - 4x^3 + 7x^2 + 3x - 4, 106069$

$x^5 - x^4 - 5x^3 + 4x^2 + 4x - 1, 117688$

$x^5 - 2x^4 - 4x^3 + 4x^2 + 3x - 1, 122821$

$x^5 - 7x^3 - 6x^2 + 2x + 1, 124817$

$x^5 - 6x^3 + 6x - 2, 126032$

A.4 Degree Six

$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1, 300125$

$x^6 - x^5 - 5x^4 + 4x^3 + 6x^2 - 3x - 1, 371293$

$x^6 - 2x^5 - 4x^4 + 5x^3 + 4x^2 - 2x - 1, 434581$

$x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1, 453789$

$x^6 - 2x^5 - 4x^4 + 8x^3 + 2x^2 - 5x + 1, 485125$

$x^6 - x^5 - 5x^4 + 4x^3 + 5x^2 - 2x - 1, 592661$

$x^6 - 2x^5 - 5x^4 + 11x^3 + 2x^2 - 9x + 1, 703493$

$x^6 - x^5 - 6x^4 + 7x^3 + 4x^2 - 5x + 1, 722000$

$x^6 - 3x^5 - 2x^4 + 9x^3 - 5x + 1, 810448$

$x^6 - 9x^4 - 4x^3 + 9x^2 + 3x - 1, 820125$

$x^6 - x^5 - 7x^4 + 9x^3 + 7x^2 - 9x - 1, 905177$

$x^6 - x^5 - 6x^4 + 4x^3 + 8x^2 - 1, 966125$

$x^6 - x^5 - 6x^4 + 6x^3 + 7x^2 - 5x - 1, 980125$

$x^6 - 7x^4 + 14x^2 - 7, 1075648$

$x^6 - 6x^4 - 2x^3 + 7x^2 + 2x - 1, 1081856$

$x^6 - 2x^5 - 4x^4 + 6x^3 + 4x^2 - 3x - 1, 1134389$

$x^6 - 6x^4 - 2x^3 + 6x^2 + x - 1, 1202933$

$x^6 - 10x^4 + 24x^2 - 8, 1229312$

$x^6 - 7x^4 - 2x^3 + 11x^2 + 7x + 1, 1241125$

$x^6 - 6x^4 + 9x^2 - 3, 1259712$

Appendix B

Mathematica Programs

Here we give example programs used to compute the unit groups in Chapter 4. The programs are specific to the number fields and the maximal orders. This is evident in the appearance of the congruence relations on the integers and the algebraic simplification of the norm.

