Derived Arithmetic Fuchsian Groups of Genus Two

Melissa L. Macasieb

CONTENTS

We classify all cocompact 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 class of quaternion algebras related to these groups. Using these results in conjunction with a computer program, one can determine an explicit set of generators for each derived arithmetic Fuchsian group containing a torsion-free subgroup of genus two. We show this for a number of examples.

1. INTRODUCTION

It is a well-known result that there are finitely many conjugacy classes of arithmetic Fuchsian groups with a given signature [Maclachlan and Rosenberger 83, Takeuchi 83]. Extensive work has been done classifying the set of $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes of various two-generator arithmetic Fuchsian groups: triangle groups [Takeuchi 77], groups of signature $(1;e)$ [Takeuchi 83], and groups of signature $(0;2,2,2,q)$ [Maclachlan and Rosenberger 92, Ackermann et al. 03]. In this paper we make progress in classifying arithmetic Fuchsian groups of signature $(2;-)$, i.e., genus-two surface groups. This is a significantly more difficult problem than the two-generator case, since these groups have much larger coarea.

An arithmetic Fuchsian group is described by the (projectivized) group of units $\Gamma^1_{\mathcal{O}}$ in a maximal order $\mathcal{O}$ of a quaternion algebra over a totally real number field. A derived arithmetic Fuchsian group is a subgroup of such a $\Gamma^1_{\mathcal{O}}$. Our first main result is the classification by commensurability class of derived arithmetic Fuchsian groups of genus two, and this is summarized in Theorem 4.10. There is a finite list of signatures of groups that contain a subgroup of signature $(2;-)$.

Following [Maclachlan and Rosenberger 92], we classify all commensurability classes of derived arithmetic Fuchsian groups of the form $\Gamma^1_{\mathcal{O}}$ with one of these signatures by invariant quaternion algebra. Furthermore, we

2000 AMS Subject Classification: 57M50, 11R52

Keywords: Hyperbolic orbifolds, arithmetic Fuchsian groups, maximal orders

1058-6458/2008 $ 0.50 per page
Experimental Mathematics **17**:3, page 347

determine all $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes of the groups $\Gamma^1_{\mathcal{O}}$. Sections 3 and 4 of this paper are devoted to this result and its proof.

Section 5 contains our second main result, a technique for finding all $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes of derived arithmetic Fuchsian groups of signature $(2;-)$. In general, the number of conjugacy classes of a subgroup of $\Gamma^1_{\mathcal{O}}$ is not necessarily equal to the number of $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes of the group $\Gamma^1_{\mathcal{O}}$. However, if $\Gamma^1_{\mathcal{O}}$ has signature $(1;2,2)$, $(0;2,2,2,2,2,2)$, or $(2;-)$, then the index of the genus-two subgroup Γ is 4, 2, or 1, respectively. In these cases, we can use a fundamental region along with our results from Theorem 4.10 to determine an explicit set of generators for $\Gamma^1_{\mathcal{O}}$ (using a computer program). This ultimately pins down the $\mathrm{PGL}_2(\mathbb{R})$-conjugacy class of the genus-two subgroup Γ, since this is determined by the traces of certain products of the group generators. Although our methods are essentially computational, we also prove some general results on the structure of maximal orders for a class of quaternion algebras associated with arithmetic Fuchsian groups. In the last section, we use our results to explicitly determine a set of generators for a few examples of derived arithmetic Fuchsian groups of signature $(2;-)$.

2. PRELIMINARIES

In order to state and prove our main results, it is necessary to give a brief overview of the theory of arithmetic Fuchsian groups. This includes a small section of number theory consisting of definitions and results that will figure prominently in our proofs.

2.1 Fuchsian Groups

In this section we collect some standard results concerning Fuchsian groups. A Fuchsian group is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ that acts properly discontinuously on the hyperbolic plane $\mathbb{H}^2$. Fuchsian groups of the first kind have a presentation of the form

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

where the c_i represent the r conjugacy classes of maximal cyclic subgroups of order m_i for $i = 1, \ldots, r$. A Fuchsian group Γ with the above presentation has *signature*

$$(g; m_1, \ldots, m_r; s). \qquad (2\text{–}1)$$

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 $(g; m_1, \ldots, m_r)$. A finitely generated Fuchsian group Γ of the first kind has finite coarea, i.e., $\mathbb{H}^2/\Gamma$ has finite hyperbolic area, and its area can be computed using the Riemann–Hurwitz formula

$$\mu(\Gamma) := \mathrm{area}(\mathbb{H}^2/\Gamma) = 2\pi\Big(2g - 2 + \sum_{i=1}^{r} \frac{m_i - 1}{m_i} + s\Big). \qquad (2\text{–}2)$$

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

Also, recall that two Fuchsian groups Γ_1 and Γ_2 are *commensurable* if they share a finite-index subgroup, 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.

2.2 Arithmetic Fuchsian and Derived Arithmetic Fuchsian Groups

An arithmetic Fuchsian group has finite coarea and therefore is necessarily of the first kind. Arithmetic Fuchsian groups are defined via quaternion algebras over totally real number fields. If k is a number field and A a quaternion algebra over k, i.e., a four-dimensional central simple algebra over k, then any quaternion algebra has an associated Hilbert symbol

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

where $i^2 = a$, $j^2 = b$, $ij = -ji$ for some $a, b \in k^*$.

The algebra A is *ramified* at a real 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 will be denoted by $\mathrm{Ram}(A)$. Furthermore, $\mathrm{Ram}(A) = \mathrm{Ram}_\infty(A) \cup \mathrm{Ram}_f(A)$, where $\mathrm{Ram}_f(A)$ (respectively $\mathrm{Ram}_\infty(A)$) denotes the set of finite (infinite) places at which A is ramified. We will denote the product of the primes at which A is ramified by $\Delta(A)$.

We will use the following standard results on quaternion algebras (see [Maclachlan and Reid 03]):

(i) Let A be a quaternion algebra over a number field k. The number of places at which A is ramified is of even cardinality.

(ii) Given a number field k, a collection $S_1 = \{\sigma_1, \dots, \sigma_r\}$ of real infinite places of k, and a collection $S_2 = \{\mathcal{P}_1, \dots, \mathcal{P}_s\}$ of finite places of k such that $r+s$ is even, there exists a quaternion algebra defined over k with $\mathrm{Ram}_\infty(A) = S_1$ and $\mathrm{Ram}_f(A) = S_2$.

(iii) Let A and A' be quaternion algebras over a number field k. Then $A \cong A'$ if and only if $\mathrm{Ram}(A) = \mathrm{Ram}(A')$.

An *order* $\mathcal{O}$ of A is a complete R_k-lattice that is also a ring with unity, where R_k is the ring of integers in the number field k. Furthermore, an order $\mathcal{O}$ is *maximal* if it is maximal with respect to inclusion.

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

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

If ρ is the unique k-embedding of A into $M_2(\mathbb{R})$ and $\mathcal{O}$ is a maximal order in A, then the image under ρ of the group $\mathcal{O}^1$ of elements of norm 1 in $\mathcal{O}$ is contained in $\mathrm{SL}_2(\mathbb{R})$ and the group $P\rho(\mathcal{O}^1) \subset \mathrm{PSL}_2(\mathbb{R})$ forms a finite-coarea Fuchsian group. A subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$ is an *arithmetic Fuchsian group* if it is commensurable with some such $P\rho(\mathcal{O}^1)$. In addition, Γ is *derived from a quaternion algebra* or is a *derived arithmetic Fuchsian group* if $\Gamma \subset P\rho(\mathcal{O}^1)$. We will denote $P\rho(\mathcal{O}^1)$ by $\Gamma^1_{\mathcal{O}}$. The area of $\mathbb{H}^2/\Gamma^1_{\mathcal{O}}$ can be computed by the following formula [Borel 81]:

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

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

Notation. 2.1. Throughout the remainder of the article, we will use DAFG to denote a derived arithmetic Fuchsian group.

If Γ is an arithmetic Fuchsian group, then the corresponding quaternion algebra $A\Gamma$ is uniquely determined up to isomorphism and is called the *invariant quaternion algebra* of Γ. Moreover, two arithmetic Fuchsian groups are commensurable if and only if their invariant quaternion algebras are isomorphic [Takeuchi 77].

2.3 Number of Conjugacy Classes

The number of $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes of an arithmetic Fuchsian group depends on the infinite places of the number field k and the number of conjugacy classes of maximal orders of the quaternion algebra A. We will be concerned solely with $\mathrm{PGL}_2(\mathbb{R})$-conjugacy classes here, so throughout the text, conjugacy class should be interpreted as $\mathrm{PGL}_2(\mathbb{R})$-conjugacy class. Most of what follows can be found in [Vignéras 80].

For any maximal order $\mathcal{O}$ of A, $\Gamma_{\mathcal{O}}$ will denote the arithmetic Fuchsian group

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

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

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

A result in [Vignéras 80] states that two 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 class number $h = h(k)$ of k is the order of the class group I_k/P_k, where I_k is the group of fractional ideals of R_k, and P_k the group of nonzero principal ideals of R_k. Let

$$k^*_\infty = \{x \in k \mid \sigma(k) > 0 \text{ for all } \sigma \in \mathrm{Ram}_\infty(A)\}.$$

The restricted class group, whose order we will denote by h_∞, is the group

$$I_k/P_{k,\infty},$$

where $P_{k,\infty}$ is the group of principal ideals with generator in k^*_∞. We also have that

$$h_\infty = \frac{h2^{n-1}}{|R^*_k : R^*_k \cap k^*_\infty|}, \quad (2\text{–}4)$$

where R^*_k is the group of units of R_k. The number of conjugacy classes of maximal orders in a quaternion algebra A defined over k, denoted by $t = t(A)$, is finite and is called the *type number* of A. It is the order of the quotient of the restricted class group of k by the subgroup generated by the squares of the ideals of R_k and the prime ideals dividing the discriminant $\Delta(A)$; so we have

$$t = \left|\frac{I_k}{I_k^2 D P_{k,\infty}}\right|, \quad (2\text{–}5)$$

where D is the subgroup of prime ideals dividing the discriminant $\Delta(A)$. It follows that t divides h_∞. In many cases, $h_\infty = 1$, and we will use this to show that $t = 1$. Also, in the case that $\mathrm{Ram}_f(A) = \varnothing$ and $h = 1$, from the definitions above one can deduce that $t = h_\infty$.