B.1 Example program for quadratic case

```
quad[r_, e_, d_, t_, tb_, s_, sb_, r1_, r2_] := Module[{list1},
  Ne = 2 + 4/(e^2); A1 = r/2*(1 + Sqrt[Ne/2]); list1 = {};
For[i = 0, i  Ceiling[A1], i++, LA2 = (i -r)/Sqrt[d];
  UA2 = (i + r)/Sqrt[d];
For[j = Floor[LA2], j  Ceiling[UA2], j++,
  Ba = N[Sqrt[(r^2 - (i - j*Sqrt[d])^2)/(-tb)]];
  B1 = 1/2*(Ba + Sqrt[(r^2*Ne - 2*(i + j*Sqrt[d])^2)/(2*t)]);
    If[Im[B1] == 0,
For[k = Floor[-B1], k  Ceiling[B1], k++,
  LB2 = (k - Ba)/Sqrt[d]; UB2 = (k + Ba)/Sqrt[d];
For[l = Floor[LB2], l  Ceiling[UB2], l++,
  Da = N[Sqrt[(Simplify[r^2 - Expand[(i -j*Sqrt[d])^2]
    + tb*Expand[(k - l*Sqrt[d])^2]])/(sb*tb)]];
  D1 = 1/2*(Da + Sqrt[(r1^2 + r2^2)*(r^2*Ne
    - 2*Expand[(i + j*Sqrt[d])^2]
    - 2*t*Expand[(k + l*Sqrt[d])^2])/(4*s^2*t)];
    If[Im[D1] == 0,
For[o = Floor[-D1], o  Ceiling[D1], o++,
 LD2 = (o - Da)/Sqrt[d]; UD2 = (o + Da)/Sqrt[d];
For[p = Floor[LD2], p  Ceiling[UD2], p++, If[Mod[i, 2] == 0
  && Mod[j, 2] == 0 && Mod[k,2] == 0 && Mod[o, 2] == 0
```

```
  && Mod[l + p, 2] == 0,
  Ca = N[Sqrt[Simplify[(r^2 - Expand[(i - j*Sqrt[d])^2]
    + tb*Expand[(k - l*Sqrt[d])^2]
    - sb*tb*Expand[(o - p*Sqrt[d])^2])/(-sb)]]];
  C1 = 1/2*(Ca + (Sqrt[(1/(r1^2 + r2^2))*( r^2*Ne -
    2*Expand[(i + j*Sqrt[d])^2] - 2*t*Expand[(k + l*Sqrt[ d])^2]
    - (4*s^2*t*Expand[(m + n*Sqrt[d])^2])/(r1^2 + r2^2))])
    + (Abs[r1^2 - r2^2]/(r1^2 + r2^2))*Sqrt[t]*Abs[o + p*Sqrt[d]]);
    If[Im[C1] == 0,
For[m = Floor[-C1], m  Ceiling[C1], m++,
  LC2 = (m - Ca)/Sqrt[d]; UC2 = (m + Ca)/Sqrt[d];
For[p = Floor[LC2], p  Ceiling[UC2], p++,
  If[Mod[m, 2] == 0 && Mod[n, 2] == 0 && Mod[i - m, 4] == 0
    && Mod[j - 2*p - m - n, 4] == 0 && Mod[k - 2*p - o, 4] == 0
    && Mod[l - o - p - m, 4] == 0
    &&Simplify[Expand[(i +  j*Sqrt[d])^2]
      - t*Expand[( k + l*Sqrt[d])^2] - s*Expand[(m + n*Sqrt[d])^2]
      + s*t*Expand[(o + p*Sqrt[d])^2]] == r^2,
        list1 = Append[list1, {i, j, k, l, m, n, o, p }]]
                          ]]]]]]]]]]]; list1
      ];
```

B.2 Example program for cubic case

```
cubic[R_, e_, w1_, w2_, w3_, t1_, t2_, t3_, s1_, s2_, s3_,R1_, R2_]
  := Module[{list1}, list1 = {}; Ne = 2 + 4/(e^2);
  Aw1 = R*Sqrt[Ne/2];
  A3 = Min[N[1/Abs[w2 - w1]*(2*R/Abs[w2 - w3]
    + (R + Aw1)/Abs[w1 - w3])],
    N[1/Abs[w3 - w1]*(2*R/Abs[w2 - w3] + (R + Aw1)/Abs[w1 - w2])],
    N[1/Abs[w2 - w3]*((R + Aw1)/Abs[w2 - w1]
    + (R + Aw1)/Abs[w1 - w3])]];
  list1 = {};
For[k = 0, k  Ceiling[A3], k++,
  UA2 = Min[N[2*R/Abs[w2 - w3] - k*(w2 + w3)],
    N[(Aw1 + R)/Abs[w1 - w3] - k*(w1 + w3)],
    N[(R + Aw1)/Abs[w2 - w1] - k*(w2 + w1)]];
  LA2 = Max[N[-2*R/Abs[w2 - w3] - k*(w2 + w3)],
```

```
    N[-(Aw1 + R)/Abs[w1 - w3] - k*(w1 + w3)],
    N[-(R + Aw1)/Abs[w2 - w1] - k*(w2 + w1)]];
For[j = Floor[LA2], j  Ceiling[UA2], j++,
  UA1 = Min[N[Aw1 - (j*w1 + k*w1^2)], N[R - (j*w2 + k*w2^2)],
    N[R - (j*w3 + k*w3^2)]];
  LA1 =Max[N[-Aw1 - (j*w1 + k*w1^2)], N[-R - (j*w2 + k*w2^2)],
    N[-R - (j*w3 + k*w3^2)]];
For[i = Floor[LA1], i  Ceiling[UA1], i++,
  Bw2 = N[Sqrt[(R^2 - Expand[(i + j*w2 + k*w2^2)^2])/(-t2)]];
  Bw3 = N[Sqrt[(R^2 - Expand[(i + j*w3 + k*w3^2)^2])/(-t3)]];
  Bw1 = N[Sqrt[(R^2*Ne - 2*(i + j*w1 + k*w1^2)^2)/(2*t1)]];
    If[Im[Bw2] == 0 && Im[Bw3] == 0 &&Im[Bw1] == 0,
      B3 = Min[N[1/Abs[w2 - w1]*((Bw2 + Bw3)/Abs[w2 -w3]
        + (Bw1 + Bw3)/Abs[w1 - w3])],
        N[1/Abs[w2 - w3]*((Bw2 + Bw1)/ Abs[w2 - w1]
        + (Bw1 + Bw3)/Abs[w1 - w3])],
        N[1/Abs[w3 - w1]*((Bw2 + Bw3)/Abs[w2 - w3]
        + (Bw1 + Bw2)/Abs[w1 - w2])]];
For[n = Floor[-B3], n  Ceiling[B3], n++,
  UB2 = Min[N[(Bw2 +Bw3)/Abs[w2 - w3] - n*(w2 + w3)],
    N[(Bw1 + Bw3)/Abs[w1 - w3] - n*(w1 + w3)],
    N[(Bw2 + Bw1)/Abs[w2 - w1] - n*(w2 + w1)]];
  LB2 = Max[N[-(Bw2 + Bw3)/Abs[w2 - w3] - n*(w2 + w3)],
    N[-(Bw1 + Bw3)/Abs[w1 - w3] - n*(w1 + w3)],
    N[-(Bw2 + Bw1)/Abs[w2 - w1] - n*(w2 + w1)]];
For[m = Floor[LB2], m  Ceiling[UB2], m++,
  UB1 = Min[N[Bw1 - (m*w1 + n*w1^2)], N[Bw2 - (m*w2 + n*w2^2)],
    N[Bw3 - (m*w3 + n*w3^2)]];
  LB1 = Max[N[-Bw1 - (m*w1 + n*w1^2)],
    N[-Bw2 - (m*w2 + n*w2^2)], N[-Bw3 - (m*w3 + n*w3^2)]];
For[l = Floor[LB1], l  Ceiling[UB1], l++,
  Dw2 = N[Sqrt[(R^2 - Expand[(i + j*w2 + k*w2^2)^2]
    + t2*Expand[(l + m*w2 + n*w2^2)^2])/(s2*t2)]];
  Dw3 = N[Sqrt[(R^2 - Expand[(i + j*w3 + k*w3^2)^2]
    + t3*Expand[(l + m*w3 + n*w3^2)^2])/(s3*t3)]];
  Dw1 = N[Sqrt[(R1^2 + R2^2)*(R^2*Ne
    - 2*Expand[(i + j*w1 + k*w1^2)^2] - 2*t1*Expand[(l + m*w1 +
    n*w1^2)^2])/(4*s1^2*t1)]];
       If[Im[Dw2] == 0 && Im[Dw3] == 0 && Im[Dw1] == 0,
```

```
         D3 = Min[N[1/Abs[w2 -w1]*((Dw2 + Dw3)/Abs[w2 - w3]
           + (Dw1 + Dw3)/Abs[w1 - w3])],
           N[1/Abs[w2 - w3]*((Dw2 + Dw1)/Abs[w2 - w1]
           + (Dw1 + Dw3)/Abs[w1 - w3])],
           N[1/Abs[w3 - w1]*((Dw2 + Dw3)/Abs[w2 - w3]
           + (Dw1 + Dw2)/Abs[w1 - w2])]];