2.4 Torsion in Arithmetic Fuchsian Groups

Throughout this section and the remainder of the text, ζ_{2m} will denote a primitive $2m$th root of unity. Also, k_m will denote the field $\mathbb{Q}(\cos(\frac{\pi}{m}))$, which is the unique totally real subfield of $\mathbb{Q}(\zeta_{2m})$ of index 2. Note that when m is odd, $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. The existence of torsion in an arithmetic Fuchsian group $\Gamma^1_{\mathcal{O}}$ defined over a number field k depends primarily on the subfields of k of the form k_m and the existence of embeddings of suitable quadratic extensions of k into the invariant quaternion algebra A. A more detailed treatment of this topic can be found in [Maclachlan and Reid 03, Chapter 12].

Let A^1 denote the elements of norm 1 in A, and $P(A^1)$ its projectivization. Let $\mathcal{O}$ be a maximal order in A and suppose the group $\Gamma^1_{\mathcal{O}}$ contains an element of order m. Then $P(A^1)$ contains an element of order m and A^1 contains an element u of order $2m$. This implies that $\mathrm{tr}\, u \in k$ and hence $k_m \subset k$. Furthermore, $k(\zeta_{2m})$ is a quadratic extension of k that embeds in A.

Conversely, using the following theorem, one can show that if $k(\zeta_{2m})/k$ is a quadratic extension that embeds in A, then $\Gamma^1_{\mathcal{O}}$ necessarily contains elements of order m.

Theorem 2.2. [Chinburg and Friedman 99] *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 both of the following conditions 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 are split in $\mathcal{L}/k$.*

The order $\Omega = R_k[\zeta_{2m}]$ is a commutative R_k-order whose field of quotients is $\mathcal{L} = k(\zeta_{2m})$. In the case of arithmetic Fuchsian groups, the field k is totally real and the field $k(\zeta_{2m})$ is a totally imaginary extension of $\mathbb{Q}$. Therefore, all real places of k are ramified in $k(\zeta_{2m})/k$; however, the algebra A is ramified at all real places but one. So condition (a) of Theorem 2.2 never holds. Thus, if $\mathcal{L} \subset A$, then every maximal order $\mathcal{O}$ of A will contain elements of order $2m$. Therefore, if $P(A^1)$ contains elements of order m, then so will $\Gamma^1_{\mathcal{O}}$ for any maximal order $\mathcal{O}$ of A. We have just proved the following result.

Theorem 2.3. *An arithmetic Fuchsian group $\Gamma^1_{\mathcal{O}}$ contains an element of order m if and only if the field $k(\zeta_{2m})$ embeds in A.*

The following theorem gives necessary and sufficient conditions for the embedding of the extension $k(\zeta_{2m})/k$ into the quaternion algebra A.

Theorem 2.4. [Maclachlan and Reid 03] *Let A be a quaternion algebra over a number field k and let ℓ/k be a quadratic extension. Then ℓ embeds in A if and only if $\ell \otimes_k k_v$ is a field for each $v \in \mathrm{Ram}(A)$.*

We can use this theorem along with Theorem 2.2 to give a characterization of the existence of torsion in the groups $\Gamma^1_{\mathcal{O}}$. This result will be used frequently in the proof of Theorem 4.10:

Lemma 2.5. *Let k be a totally real number field such that $k_m \subset k$, A is a quaternion algebra ramified at all but one real place over k, and $\mathcal{O}$ is a maximal order in A. The group $\Gamma^1_{\mathcal{O}}$ will contain an element of order m if and only if $\mathcal{P}$ does not split in $k(\zeta_{2m})/k$ for all $\mathcal{P} \in \mathrm{Ram}_f(A)$.*

Proof: Let ζ_{2m} be a primitive $2m$th root of unity. By Theorem 2.4, the quadratic extension $k(\zeta_{2m})$ of k embeds in A if and only if $k(\zeta_{2m}) \otimes_k k_v$ is a field for each $v \in \mathrm{Ram}(A)$. Since $k(\zeta_{2m})$ is totally imaginary, $k(\zeta_{2m}) \otimes_k k_v$ is always a field for all $v \in \mathrm{Ram}_\infty(A)$. Moreover, for $\mathcal{P} \in \mathrm{Ram}_f(A), k(\zeta_{2m}) \otimes_k k_{\mathcal{P}}$ is a field if and only if $\mathcal{P}$ does not split in $k(\zeta_{2m})/k$. Theorem 2.3 now gives the desired conclusion. □

If k is a totally real field, the relative class number h^- for the extension $k(\zeta_{2m})/k$ is defined as

$$h^- = \frac{h(k(\zeta_{2m}))}{h(k)} \in \mathbb{Z},$$

where $h(k(\zeta_{2m}))$ is the class number of $k(\zeta_{2m})/\mathbb{Q}$ and $h(k)$ is the class number of k (see [Washington 97, p. 38]).

If a maximal order $\mathcal{O}$ in A contains elements of finite order, then we can calculate the number a_m of conjugacy classes of maximal cyclic subgroups of order m in $\Gamma^1_{\mathcal{O}}$, provided that $\{1, \zeta_{2m}\}$ is a relative integral basis for the quadratic extension $k(\zeta_{2m})/k$ [Schneider 75]. If this assumption holds, then

$$a_m = \frac{h^-}{|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}|} \Pi_{\mathcal{P}|\Delta(A)} \left(1 - \left(\frac{k(\zeta_{2m})}{\mathcal{P}}\right)\right), \tag{2–6}$$

where $\left(\frac{k(\zeta_{2m})}{\mathcal{P}}\right)$ is the Artin symbol (which is equal to 1, 0, or -1, according to whether $\mathcal{P}$ splits, ramifies, or is inert in the extension $k(\zeta_{2m})/k$) and

$$R^{*(2)}_{k(\zeta_{2m})} = \left\{x \in R^*_{k(\zeta_{2m})} | N_{k(\zeta_{2m})|k}(x) \in R^{*(2)}_k\right\}.$$

In some cases, we can use the following lemma to simplify formula (2–6).

Lemma 2.6. *Let k be a totally real number field of odd degree and suppose $\{1, \zeta_{2m}\}$ is a relative integral basis for $k(\zeta_{2m})/k$. If h^- is odd, then $|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}| = 1$.*

Proof: Both quantities $h(k(\zeta_{2m}))/h$ and $|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}|$ depend only on the number field k and hence are independent of the quaternion algebra A. Since $\left|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}\right|$ is a finite 2-group, its order is 2^n, for some nonnegative integer n. If $|k : \mathbb{Q}|$ is odd, then let A be a quaternion algebra unramified at all finite places. Since

$$a_m = \frac{h(k(\zeta_{2m}))}{h|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}|} \in \mathbb{Z}$$

and $h^- = h(k(\zeta_{2m}))/h$ is odd, we must have

$$\left|R^*_{k(\zeta_{2m})} : R^{*(2)}_{k(\zeta_{2m})}\right| = 1,$$

completing the proof of the lemma. □

Since ζ_3 will arise frequently in our calculations, we will fix the notation $\omega = \zeta_3$. Furthermore, the following lemma can often be used to simplify formula (2–6).

Lemma 2.7. *Suppose that k is a totally real number field and that 2 is unramified in $k/\mathbb{Q}$. Then*

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

Likewise, if 3 is unramified in $k/\mathbb{Q}$, then

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

The proof of Lemma 2.7 requires the following two general facts (see respectively [Ribenboim 72, Chapter 10] and [Parry 75]).

Fact 2.8. *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 $k(\omega)/k$.*

Fact 2.9. *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 Proof of Lemma 2.7.: 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

$$\cos\left(\frac{\pi}{m}\right) + i \sin\left(\frac{\pi}{m}\right)$$

is a root of unity in $k(i)$. 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

$$\cos\left(\frac{\pi}{m}\right) + i \sin\left(\frac{\pi}{m}\right) = a + bi$$

correspond to the units ± 1 and $\pm i$. By Fact 2.9, 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 $a, b \in R_k$. Any unit $\epsilon \in k(i)$ must satisfy the equation

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

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, we must have $a = \pm b$ 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. Therefore, the units in $k(i)$ are of the form $\epsilon = \pm a$ or $\epsilon = \pm bi$. Since ϵ is a unit, this implies $a \in R^*_k$ or $b \in R^*_k$ and hence $\eta^2 \in R^{*2}_k$. In either case, we have

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

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

$$\left|R^*_{k(i)} : R^{*(2)}_{k(i)}\right| = 1.$$

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

It will be necessary for us to determine which periods can arise in the various number fields k. First, If $k_m \subset k$, then $|k_m : \mathbb{Q}|$ divides $|k : \mathbb{Q}|$ and d_{k_m} divides d_k. With this in mind, we will require the following properties of the cyclotomic field $\mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p)$ and its proper subfield $k_p = \mathbb{Q}(\cos(\pi/p))$ when $p > 3$ is a prime.

Proposition 2.10. *Let $p > 3$ be a prime. Then:*

(i) $|k_p : \mathbb{Q}| = \frac{p-1}{2}$;

(ii) $d_{\mathbb{Q}(\zeta_p)} = p^{p-2}$;

(iii) $d_{k_p} = p^{\frac{p-3}{2}}$.

Proof: This first part follows from the fact that $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$ and that k_p is a proper subfield of index two. The second and third parts can be found in [Washington 97, pp. 9, 28]. □

3. BOUNDS ON THE DEGREE OF THE NUMBER FIELD K

In this section, we classify commensurability classes of DAFGs of signature $(2; -)$ by invariant quaternion algebra. First, we determine all possible signatures of Fuchsian groups that can contain a subgroup of signature $(2; -)$. Then, using arithmetic data, we show that all arithmetic Fuchsian groups $\Gamma^1_{\mathcal{O}}$ with one of these signatures are defined over number fields of degree less than or equal to 5.

The following theorem gives necessary and sufficient conditions for the existence of torsion-free subgroups of a given index in a Fuchsian group:

Theorem 3.1. [Edmonds et al. 82] *Let Γ be a finitely generated Fuchsian group with the standard presentation*

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

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 $\lambda = \mathrm{lcm}(m_1, \ldots, m_r)$, 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.)