For[t = Floor[-D3], t  Ceiling[D3], t++,
  UD2 = Min[N[(Dw2 + Dw3)/Abs[w2 - w3] - t*(w2 + w3)],
    N[(Dw1 + Dw3)/Abs[w1 - w3] - t*(w1 + w3)],
    N[(Dw2 + Dw1)/Abs[w2 - w1] - t*(w2 + w1)]];
  LD2 = Max[N[-(Dw2 + Dw3)/Abs[w2 - w3] - t*(w2 + w3)],
    N[-(Dw1 + Dw3)/Abs[w1 - w3] - t*(w1 + w3)],
    N[-(Dw2 + Dw1)/Abs[w2 - w1] - t*(w2 + w1)]];
For[s = Floor[LD2], s  Ceiling[UD2], s++,
  UD1 = Min[N[Dw1 - (s*w1 + t*w1^2)],
    N[Dw2 - (s*w2 + t*w2^2)], N[Dw3 - (s*w3 + t*w3^2)]];
  LD1 = Max[N[-Dw1 - (s*w1 + t*w1^2)],
    N[-Dw2 - (s*w2 + t*w2^2)], N[-Dw3 - (s*w3 + t*w3^2)]];
For[r = Floor[LD1], r  Ceiling[UD1], r++,
  Cw2 = N[Sqrt[(R^2 - Expand[(i + j*w2 + k*w2^2)^2]
    + t2*Expand[(l + m*w2 + n*w2^2)^2]
    - s2*t2*Expand[(r + s*w2 + t*w2^2)^2])/(-s2)]];
  Cw3 = N[Sqrt[(R^2 - Expand[(i + j*w3 + k*w3^2)^2]
    + t3*Expand[(l + m*w3 + n*w3^2)^2]
    - s3*t3*Expand[(r + s*w3 + t*w3^2)^2])/(-s3)]];
  Cw1 = N[Sqrt[(1/(R1^2 + R2^2))*(R^2*Ne
    - 2*Expand[(i + j*w1 + k*w1^2)^2]
    - 2*t1*Expand[(l + m*w1 + n*w1^2)^2]
    - (4*s1^2*t1*Expand[(r + s*w1 + t*w1^2)^2])/(R1^2 + R2^2))]
    + Abs[R1^2 - R2^2]/(R1^2 + R2^2)*
    Sqrt[t1]*Abs[r +  s*w1 + t*w1^2]];
      If[Im[Cw2] == 0 && Im[Cw3] == 0 && Im[Cw1] == 0,
        C3 = Min[N[1/Abs[w2 - w1]*((Cw2 + Cw3)/Abs[w2 - w3]
          + (Cw1 + Cw3)/Abs[w1 - w3])],
          N[1/Abs[w3 - w1]*((Cw2 + Cw3)/Abs[w2 - w3]
          + (Cw1 + Cw2)/Abs[w1 - w2])],
          N[1/Abs[w2 - w3]*((Cw2 + Cw1)/Abs[w2 - w1]
          + (Cw1 + Cw3)/Abs[w1 - w3])]];
For[q = Floor[-C3], q  Ceiling[C3], q++,
```

```
  If[Mod[q + k, 2] == 0 && Mod[n - q - t, 2] == 0,
    UC2 = Min[N[(Cw2 + Cw3)/Abs[w2 - w3] - q*(w2 + w3)],
      N[(Cw1 + Cw3)/Abs[w1 - w3] - q*(w1 + w3)],
      N[(Cw2 + Cw1)/Abs[w2 - w1] - q*(w2 + w1)]];
    LC2 = Max[N[-(Cw2 + Cw3)/Abs[w2 - w3] - q*(w2 + w3)],
      N[-(Cw1 + Cw3)/Abs[w1 - w3] - q*(w1 + w3)],
      N[-(Cw2 + Cw1)/Abs[w2 - w1] - q*(w2 + w1)]];
For[p = Floor[LC2], p  Ceiling[UC2], p++,
  If[Mod[p + j, 2] == 0 && Mod[m - p - s, 2] == 0,
    UC1 = Min[N[Cw1 - (p*w1 + q*w1^2)], N[Cw2 - (p*w2 + q*w2^2)],
      N[Cw3 - (p*w3 + q*w3^2)]];
    LC1 = Max[N[-Cw1 - (p*w1 + q*w1^2)],
      N[-Cw2 - (p* w2 + q*w2^2)],
      N[-Cw3 - (p*w3 + q*w3^2)]];
For[o = Floor[LC1], o  Ceiling[UC1], o++,
  If[Mod[o + i, 2] == 0&&Mod[l - o - r, 2] == 0,
    norm = Simplify[Expand[(Expand[(i + j*w + k*w^2)^2]
      - a*Expand[(l + m*w + n*w^2)^2] - b*Expand[(o + p*w +q*w^2)^2]
      + a*b*Expand[(r + s*w + t*w^2)^2] - R^2)
       /. {w^3 -> w^2 + 2*w - 1, w^4 -> 3*w^2 + w - 1,
         w^5 -> 4*w^2 + 5*w - 3}] /. {w^3 -> w^2 + 2*w - 1,
         w^4 -> 3*w^2 + w - 1, w^5 -> 4*w^2 + 5*w - 3}];
           If[norm == 0, list1 = Append[list1,
             {i, j, k, l, m,n, o, p, q, r, s, t}
               ]]]]]]]]]]]]]]]]]]]]; list1];
```