We will use this result to prove the following lemma:

Lemma 3.2. *Let Γ be a cocompact Fuchsian group containing a genus-two surface group. Then Γ has one of the following signatures:*

$(0; 2, 3, 7)$, $(0; 2, 3, 8)$, $(0; 2, 3, 9)$, $(0; 2, 3, 10)$,
$(0; 2, 3, 12)$, $(0; 2, 4, 5)$, $(0; 2, 4, 6)$, $(0; 2, 4, 8)$,
$(0; 2, 4, 12)$, $(0; 2, 5, 5)$, $(0; 2, 5, 6)$, $(0; 2, 5, 10)$,
$(0; 2, 6, 6)$, $(0; 2, 8, 8)$, $(0; 3, 3, 4)$, $(0; 3, 3, 5)$,
$(0; 3, 3, 6)$, $(0; 3, 3, 9)$, $(0; 3, 4, 4)$, $(0; 3, 6, 6)$,
$(0; 4, 4, 4)$, $(0; 5, 5, 5)$, $(0; 2, 2, 2, 3)$, $(0; 2, 2, 2, 4)$,
$(0; 2, 2, 2, 6)$, $(0; 2, 2, 3, 3)$, $(0; 2, 2, 4, 4)$, $(0; 3, 3, 3, 3)$,
$(0; 2, 2, 2, 2, 2)$, $(0; 2, 2, 2, 2, 2, 2)$, $(1; 2)$, $(1; 3)$, $(1; 2, 2)$.

Proof: If Γ_1 is a genus-two surface subgroup of Γ, then $M\mu(\Gamma) = \mu(\Gamma_1) = 4\pi$, where $M = |\Gamma : \Gamma_1|$. 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 3.1, depending on the signature of the group Γ, either λ or 2λ divides the index M, where $\lambda = \mathrm{lcm}(m_1, \ldots, m_r)$. 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 (2–2),

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

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

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

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

$$\sum_{i=1}^{4} \frac{m_i - 1}{m_i} = \frac{2}{M} + 2. \tag{3–1}$$

In addition, $\lambda = \mathrm{lcm}(m_1, \ldots, m_4)$ divides M. Since $\mu(\Gamma) > 0$, there exists at least one x_i with order $m_i > 2$. Also, we can deduce the following two facts:

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

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

If (i) does not hold, then $m_1 \ge 2$, $m_2 \ge 3$, $m_3 \ge 4$, and $M \ge \lambda \ge 6$, and this gives the following contradiction:

$$\frac{29}{12} \le \sum_{i=1}^{4} \frac{m_i - 1}{m_i} = \frac{2}{M} + 2 \le \frac{28}{12}.$$

Similarly, if (ii) does not hold, then $M \ge \lambda \ge 4$, and we arrive at the contradiction

$$\frac{10}{4} \le \sum_{i=1}^{4} \frac{m_i - 1}{m_i} = \frac{2}{M} + 2 \le \frac{9}{4}.$$

Without loss of generality, suppose $x_1 \le x_2 \le \cdots \le x_4$. We then have the following four cases:

Case 1: $m_1 = m_2 = m_3 = 2$ and $m_4 = m > 2$. In this case, equation (3–1) becomes

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

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

Case 2: $m_1 = m_2 = 2$ and $m = m_3 = m_4 > 2$. Again, equation (3–1) becomes

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

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

Case 3: $m_1 = 2$ and $m = m_2 = m_3 = m_4 > 2$. Equation (3–1) translates to

$$\frac{1}{2} + \frac{3(m-1)}{m} = \frac{2}{M} + 2,$$

and one can easily verify that there exist no integer solutions to this equation.

Case 4: $m = m_1 = m_2 = m_3 = m_4 > 2$. In this situation,

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

and $m = M = 3$ is the only solution.

The existence of a torsion-free subgroup of index M for a group of fixed signature is guaranteed by Theorem 3.1. Therefore, the only Fuchsian groups with signature $(0; x_1, x_2, x_3, x_4)$ containing a torsion-free subgroup of genus 2 are those with signatures $(0; 2, 2, 2, 3)$, $(0; 2, 2, 2, 4)$, $(0; 2, 2, 2, 6)$, $(0; 2, 2, 3, 3)$, $(0; 2, 2, 4, 4)$, 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 3.3. *There exist no* DAFGs *of signature* $(2; -)$ *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

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

In particular, this implies

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

Note that

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

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

$$4\pi \ge \frac{8\pi d_k^{3/2}}{(4\pi^2)^{|k:\mathbb{Q}|}}. \tag{3–5}$$

We now use Odlyzko's lower bounds [Odlyzko 75] on the discriminant of a totally real number field to get an upper bound on the degree of k:

$$|d_k| \ge (2.439 \times 10^{-4})(29.099)^n,$$

where $n = |k : \mathbb{Q}|$. Using these estimates in inequality (3–5) gives $n \le 8$.

However, the smallest discriminant of a totally real field of degree 7 or 8 is 20,134,393 or 282,300,416, respectively [Cohen et al. 95, Pohst et al. 90]. In each case, inequality (3–3) is violated:

$$4\pi \ge \frac{8\pi d_k^{3/2}}{(4\pi^2)^{|k:\mathbb{Q}|}} \ge \begin{cases} \frac{8\pi(20{,}134{,}393)^{3/2}}{(4\pi^2)^7} \approx 15.1925 > 4\pi, \\ \frac{8\pi(282{,}300{,}416)^{3/2}}{(4\pi^2)^8} \approx 20.2036 > 4\pi. \end{cases}$$

Hence, there cannot exist a DAFG of signature $(2;-)$ if $|k:\mathbb{Q}| \geq 7$.

To eliminate the case $|k:\mathbb{Q}| = 6$, we again exploit the area formula (2–3) and inequality (3–4) to get the following inequality:

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

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

$$d_k \leq \left(\frac{3(4\pi^2)^6}{8}\right)^{2/3} < 1{,}263{,}165. \qquad (3\text{–}6)$$

According to the lists from [Cohen et al. 95], there are 20 number fields k of degree 6 satisfying the above inequality. For each field k, we investigate the behavior of small primes and, if necessary, estimate $\zeta_k(2)$ using PARI. Since $n = 6$, $|\operatorname{Ram}_f(A)| \neq \varnothing$. 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 norm in k.

For example, consider the totally real field k of degree 6 and discriminant $d_k = 722{,}000$. A minimal polynomial for k is $f(x) = x^6 - x^5 - 6x^4 + 7x^3 + 4x^2 - 5x + 1$. By PARI, 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 area 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 DAFGs of signature $(2;-)$ defined over k. In this fashion, we obtain a contradiction to the inequality $\mu(\Gamma) \leq 4\pi$ for each totally real field k of degree 6 with discriminant d_k satisfying (3–6). □

4. CLASSIFICATION BY COMMENSURABILITY CLASS

In this section, we classify DAFGs of signature $(2;-)$ by invariant quaternion algebra. All the groups in Lemma 3.2 except those with one of the three signatures $(1;2,2)$, $(0;2,2,2,2,2,2)$, and $(2;-)$ have commensurability classes that have already been classified; i.e., they are all commensurable with an arithmetic Fuchsian triangle group or one having signature $(1;e)$ or $(0;2,2,2,e)$. So it suffices to classify the commensurability classes of the groups $\Gamma^1_{\mathcal{O}}$ of these remaining three types and to extract the relevant results from [Ackermann et al. 03, Maclachlan and Rosenberger 92, Takeuchi 77, Takeuchi 83].

The proof classification is exhaustive. For each fixed degree $|k:\mathbb{Q}|$, we use equation (2–3) to get upper bounds on the discriminant of the number field k. Then we determine the existence of all quaternion algebras whose unit groups have one of the above three signatures. Rather than go through an analysis of each number field that can correspond to such an arithmetic Fuchsian group, we give an idea of the overall approach by a few illustrative examples. Our argument will be organized by the degree of the number field.

We will make extensive use of the following lemma, which is particularly useful in the case $|k:\mathbb{Q}|$ odd (since we can have $\operatorname{Ram}_f(A) = \varnothing$ in this case):

Lemma 4.1. *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 Γ is a genus-two surface group contained in $\Gamma^1_{\mathcal{O}}$ for $\mathcal{O}$ a maximal order in A, then 6 divides $|\Gamma^1_{\mathcal{O}}:\Gamma|$.*

Proof: Since $\operatorname{Ram}_f(A)$ is empty, by Lemma 2.5, there is no obstruction to embedding $\mathcal{L}$ in $\mathcal{O}$, where $\mathcal{L} \cong \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$. Therefore, any order $\mathcal{O}$ in A will contain elements of orders 2 and 3. By Theorem 3.1, 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 in turn divides $|\Gamma^1_{\mathcal{O}}:\Gamma|$. □

4.1 Quintic Number Fields

Lemma 4.2. *For $|k:\mathbb{Q}| = 5$, the only DAFGs of signature $(2;-)$ arise from quaternion algebras over the totally real fields of discriminants $d_k = 38{,}569$, $36{,}497$, and $24{,}217$.*

Proof: Suppose there exists a DAFG $\Gamma < \Gamma^1_{\mathcal{O}}$ of genus two that is torsion-free and defined over a totally real quintic number field k. Using the inequalities $\zeta_k(2) \geq 1$, $\prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1) \geq 1$ in conjunction with (2–3), we get that

$$d_k \leq 131{,}981.$$

However, if $\operatorname{Ram}_f(A) = \varnothing$, the index $M = [\Gamma^1_{\mathcal{O}}:\Gamma]$ is greater than or equal to 6 by Lemma 4.1. Substituting back into the area formula (2–3) gives $d_k \leq 39{,}970$. For those fields with $39{,}970 \leq d_k \leq 131{,}981$, we analyze the behavior of small primes in k to determine the possible ramification sets for each field k. According to [Cohen et al. 95], there are 15 number fields with $d_k < 131{,}981$. In a few cases, small primes do exist, but we can eliminate these cases using torsion.

For example, let k be the number field with discriminant $d_k = 106{,}069$. Using the minimal polynomial $f(x) = x^5 - 2x^4 - 4x^3 + 7x^2 + 3x - 4$ to generate the k in PARI, we compute that

$$\frac{8\pi \cdot 106{,}069^{3/2}\zeta_k(2)}{(4\pi^2)^5} = 4\pi.$$

Furthermore, there exists a unique prime $\mathcal{P}_2$ of norm 2 in R_k. Together with the fact that $|\operatorname{Ram}_f(A)|$ is even, this implies that $\operatorname{Ram}_f(A) = \varnothing$. So, by (2–3), $\mu(\Gamma^1_{\mathcal{O}}) = 4\pi$ for any maximal order $\mathcal{O}$ in A. However, by Lemma 4.1, $\Gamma^1_{\mathcal{O}}$ contains elements of orders 2 and 3. Hence, $\Gamma^1_{\mathcal{O}}$ is not torsion-free, and since $\mu(\Gamma^1_{\mathcal{O}}) = 4\pi$, it is not a genus-two surface group, nor does it contain a genus-two subgroup.

The case $d_k = 38{,}569$ yields a positive result. By PARI, using the minimal polynomial $f(x) = x^5 - 5x^3 + 4x - 1$, we compute that

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{8\pi \cdot 38{,}569^{3/2}\zeta_k(2)}{(4\pi^2)^5} = \frac{2\pi}{3}.$$

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

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

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

Again the only solution to the above equation occurs when $M = 6$ and $\operatorname{Ram}_f(A) = \varnothing$. Since $d_k = 38{,}569$ is prime, 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 4.1, 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, and Theorem 3.1 guarantees the existence of a torsion-free subgroup of index 6.

The totally real number fields of degree 5 with discriminants 36,497 and 24,217 are the only other fields that yield positive existence results. □

4.2 Quartic Number Fields

For $|k:\mathbb{Q}| = 4$, $\operatorname{Ram}_f(A) \neq \varnothing$. Using Proposition 2.10 to analyze the cyclotomic extensions with degree dividing 8, one can easily show that 2, 3, 4, 5, 6, 8, 10, 12, 15 are the only possible cycles for elliptic elements in this case.

Using equation (3–2) in conjunction with inequality (3–4), 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 given in [Cohen et al. 95]. Again, we eliminate all fields except those listed in Theorem 4.10 by estimating $\zeta_k(2)$ and examining the factorization of small primes using PARI.

Lemma 4.3. *There exist no DAFGs of signature $(2;-)$ 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

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{8\pi \cdot 5744^{3/2}\zeta_k(2)}{(4\pi^2)^4} = \frac{5\pi}{3}.$$

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

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

Lemma 4.4. *Let k be the totally real number field with $d_k = 3981$. Then the only DAFG of signature $(2;-)$ defined over k has invariant quaternion algebra A with $\operatorname{Ram}_f(A) = \mathcal{P}_3$, where $\mathcal{P}_3$ is the unique prime in R_k lying over 3. Furthermore, there is only one conjugacy class of DAFGs of this signature defined 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 nontrivial elements of finite order of $\Gamma^1_{\mathcal{O}}$ are those of order 2 or 3. By PARI, we compute

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{8\pi \cdot 3981^{3/2}\zeta_k(2)}{(4\pi^2)^4} = \pi.$$

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

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 4. \tag{4–2}$$

This implies that $N(\mathcal{P}) \leq 5$ for any prime $\mathcal{P} \in \mathrm{Ram}_f(A)$. 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 $N(\mathcal{P}_5) = 5$.

Therefore $M = 1$, $\mathrm{Ram}_f(A) = \{\mathcal{P}_5\}$ is a possible solution to (4–2). However, $\mathcal{P}_5$ is inert in $k(\omega)/k$, which, by Lemma 2.5, implies that $a_3 \neq 0$. However, by Theorem 3.1, $3 \mid M = 1$, which is a contradiction.

We also have $M = 2$ and $\mathrm{Ram}_f(A) = \{\mathcal{P}_3\}$ as a possible solution to (4–2). Furthermore, 6 does not divide d_k, so by Lemma 2.8 we can calculate a_2 and a_3 using (2–6). Using PARI, we compute that $\mathcal{P}_3$ is inert in the extension $k(i)/k$, that $h(k(i)) = 3$, and that $h(k) = 1$. Also, since 2 does not divide d_k, by Lemma 2.7 we have that $|R^*_{k(i)} : R^{*(2)}_{k(i)}| = 1$. Therefore

$$a_2 = \frac{h^-}{|R^*_{k(i)} : R^{*(2)}_{k(i)}|} \Pi_{\mathcal{P}|\Delta(A)} \left(1 - \left(\frac{k(\zeta_i)}{\mathcal{P}}\right)\right) = 3 \cdot 2 = 6.$$

The prime $\mathcal{P}_3$ splits in $k(i)$, so by either Lemma 2.5 or equation (2–6), $a_3 = 0$.

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 3.1; since $\mu(\Gamma) = 4\pi$, Γ must have signature $(2;-)$.

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 infinite places of k will 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	$\alpha - 1$	$\alpha^2 + \alpha - 1$
$\alpha_1 \approx -1.7508$	$-$	$-$	$+$
$\alpha_2 \approx -0.3184$	$-$	$-$	$-$
$\alpha_3 \approx 0.7853$	$+$	$-$	$+$
$\alpha_4 \approx 2.2840$	$+$	$+$	$+$

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 k. □

Lemma 4.5. *Let $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be the number field with $d_k = 2304$. The only* DAFG *of signature $(2;-)$ arising from a quaternion algebra A over k has $\mathrm{Ram}_f(A) = \mathcal{P}_3$, where $\mathcal{P}_3$ is the unique prime of norm 9 in k.*

Proof: The periods 2, 3, 4, and 6 are all obvious possibilities for torsion, since $\mathbb{Q}$, k_2, k_3 are proper subfields of k. The fact that $5 \nmid 2304 = 2^8 \cdot 3^2$ implies that these are the only possibilities. In this case, $k = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $f(x) = x^4 - 4x^2 + 1$. Using PARI, we compute that

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

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

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 8. \tag{4–3}$$

The only primes $\mathcal{P}$ in R_k 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 $|\mathrm{Ram}_f(A)|$ is odd, the only solution to (4–3) is $M = 1$ and $\mathrm{Ram}_f(A) = \{\mathcal{P}_3\}$. The prime $\mathcal{P}_3$ splits in both $k(i)/k$ and $k(\omega)/k$. So, by Lemma 2.5, for any maximal order $\mathcal{O}$, the group $\Gamma^1_{\mathcal{O}}$ contains no elements of order 2 or 3. This also implies that $\Gamma^1_{\mathcal{O}}$ contains no elements of order 4 or 6; therefore, $\Gamma^1_{\mathcal{O}}$ is torsion-free and has genus 2. Since $k/\mathbb{Q}$ is Galois, there is only one conjugacy class of arithmetic Fuchsian groups $\Gamma^1_{\mathcal{O}}$ defined over k. □

Lemma 4.6. *Let k be the number field with $d_k = 1957$. Then the only* DAFG*s of signature $(2;-)$ arising from a quaternion algebra A over k containing genus-two subgroups are those listed in Theorem 4.10.*

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

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

Again, we consider solutions to the equation

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

or equivalently,

$$M \prod_{\mathcal{P}|\Delta(A)} (N(\mathcal{P}) - 1) = 12, \tag{4–4}$$

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 $\mathrm{Ram}_f(A)$. By PARI, there are two primes $\mathcal{P}_3 = (\alpha - 2)R_k$ and $\mathcal{P}'_3$ lying over 3, with norms $N(\mathcal{P}_3) = 3$ and $N(\mathcal{P}'_3) = 9$, respectively. There also exists a prime $\mathcal{P}_7 = (2\alpha + 1)R_k$ of norm 7. Combining this with the fact that $|\mathrm{Ram}_f(A)|$ is odd, we get that the only possible solutions $(M, \mathrm{Ram}_f(A))$ to the above equation are $(6, \mathcal{P}_3)$ and $(2, \mathcal{P}_7)$. The quaternion algebras with $\mathrm{Ram}_f(A) = \{\mathcal{P}_3\}$ appear in the lists of [Maclachlan and Rosenberger 92], and the unit groups $\Gamma^1_{\mathcal{O}}$ have signature $(0; 2, 2, 2, 3)$ in this case.

Let us consider the algebra with $\mathrm{Ram}_f(A) = \{\mathcal{P}_7\}$. Since $6 \nmid 1957$ and k contains no proper subfields other than $\mathbb{Q}$, $\Gamma^1_{\mathcal{O}}$ can have elements only of orders 2 and 3. Moreover, we can compute the number of elements of orders 2 and 3 using formula (2–6). 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 number of 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 lists the signs of the generators:

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

Since the extension $k/\mathbb{Q}$ is not Galois and k contains no proper subfields, we again get at least one conjugacy class corresponding to the algebra unramified at the place $\alpha_i, 1 \le i \le 4$. The class number of k is 1, so $h_\infty = 2^3/|R^*_k/R^*_k \cap k^*_\infty|$. 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.

4.3 Cubic Number Fields

Lemma 4.7. *The only possible 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 contains no proper subfields other than $\mathbb{Q}$, 2 and 3 are the only possible periods than can arise from proper subfields of k. By Proposition 2.10, 7 is the only prime for which $|k_p : \mathbb{Q}| = 3$. In fact, $k_7 = \mathbb{Q}(\cos(\frac{\pi}{7}))$ is the totally real cubic field with discriminant 49. For prime powers $m = p^k$, the only field $\mathbb{Q}(\zeta_{2m})$ with $|\mathbb{Q}(\zeta_{2m}) : \mathbb{Q}| = 6$ is $m = 9$. This corresponds to the totally real field of discriminant 81. There are no composite m for which $|\mathbb{Q}(\zeta_{2m}) : \mathbb{Q}| = 6$; this finishes the proof. □

If $[k : \mathbb{Q}] = 3$, it is possible that $\mathrm{Ram}_f(A) = \varnothing$. As in the case $[k : \mathbb{Q}] = 5$, this helps to simplify the process immensely, since this implies $d_k \le 297$. If $\mathrm{Ram}_f(A) \ne \varnothing$, then $d_k \le 981$. In the lists [Cohen et al. 95], there are 25 number fields k with discriminants satisfying the latter inequality (see [Macasieb 05, Appendix A]). The cases $k = \mathbb{Q}(\cos(\frac{\pi}{9}))$ and $k = \mathbb{Q}(\cos(\frac{\pi}{7}))$, in which 9 and 7, respectively, are possible periods, require special examination. We analyze the latter case in detail below.