Bibliography

[1] P. Ackermann, M. Näätänen, and G. Rosenberger. The arithmetic Fuchsian groups with signature $(0; 2, 2, 2, q)$. In *Recent advances in group theory and low-dimensional topology (Pusan, 2000)*, volume 27 of *Res. Exp. Math.*, pages 1–9. Heldermann, Lemgo, 2003.

[2] A. Borel. Commensurability classes and volumes of hyperbolic 3-manifolds. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 8(1):1–33, 1981.

[3] Ted Chinburg and Eduardo Friedman. An embedding theorem for quaternion algebras. *J. London Math. Soc. (2)*, 60(1):33–44, 1999.

[4] H. Cohen et. al. List of number fields of degree ≤ 7. *available at ftp://math.u-bordeaux.fr/pub/number fields.*

[5] H. Cohen et. al. Pari. *Freeware available by anonymous FTP from megrez@math.u-bordeaux, directory pub/pari.*

[6] Allan L. Edmonds, John H. Ewing, and Ravi S. Kulkarni. Torsion free subgroups of Fuchsian groups and tessellations of surfaces. *Invent. Math.*, 69(3):331–346, 1982.

[7] Leon Greenberg. Maximal Fuchsian groups. *Bull. Amer. Math. Soc.*, 69:569–573, 1963.

[8] Stefan Johansson. Genera of arithmetic Fuchsian groups. *Acta Arith.*, 86(2):171–191, 1998.

[9] Stefan Johansson. On fundamental domains of arithmetic Fuchsian groups. *Math. Comp.*, 69(229):339–349, 2000.

[10] Svetlana Katok. *Fuchsian groups*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[11] C. Maclachlan and G. Rosenberger. Two-generator arithmetic Fuchsian groups. *Math. Proc. Cambridge Philos. Soc.*, 93(3):383–391, 1983.

[12] C. Maclachlan and G. Rosenberger. Two-generator arithmetic Fuchsian groups. II. *Math. Proc. Cambridge Philos. Soc.*, 111(1):7–24, 1992.

[13] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[14] A. M. Odlyzko. Some analytic estimates of class numbers and discriminants. *Invent. Math.*, 29(3):275–286, 1975.

[15] Charles J. Parry. Units of algebraic numberfields. *J. Number Theory*, 7(4):385–388, 1975.

[16] M. Pohst, J. Martinet, and F. Diaz y Diaz. The minimum discriminant of totally real octic fields. *J. Number Theory*, 36(2):145–159, 1990.

[17] Paulo Ribenboim. *Algebraic numbers*. Wiley-Interscience [A Division of John Wiley & Sons, Inc.], New York-London-Sydney, 1972. Pure and Applied Mathematics, Vol. 27.

[18] Volker Schneider. Die elliptischen Fixpunkte zu Modulgruppen in Quaternionenschiefkörpern. *Math. Ann.*, 217(1):29–45, 1975.

[19] Kisao Takeuchi. Commensurability classes of arithmetic triangle groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 24(1):201–212, 1977.

[20] Kisao Takeuchi. Arithmetic Fuchsian groups with signature $(1; e)$. *J. Math. Soc. Japan*, 35(3):381–407, 1983.

[21] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[22] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

Vita

Melissa Lorena Macasieb was born on February 8, 1974 in Belleville, New Jersey. In 1995, she received a B.A. in English Literature and Mathematics from Columbia College, Columbia University, in New York City. In 1998, she received her M.S. in Mathematics from New York University in New York City.

Permanent address: 603 East 43rd Street
Austin, Texas 78751

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.