Lemma 4.8. *There exist no DAFGs of signature $(2; -)$ arising from a quaternion algebra defined over the totally real cubic number field of discriminant 361.*

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

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{8\pi \cdot 361^{3/2}\zeta_k(2)}{(4\pi^2)^3} = \pi.$$

By the preceding comments, $\mathrm{Ram}_f(A) \ne \varnothing$. The equation

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

has no solutions, since 2, 3, and 5 are inert in $k/\mathbb{Q}$. Therefore, there are no DAFGs of signature $(2; -)$ defined over k. □

Lemma 4.9. *For $k = \mathbb{Q}(\cos(\frac{\pi}{7}))$, the only possible $\Gamma^1_{\mathcal{O}}$ containing a subgroup Γ of signature $(2; -)$ are those listed in Theorem 4.10.*

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

$$\mu(\Gamma^1_{\mathcal{O}}) = \frac{8\pi \cdot 49^{3/2}\zeta_k(2)}{(4\pi^2)^3} = \frac{\pi}{21}.$$

$[k:\mathbb{Q}]$	d_k	$\Delta(A)$	$\lvert\Gamma^1_{\mathcal{O}}:\Gamma\rvert$	$\Gamma^1_{\mathcal{O}}$	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	$(2;-)$	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	$(2;-)$	1
2	5	$\mathcal{P}'_{61}$	1	$(2;-)$	1
2	8	$\mathcal{P}_2$	24	$(0;3,3,4)$	1
2	8	$\mathcal{P}_7$	4	$(0;2,2,4,4)$	1
2	8	$\mathcal{P}_3$	3	$(1;3)$	1
2	8	$\mathcal{P}_5$	1	$(2;-)$	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	$(2;-)$	1
2	12	$\mathcal{P}'_{13}$	1	$(2;-)$	1
2	13	$\mathcal{P}_3$	6	$(0;2,2,3,3)$	1
2	13	$\mathcal{P}'_3$	6	$(0;2,2,3,3)$	1
2	13	$\mathcal{P}_2$	4	$(1;2)$	1
2	13	$\mathcal{P}_{13}$	1	$(2;-)$	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	21	$\mathcal{P}_2$	1	$(1;2,2)$	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

TABLE 1. DAFG of signature $(2;-)$.

$[k:\mathbb{Q}]$	d_k	$\Delta(A)$	$\lvert\Gamma^1_{\mathcal{O}}:\Gamma\rvert$	$\Gamma^1_{\mathcal{O}}$	c
3	49	$\varnothing$	84	$(0;2,3,7)$	1
3	49	$\mathcal{P}_2\mathcal{P}_7$	2	$(1;2,2)$	1
3	49	$\mathcal{P}_2\mathcal{P}_{13}$	1	$(2;-)$	1
3	49	$\mathcal{P}_2\mathcal{P}'_{13}$	1	$(2;-)$	1
3	49	$\mathcal{P}_2\mathcal{P}''_{13}$	1	$(2;-)$	1
3	81	$\varnothing$	36	$(0;2,3,9)$	1
3	148	$\varnothing$	12	$(0;2,2,2,3)$	3
3	148	$\mathcal{P}_2\mathcal{P}_5$	3	$(0;3,3,3,3)$	3
3	148	$\mathcal{P}_2\mathcal{P}_{13}$	1	$(2;-)$	3
3	169	$\varnothing$	12	$(0;2,2,2,3)$	1
3	229	$\varnothing$	6	$(0;2,2,3,3)$	4
3	229	$\mathcal{P}_2,\mathcal{P}'_2$	2	$(1;2,2)$	3
3	257	$\varnothing$	6	$(0;2,2,3,3)$	4
3	316	$\mathcal{P}_2,\mathcal{P}'_2$	3	$(0;3,3,3,3)$	3
4	725	$\mathcal{P}_{11}$	6	$(0;2,2,3,3)$	2
4	725	$\mathcal{P}'_{11}$	6	$(0;2,2,3,3)$	2
4	725	$\mathcal{P}_2$	4	$(1;2)$	2
4	725	$\mathcal{P}_{31}$	2	$(1;2,2)$	2
4	725	$\mathcal{P}'_{31}$	2	$(1;2,2)$	2
4	725	$\mathcal{P}_{61}$	1	$(2;-)$	2
4	725	$\mathcal{P}'_{61}$	1	$(2;-)$	2
4	1125	$\mathcal{P}_2$	2	$(1;2,2)$	1
4	1957	$\mathcal{P}_3$	6	$(0;2,2,3,3)$	4
4	1957	$\mathcal{P}_7$	2	$(1;2,2)$	4
4	2000	$\mathcal{P}_2$	10	$(0;5,5,10)$	1
4	2000	$\mathcal{P}_5$	2	$(0;3,3,3,3)$	2
4	2304	$\mathcal{P}_3$	1	$(2;-)$	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	$(2;-)$	2
5	24217	$\varnothing$	12	$(0;2,2,2,3)$	5
5	36497	$\varnothing$	6	$(0;2,2,3,3)$	6
5	38569	$\varnothing$	6	$(0;2,2,3,3)$	6

TABLE 2. DAFG of signature $(2;-)$ (cont.).

Thus,

$$4\pi = \mu(\Gamma) = M\mu(\Gamma^1_{\mathcal{O}}) = M\frac{\pi\prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{21}. \tag{4–5}$$

If we take $\mathrm{Ram}_f(A)=\varnothing$, then $M=84$. So $\mu(\Gamma^1_{\mathcal{O}})=\frac{\pi}{21}$. Since $\mathrm{Ram}_f(A)=\varnothing$, and $k=k_7$, we have $a_2,a_3,a_7\neq 0$ by Lemma 2.5. Therefore,

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

The only solution to this equation is $a_2=a_3=a_7=1$, and in this case $\Gamma^1_{\mathcal{O}}$ is a triangle group of signature $(0;2,3,7)$ (see [Takeuchi 77]). Again the existence of a torsion-free subgroup of $\Gamma^1_{\mathcal{O}}$ of index 84 is guaranteed by Theorem 3.1.

If $\mathrm{Ram}_f(A)\neq\varnothing$, then $\prod_{\mathcal{P}|D(A)}(N(\mathcal{P})-1)\geq 42$. This is because the primes of smallest norm in R_k, $\mathcal{P}_2$ and $\mathcal{P}_7$, have norms 8 and 7, respectively, in k, and $|\mathrm{Ram}_f(A)|\geq 2$. This implies $M\leq 2$. However, since $\Gamma^1_{\mathcal{O}}$ will not be torsion-free, Theorem 3.1 implies that $M\geq 2$. Thus, the only other possible solution to (4–5) occurs when $M=2$.

In this case, $\mathrm{Ram}_f(A)=\{\mathcal{P}_2,\mathcal{P}_7\}$ is a solution to (4–5) when $M=2$. Since $6\nmid d_k$, we can apply Lemma 4.1. By PARI, we find that $h=h(k(i))=h(k(\omega))=1$ and that $\mathcal{P}_2$ ramifies and $\mathcal{P}_7$ is inert in $k(i)/k$; therefore $a_2=2$. Since the ideal $\mathcal{P}_7$ splits in $k(\omega)/k$, we have $a_3=0$. But

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

and $g=1$, $e_7=0$ is the only solution. Thus, $\Gamma^1_{\mathcal{O}}$ has signature $(1;2,2)$, and again by Theorem 3.1, it has a torsion-free subgroup of genus two and of index two. Since $k/\mathbb{Q}$ is Galois, there is only one conjugacy class of groups $\Gamma^1_{\mathcal{O}}$ of this signature.

Similarly, $\mathrm{Ram}_f(A)=\{\mathcal{P}_2,\mathcal{P}_{13}\}$ and $M=1$ is a solution to (4–5), where $\mathcal{P}_{13}$ is any of the three prime ideals of norm 13 in R_k. Since each prime $\mathcal{P}_{13}$ splits in each of the extensions $k(i)/k$ and $k(\omega)/k$, the group $\Gamma^1_{\mathcal{O}}$ is torsion-free and therefore has signature $(2;-)$. Lastly, note that each of the three distinct primes of norm 13 in R_k corresponds to a distinct commensurability class of DAFG of signature $(2;-)$ and each contributes exactly one conjugacy class, since $k/\mathbb{Q}$ is Galois. □

Johansson [Johansson 98] has determined the signatures of all DAFGs of genus less than 3 arising from quaternion algebras over the rationals and quadratic number fields, so it suffices to consider those number fields of degree $|k:\mathbb{Q}|>2$. Combining Lemma 3.2 and our results with the relevant results in [Johansson 98, Maclachlan and Rosenberger 92, Takeuchi 77, Takeuchi 83] we obtain the following theorem.

Theorem 4.10. *Table 1 and its continuation Table 2 give a complete list of all groups $\Gamma^1_{\mathcal{O}}$ containing a derived arithmetic Fuchsian group Γ of signature $(2;-)$ arising from quaternion algebras over totally real number fields. The number c denotes the number of conjugacy classes of the group $\Gamma^1_{\mathcal{O}}$ in each case.*

Remark 4.11. Using a theorem from [Greenberg 63] on maximal Fuchsian groups in conjunction with the results in [Ackermann et al. 03, Maclachlan and Rosenberger 92, Takeuchi 77, Takeuchi 83] gives all the conjugacy classes of the groups $\Gamma^1_{\mathcal{O}}$ listed in Tables 1 and 2 except for those with signatures $(1;2,2)$, $(0;2,2,2,2,2,2)$, and $(2;-)$.

5. MAXIMAL ORDERS AND FUNDAMENTAL DOMAINS

The group $\mathrm{SU}(1,1)$ is the group of orientation-preserving isometries of the unit disk $\mathcal{U}=\{z\in\mathbb{C}\mid |z|\le 1\}$. By embedding a cocompact arithmetic Fuchsian group Γ into $\mathrm{SU}(1,1)$, one can determine a fundamental domain for its image Γ' using a theorem of Ford. The elements of Γ' that give the side pairings of the fundamental domain are generators for Γ'. This technique is described for the rational numbers and quadratic number fields in [Vignéras 80] and [Katok 92] and more generally in [Johansson 00]. In order to find a fundamental domain for Γ using this technique, the maximal order must be written explicitly as an R-module, where $R=R_k$ is the ring of integers of the number field k. We first state and prove some results on the existence and form of maximal orders in certain cases in which the Hilbert symbol for a quaternion algebra A is "nice." The invariant quaternion algebras of arithmetic Fuchsian groups with small genus will often fall into this class.

5.1 Maximal Orders

Recall that any quaternion algebra A has an 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. 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 any R-order $\mathcal{O}$ in A, the discriminant $d(\mathcal{O})$ is defined to be the R-ideal generated by the set $\{\det(\mathrm{tr}(x_ix_j)), 1\le i,j\le 4\}$, where $x_i\in\mathcal{O}$. We will use the following facts about orders (cf. [Maclachlan and Reid 03]):

(i) Any order is contained in a maximal order.

(ii) An order $\mathcal{O}$ is maximal if and only if $d(\mathcal{O})=\Delta(A)^2$.

(iii) If $\mathcal{O}$ has the free R-basis $\{e_1,e_2,e_3,e_4\}$, then the discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is the principal ideal $\det(\mathrm{tr}(e_ie_j))R$.

Proposition 5.1. *Suppose that k has class number 1 and that ab is square-free, where $a,b\in R$. 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 $\pi_iR=\mathcal{P}_i$ for each $\mathcal{P}_i\notin\mathrm{Ram}_f(A)$ and*

$$r=\begin{cases}1 & \text{if } \Delta(A)=abR,\\ \prod\limits_{\substack{\mathcal{P}_i\mid abR\\ \mathcal{P}_i\nmid\Delta(A)}}\pi_i & \text{if } \Delta(A)\ne abR.\end{cases}$$

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

$$\beta\in\frac{1}{2r}\mathcal{O}'.$$

Proof: By assumption, all ideals of R are principal. Since $d(\mathcal{O}')=16a^2b^2R$, the order $\mathcal{O}'$ is not maximal and $\mathcal{O}'\subset\mathcal{O}$ for some maximal order $\mathcal{O}$. In particular, $d(\mathcal{O})=\Delta(A)^2$. Since ab is square-free, $abR=r_1\Delta(A)$, up to multiplication by a unit. Moreover, R is a principal ideal domain, so both $\mathcal{O}'$ and $\mathcal{O}$ have free bases, say $\{e_i\}_{i=1}^4$ and $\{f_j\}_{j=1}^4$, respectively. Since $\mathcal{O}'\subset\mathcal{O}$, we can write each e_i as $\sum_{j=1}^4 a_{ij}f_j$, where $a_{ij}\in R$. We therefore have

$$\begin{aligned}16a^2b^2=d(\mathcal{O}')&=\det(\mathrm{tr}(e_ie_j))=(\det M)^2\det(\mathrm{tr}(f_if_j))\\&=(\det M)^2 d(\mathcal{O}),\end{aligned}$$

where $M=(a_{ij})$. Thus, up to multiplication by a unit, $\det M=4r$. This implies $\mathcal{O}\subset\frac{1}{4r}\mathcal{O}'$, i.e.,

$$\beta=\frac{1}{4r}(x_0+x_1i+x_2j+x_3ij),$$

where $x_i\in R$, $0\le i\le 3$. But since β is an integer, its trace must be integral: $\mathrm{tr}(\beta)=\frac{x_0}{2r}\in R$. From this it follows that $x_0\in 2R$. Similarly, taking the products $i\beta$, $j\beta$, and $ij\beta$ and using the hypothesis that $\mathcal{O}'[\beta]$ is an order, it follows that $x_1,x_2,x_3\in 2R$. Therefore, $\beta\in\frac{1}{2r}\mathcal{O}'$, as claimed. □

Lemma 5.2. *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*

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

and either of the following conditions:

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

(ii)′ $b = -1$ *and* $\exists\, \tilde{a} \in R$ *such that* $\tilde{a}^2 \equiv a \bmod 4R$.

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 exist $x, y \in R$ such that $x^2 - ay^2 \equiv b \bmod 4R$, or equivalently, such that $x^2 - ay^2 - b \in 4R$. Suppose conditions (i) and (ii) hold. Then $x^2 - ay^2 - b \equiv 0 \bmod 4R$ is equivalent to $x^2 - \tilde{a}^2 y^2 \equiv \tilde{b}^2 \bmod 4R$.

The equation

$$x - \tilde{a}y \equiv \tilde{b} \bmod 2R \tag{5–1}$$

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

$$x - \tilde{a}_{\mathcal{P}} y \equiv \tilde{b}_{\mathcal{P}} \bmod R_{\mathcal{P}} \tag{5–2}$$

has a nonzero solution $(\tilde{x}_{\mathcal{P}}, \tilde{y}_{\mathcal{P}})$ 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 (5–2) clearly has a nonzero solution $(\tilde{x}_{\mathcal{P}}, \tilde{y}_{\mathcal{P}})$ for each prime $\mathcal{P}$ dividing 2. Therefore, (5–1) has a nontrivial solution $(x, y) \in R$. Since $x - \tilde{a}y \equiv \tilde{b} \bmod 2R$ if and only if $x + \tilde{a}y \equiv \tilde{b} \bmod 2R$, it follows that (x, y) satisfies

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

If conditions (i) and (ii)′ hold, then the equation $x^2 - ay^2 - b \equiv x^2 - \tilde{a}^2 y^2 - b \equiv 0 \bmod 4R$ is equivalent to

$$-x^2 + \tilde{a}y^2 \equiv 1 \bmod 4R.$$

Again, by the Chinese remainder theorem, there exists $(x, y) \in R \times R$ such that $-x + \tilde{a}y \equiv 1 \bmod 2R$, and the proof now follows as above. □

Lemma 5.3. *Let $A = \left(\frac{a,b}{k}\right)$ be a quaternion algebra with $a, b \in R$ such that $abR = \Delta(A)$. Let $\mathcal{O}' = R[1, i, j, ij]$, so that $\mathcal{O}'$ is an order in A. If $\beta \in \frac{1}{2}\mathcal{O}' \setminus \mathcal{O}'$ has the form $\frac{1}{2}(x_0 + x_1 i + x_2 j)$ and is integral, then $\mathcal{O} = R[1, i, \beta, i\beta]$ is a ring of integers. If, in addition, $x_2 \in R^*$, 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:

(i) $e_k e_l$ is integral for $0 \le k, l \le 3$;

(ii) $e_k + e_l$ is integral for $0 \le k, l \le 3$.

The simple structure of this order makes many of these conditions redundant. The conditions in (i) and (ii) are conditions that the norms and traces of these elements belong to R. Moreover, (i) and (ii) also establish that $\mathcal{O}$ is closed under multiplication. The norms and traces of these elements are listed in Tables 3 and 4. Note that although the elements $e_k e_l$ and $e_l e_k$, $k \neq l$, may not be equal, their traces and norms are equal (hence, both tables are symmetric). We have also omitted the obvious cases, e.g., 1 and i.

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

(i) $x_0^2 - ax_1^2 - bx_2^2 \in 4R$;

(ii) $(x_0^2 - ax_1^2 - bx_2^2)^2 \in 16R$;

(iii) $x_0^2 + ax_1^2 + bx_2^2 \in 2R$.

Condition (i) implies all the others. We will show that (i) implies (iii). The condition $x_0^2 - ax_1^2 - bx_2^2 \in 4R$ implies $x_0^2 - ax_1^2 - bx_2^2 \in 2R$, since $4R \subset 2R$. But $x_0^2 - ax_1^2 - bx_2^2 \equiv x_0^2 - ax_1^2 - bx_2^2 \bmod 2R$, so $x_0^2 - ax_1^2 - bx_2^2 \in 2R$ if and only if $x_0^2 + ax_1^2 + bx_2^2 \in 2R$. However, condition (i) is equivalent to the integrality of β. This shows that the integrality of β implies the integrality of all elements of $\mathcal{O} = R[1, i, \beta, i\beta]$. Thus, if β is integral, then $\mathcal{O}$ is a ring of integers.

We will now assume that $x_2 \in R^*$. In order to show that $\mathcal{O}$ is an order, we must show that $R[1, i, \beta, i\beta]$ is a complete R-lattice with 1. It is clear that $\mathcal{O}$ is an R-lattice. Since $1, i \in \mathcal{O}$, it remains to show that $j \in \mathcal{O}$. Since $\beta = \frac{1}{2}(x_0 + x_1 i + x_2 j) \in \mathcal{O}$, we have $j = x_2^{-1}(2\beta - x_1 - x_2 i) \in \mathcal{O}$, and hence I is complete. Therefore, $R[1, i, \beta, i\beta]$ is an order. Moreover, the discriminant of the order $R[1, i, \beta, i\beta]$ is $d(\mathcal{O}) = a^2 b^2 x_2^4 R = a^2 b^2 R = \Delta A^2$, since $x_2 \in R^*$. Hence, $\mathcal{O} = R[1, i, \beta, i\beta]$ is maximal. □

Proposition 5.4. *Let $A = \left(\frac{a,b}{k}\right)$ be a quaternion algebra over a number field k with finite ramification set $\mathrm{Ram}_f(A)$ 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 5.2 and in addition, that $\Delta(A) = abR$.*

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

TABLE 3. Norms and traces of sums of the R-basis of $\mathcal{O}$ in Lemma 5.3.

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

TABLE 4. Norms and traces of products of the R-basis of $\mathcal{O}$ in Lemma 5.3.

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: As noted previously, the order $\mathcal{O}' = R[1, i, j, k]$ has discriminant $d(\mathcal{O}') = 16a^2b^2R$ and is therefore 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, $d(\mathcal{O}) = a^2b^2R = \Delta(A)^2$. The ideal $I = \frac{1}{2}\mathcal{O}' \supset \mathcal{O}'$ is not an order, since its elements, $\frac{1}{2}$ for instance, are not all integral. But the discriminant of I is equal to a^2b^2R. Therefore, $\mathcal{O}' \subset \mathcal{O}$. This implies that there exists some $\beta \in \frac{1}{2}\mathcal{O}'$ such that $\beta \in \mathcal{O}$.

Since a, b satisfy the hypothesis of Lemma 5.2, 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 5.3, $I = R[1, i, \beta, i\beta]$ is a maximal order. □

If the Hilbert symbol of A does not satisfy the conditions of the previous proposition, we can still use Proposition 5.1 as a starting point, but the process of finding a free basis for $\mathcal{O}$ becomes more ad hoc. One uses an intermediate order $\mathcal{O}''$, where $\mathcal{O}' \subset \mathcal{O}'' \subset \frac{1}{2}\mathcal{O}'$ with $d(\mathcal{O}'') = a^2b^2R$, and searches for integral elements in the ideal $\frac{1}{r}\mathcal{O}''$, where $r \in R$ is as stated in the proof of Lemma 5.1. By testing 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 computing the discriminants of these orders, one can determine a maximal order in the algebra.

5.2 Fundamental Domains and Generators

Let A be the invariant quaternion algebra corresponding to the arithmetic Fuchsian group $\Gamma^1_{\mathcal{O}}$. For any maximal order $\mathcal{O}$ of A, fix an embedding ρ of $\mathcal{O}^1$ in $\mathrm{PSL}_2(\mathbb{R})$ and denote the image by $\Gamma^1_{\mathcal{O}}$. Choose ρ such that $i \in \mathbb{H}^2$ is not the fixed point of any nontrivial element in $\Gamma^1_{\mathcal{O}}$. The Möbius transformation

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

maps $\mathbb{H}^2$ to the unit disk $\mathcal{U}$. Furthermore, the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}^2$ is conjugate to the action of $\mathrm{SU}(1,1)$ on $\mathcal{U}$, since

$$\mathrm{SU}(1,1) = \varphi\,\mathrm{SL}_2(\mathbb{R})\varphi^{-1}.$$

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

For any $g \in \mathrm{SU}(1,1)$ or $\mathrm{SL}_2(\mathbb{R})$,

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

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.

The following theorem of Ford (cf. [Katok 92, Chapter 3]) characterizes a fundamental domain of $\Gamma \subset \mathrm{SU}(1,1)$ in terms of the isometric circles of its elements.

Theorem 5.5. *Let Γ be a discrete subgroup of $\mathrm{SU}(1,1)$ 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 $\varphi^{-1}(\Gamma)\varphi$. Let r_g be the radius of the isometric circle C_g, where $g \in \Gamma$ for a discrete subgroup Γ of $\mathrm{SU}(1,1)$. Since

$$\mathrm{SU}(1,1) = \left\{ \begin{pmatrix} a & c \\ \bar{c} & \bar{a} \end{pmatrix} \middle| a, c \in \mathbb{C},\ a\bar{a} - c\bar{c} = 1 \right\},$$

the radius r_g is equal to $\frac{1}{|c|}$. 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, $0 < \epsilon < 1$. If for some $\epsilon > 0$,

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

then $\mathcal{F}_\epsilon$ will be a fundamental domain for Γ. This will be the case for some sufficiently small $\epsilon > 0$, since Γ has finite coarea and no parabolic elements.

Using this consequence of Ford's theorem one can systematically obtain the generators for arithmetic Fuchsian groups if one can a find free R-basis for the maximal order. We use this technique in conjunction with our results on maximal orders to obtain generators for some of the unit groups $\Gamma^1_{\mathcal{O}}$ listed in Theorem 4.10. Our main interest will be in the cases $3 \le |k : \mathbb{Q}| \le 4$, since examples of this type are lacking in the literature. Although this technique is described in generality in [Johansson 00], we will include a description here for completeness.

Let r_g denote the radius of the isometric circle $\varphi g \varphi^{-1}$, where $g \in \Gamma \subset \mathrm{PSL}_2(\mathbb{R})$. If

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

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,

$$r_g = \frac{2}{|(b+c) - i(a-d)|} = \frac{2}{\sqrt{(a-d)^2 + (b+c)^2}} = \frac{2}{\sqrt{a^2 + b^2 + c^2 + d^2 - 2}}. \tag{5–3}$$

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.

Let $|k : \mathbb{Q}| = n$ and suppose that k has the integral power basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. By properties of quaternion algebras over the real numbers, we may assume that $A = \left(\frac{a,b}{k}\right)$, 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 Proposition 5.1, 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

$$g = \frac{1}{r} \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{5–4}$$

with

$$\begin{aligned} A &= \left(\sum x_i \alpha^i\right) + \left(\sum y_i \alpha^i\right)\sqrt{a}, \\ B &= b_1\left(\left(\sum u_i \alpha^i\right) + \left(\sum v_i \alpha^i\right)\sqrt{a}\right), \\ C &= b_2\left(\left(\sum u_i \alpha^i\right) - \left(\sum v_i \alpha^i\right)\sqrt{a}\right), \\ D &= \left(\sum x_i \alpha^i\right) - \left(\sum y_i \alpha^i\right)\sqrt{a}, \end{aligned}$$

where $r \in R \setminus \{0\}$ and the integers x_i, y_i, u_i, v_i, $0 \le i \le n-1$, are in $\mathbb{Z}$. The integrality of the elements in $\mathcal{O}$ translates 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 $n(g) = \frac{1}{r^2}(x^2 - ay^2 - bu^2 + abv^2)$. Since norm is invariant under each embedding σ_i of the number field, $n(g) = 1$ implies $n(\sigma_i(g)) = 1$, for $1 \le i \le n$. 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 $\sigma_1(a) > 0$, $\sigma_1(b) < 0$,

$\sigma_i(a) < 0$, and $\sigma_i(b) < 0$ for $2 \le i \le n$. Therefore, for each i, $2 \le i \le n$,

$$|\sigma_i(x)| \le \sigma(r), \tag{5–5}$$
$$|\sigma_i(y)| \le \sqrt{\frac{\sigma(r)^2 - \sigma_i(x)^2}{-\sigma_i(a)}},$$
$$|\sigma_i(v)| \le \sqrt{\frac{\sigma(r)^2 - \sigma_i(x)^2 + \sigma_i(a)\sigma_i(y)^2}{\sigma_i(a)\sigma_i(b)}},$$
$$|\sigma_i(u)| \le \sqrt{\frac{\sigma(r)^2 - \sigma_i(x)^2 + \sigma_i(a)\sigma_i(y)^2 - \sigma_i(a)\sigma_i(b)\sigma_i(v)^2}{-\sigma_i(b)}}.$$

Substituting into (5–3), we get that $r_g = \frac{2}{\sqrt{q-2}}$, where

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

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

$$|x| < r\sqrt{\frac{M_\epsilon}{2}},$$
$$|y| < \sqrt{\frac{1}{2a}\left(r^2M_\epsilon - 2x^2\right)},$$
$$|v| < \sqrt{\frac{b_1^2+b_2^2}{4ab^2}\left(r^2M_\epsilon - 2x^2 - 2ay^2\right)}, \tag{5–6}$$
$$|u| < \sqrt{\frac{1}{b_1^2+b_2^2}\left(r^2M_\epsilon - 2x^2 - 2ay^2 - \frac{4ab^2}{b_1^2+b_2^2}v^2\right)} + \frac{b_1^2-b_2^2}{b_1^2+b_2^2}\sqrt{a}|v|.$$

By taking various linear combinations of these inequalities, we obtain bounds on the integers $x_i, y_i, u_i, v_i \in \mathbb{Z}$, $0 \le i \le n-1$.

6. EXAMPLES

In this section, we use our previous results to find generators for a few examples of the DAFGs $\Gamma^1_{\mathcal{O}}$ in Theorem 4.10 with signature $(1; 2, 2)$, $(0; 2, 2, 2, 2, 2, 2)$, or $(2; -)$ using programs written in Mathematica [Macasieb 05, Appendix B]. (A complete list of generators for all the groups $\Gamma^1_{\mathcal{O}}$ with one of these signatures can be found in [Macasieb 05, Chapter 5].) Using a standard presentation of the group $\Gamma^1_{\mathcal{O}}$ and MAGMA, we also explicitly determine generators for each subgroup Γ of signature $(2; -)$.

Here we give examples in which the Hilbert symbol of A satisfies the hypotheses of Proposition 5.4 and examples in which it does not. All elements of $\Gamma^1_{\mathcal{O}}$ will be given as a vector of integers using an integral power basis of R with a specified denominator r; cf. (5–4). Also, we will abuse notation and use the same vector to describe the corresponding matrix in $\mathrm{SL}_2(\mathbb{R})$.

Example 6.1. Let $k = \mathbb{Q}(\cos(\frac{\pi}{7})) = k(\alpha)$ be the totally real cubic field of degree 3, where α is a root of the polynomial $f(x) = x^3 - x^2 - 2x + 1$. The group $\Gamma^1_{\mathcal{O}}$ with invariant quaternion algebra A defined over k with $\mathrm{Ram}_f(A) = \{\mathcal{P}_2, \mathcal{P}_7\}$ is generated by the elements shown in Table 5, where $r = 2$ and $\langle A_1, B_1, X_1 | ([A_1, B_1]X_1)^2, X_1^2\rangle$. Here the vectors A_1, B_1, and X_1 are as described in (5–4) with $a = 2(2\alpha - 3)$ and $b = -1$.

Proof: The cubic field k_7 has minimal polynomial $f(x) = x^3 - x^2 - 2x + 1$ and discriminant 49. By Proposition 4.10, there is only one conjugacy class of groups $\Gamma^1_{\mathcal{O}}$ of signature $(1; 2, 2)$ defined over k. If we denote the three roots of $f(x)$ by α_1, α_2, and α_3, where $\alpha_1 < 0 < \alpha_2 < \alpha_3$, then the algebra

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

has the correct ramification set. This can easily be checked using standard results in algebra (cf. [Maclachlan and Reid 03, Chapter 2]).

In this case, one can check that A does not satisfy the hypotheses of Proposition 5.4. However, since $\mathcal{P}_2 = 2R$ and $\mathcal{P}_7 = (2\alpha-3)R$, we have $abR = 2(2\alpha-3)R = \mathcal{P}_2\mathcal{P}_7 = \Delta(A)$. Therefore, a maximal order $\mathcal{O}$ of A will nonetheless be of the form $R[1, i, \beta, i\beta]$, where $\beta \in \frac{1}{2}\mathcal{O}' \backslash \mathcal{O}'$, where $\mathcal{O}' = R[1, i, j, ij]$. The element $\beta = \frac{1}{2}(1 + i + j)$ is integral, since $\mathrm{tr}(\beta) = 1 \in R$, $n(\beta) = -\alpha + 2 \in R$, and $d(\mathcal{O}') = \mathcal{P}_2^2\mathcal{P}_7^2 = \Delta(A)^2$, so that $\mathcal{O}'$ is maximal. We can write $\frac{1}{2}R[1, i, j, ij]$ as the $\mathbb{Z}$-module

$$\left\{\frac{1}{2}\Big(\sum_{k=1}^{3} x_k\alpha^k + i\sum_{k=1}^{3} y_k\alpha^k + j\sum_{k=1}^{3} u_k\alpha^k + ij\sum_{k=1}^{3} v_k\alpha^k\Big) \Big| \; x_i, y_i, u_i, v_i \in \mathbb{Z}\right\}.$$

Similarly, we write $\mathcal{O} = (m_i + n_i i + o_i\beta + p_i i\beta)$, where $m_i, n_i, o_i, p_i \in \mathbb{Z}[1, \alpha, \alpha^2, \alpha^3]$. Clearly, $\mathcal{O} \subset \frac{1}{2}R[1, i, j, ij]$. Equating the two $\mathbb{Z}$-modules 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

	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
X_1	0	0	0	0	0	0	2	0	0	0	0	0

TABLE 5. Generators for the group $\Gamma^1_{\mathcal{O}}$ in Example 6.1.

of $\mathcal{O}$. In this particular case, $\mathcal{O}$ is the set of elements of $\frac{1}{2}R[1, i, j, ij]$ satisfying the following congruence relations:

$$x_0 + u_0 \equiv 0 \bmod 2, \qquad y_0 + u_0 + v_0 \equiv 0 \bmod 2,$$
$$x_1 + u_1 \equiv 0 \bmod 2, \qquad y_1 + u_1 + v_1 \equiv 0 \bmod 2,$$
$$x_2 + u_2 \equiv 0 \bmod 2, \qquad y_2 + u_2 + v_2 \equiv 0 \bmod 2.$$

We implement the inequalities (5–5) and (5–6) with the values $r = 2$, $b_1 = 2$, and $b_2 = -\frac{1}{2}$, and in this case, $\epsilon = 0.15$ is sufficient to obtain the Ford domain for $\Gamma^1_{\mathcal{O}}$.

The Ford domain for the group $\Gamma^1_{\mathcal{O}}$ is shown in Figure 1. Since v_1 and v_2 are distinct fixed points of elements of order two, $\Gamma^1_{\mathcal{O}}$ has signature $(1; 2, 2)$. The elements listed in Table 6 are the generators for $\Gamma^1_{\mathcal{O}}$ corresponding to the side pairings of the Ford domain.

The elements $A_1 = h_2^{-1}$, $h = h_1 h_3^{-1}$, $X_1 = g_1$ are noncommuting hyperbolic elements that satisfy the relation $([A_1, B_1]X_1)^2 = -I$. Furthermore, no proper subrelation is trivial. Therefore, if we denote the group $\langle A_1, B_1, X_1 | ([A_1, B_1]X_1)^2, X_1^2\rangle$ by Γ', then Γ' has signature $(1; 2, 2)$. Since $h_1 = A_1^{-1}X_1$ and $h_4 = A_1^{-1}B_1^{-1}$, we have $\langle A_1, B_1, X_1\rangle \subset \Gamma^1_{\mathcal{O}}$. But since Fuchsian groups are Hopfian, $\Gamma^1_{\mathcal{O}}$ cannot contain a proper isomorphic subgroup. Therefore, $\Gamma^1_{\mathcal{O}} = \langle A_1, B_1, X_1 | ([A_1, B_1]X_1)^2, X_1^2\rangle$ and A_1, B_1, X_1 are generators for $\Gamma^1_{\mathcal{O}}$.

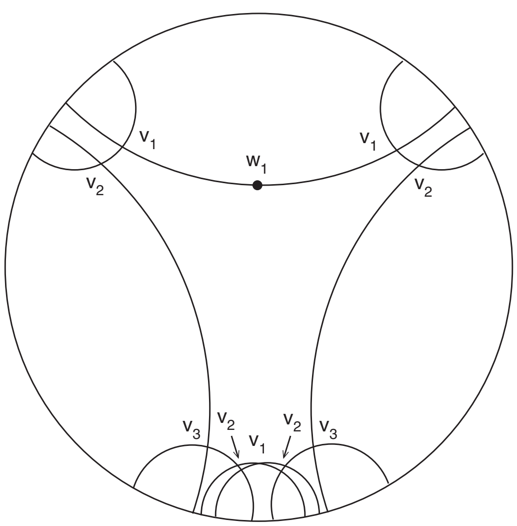

FIGURE 1. Fundamental region for $\Gamma^1_{\mathcal{O}}$ in Example 6.1.

In this case, one can easily check that the group $\Gamma^1_{\mathcal{O}}$ has four distinct subgroups Γ_i, $1 \le i \le 4$, of signature $(2; -)$ of index two. Using the standard presentation

$$\left\langle A_1, B_1, X_1, Y_1 \mid [[A_1, B_1]X_1Y_1, X_1^2, Y_1^2]\right\rangle$$

for $\Gamma^1_{\mathcal{O}}$, 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 presentations for these subgroups are as follows:

$$\Gamma_1 = \left\langle B_1A_1^{-1}, X_1A_1^{-1}, Y_1A_1^{-1}, A_1^{-2}\right\rangle,$$
$$\Gamma_2 = \left\langle B_1, X_1A_1^{-1}, Y_1A_1^{-1}, A_1^{-2}\right\rangle,$$
$$\Gamma_3 = \left\langle A_1, X_1B_1^{-1}, Y_1B_1^{-1}, B_1^{-2}\right\rangle,$$
$$\Gamma_4 = \left\langle A_1, B_1, X_1A_1X_1, X_1B_1X_1\right\rangle.$$

For each Γ_i, we determine the trivial relation in the group. After putting each group in the standard presentation $\langle a_i, b_i, c_i, d_i | [a_i, b_i][c_i, d_i]\rangle$, $1 \le i \le 4$, we obtain the corresponding list of generators (see Table 7).

□

Example 6.2. Let $k = \mathbb{Q}(\alpha)$ be the totally real quartic field of discriminant 3981, where α is a root of the polynomial $f(x) = x^4 - x^3 - 4x^2 + 2x + 1$. The group $\Gamma^1_{\mathcal{O}}$ corresponding to the quaternion algebra A with $\mathrm{Ram}_f(A) = \{\mathcal{P}_3\}$ that is unramified at the infinite place corresponding to the root α_2, where $-1 < \alpha_2 < 0$, defined over k has generators as shown in Table 8, where $r = 2$ and

$$\left\langle X_1, X_2, X_3, X_4, X_5 \mid X_1^2, X_2^2, X_3^2, X_4^2, X_5^2, (X_1X_2X_3X_4X_5)^2\right\rangle.$$

Here $a = -\alpha(\alpha + 1)$ and $b = -1$.

Proof: Let $\alpha_1 < -1 < \alpha_2 < 0 < \alpha_3 < 1 < \alpha_4$ denote the four roots of $f(x)$. 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 $-\alpha_2(\alpha_2 + 2) > 0$. There is a unique prime of norm 3 in R_k: $\mathcal{P}_3 = (3, \alpha+1)R = (\alpha+1)R$. Furthermore, one can easily verify that $\mathrm{Ram}_f(A) = \{\mathcal{P}_3\}$. This is a "nice" Hilbert symbol, so Proposition 5.4 applies, and we

	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 6. Generators for $\Gamma^1_{\mathcal{O}}$ in Example 6.1.

	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
c_1	0	2	2	−1	2	2	0	2	2	−1	2	2
d_1	30	−42	−52	−30	42	53	−32	46	58	−26	38	47
a_2	−3	2	3	1	−2	−2	1	−2	−3	−2	2	3
b_2	−14	20	24	−12	18	22	−12	20	24	12	−18	−22
c_2	30	−42	−52	−30	42	53	−32	46	58	−26	38	47
d_2	0	2	2	−1	2	2	0	2	2	−1	2	2
a_3	0	2	2	−1	2	2	0	2	2	1	−2	−2
b_3	−14	21	25	13	−18	−23	18	−25	−31	−15	23	28
c_3	1	−2	−3	−2	2	3	3	−2	−3	−1	2	2
d_3	−37	52	65	−33	47	59	−3	2	3	2	−3	−4
a_4	0	2	2	−1	2	2	0	2	2	1	−2	−2
b_4	−3	2	3	1	−2	−2	1	−2	−3	−2	2	3
c_4	0	−2	−2	−1	2	2	0	−2	−2	1	−2	−2
d_4	3	−2	−3	1	−2	−2	−1	2	3	−2	2	3

TABLE 7. Generators for $\Gamma_i, 1 \leq i \leq 4$ in Example 6.1.

	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
X_1	0	−2	4	1	−1	2	−4	−1	1	−3	4	1	−1
X_2	0	0	0	0	2	0	0	0	0	0	0	0	0
X_3	0	−2	4	1	−1	−2	4	1	−1	3	−4	−1	1
X_4	0	−3	4	1	−1	−17	18	7	−5	36	−39	−15	11
X_5	0	0	0	0	0	20	−22	−8	6	−42	50	18	−14

TABLE 8. Generators for $\Gamma^1_{\mathcal{O}}$ in Example 6.2.

find that $\mathcal{O} = R[1, i, \beta, i\beta]$, where $\beta = \frac{1}{2}(1 + \alpha + \alpha^2 i + j)$ is a maximal order. The congruence relations in this case are

$$x_0 + u_0 + u_3 + v_0 \equiv 0 \bmod 2,$$
$$y_0 + u_2 + u_3 + v_0 + v_3 \equiv 0 \bmod 2,$$
$$x_1 + u_0 + v_1 \equiv 0 \bmod 2,$$
$$y_1 + u_3 + v_0 + v_1 \equiv 0 \bmod 2,$$
$$x_2 + u_1 + u_2 + v_2 \equiv 0 \bmod 2,$$
$$y_2 + u_0 + v_1 + v_2 \equiv 0 \bmod 2,$$
$$x_3 + u_2 + v_3 \equiv 0 \bmod 2,$$
$$y_3 + u_1 + u_2 + u_3 + v_2 \equiv 0 \bmod 2.$$

In this case, we implement inequalities (5–5) and (5–6) using $r = 2$, $b_1 = 2$, $b_2 = -\frac{1}{2}$, and $\epsilon = 0.15$. We obtain the fundamental region shown in Figure 2, and the corresponding generators are listed in Table 9. The points w_i are the fixed points of the g_i, $1 \leq i \leq 6$, which all have order two; this verifies that $\Gamma^1_{\mathcal{O}}$ has signature $(0; 2, 2, 2, 2, 2, 2)$.

After putting the group in the required presentation, we obtain the list as stated above. A group of signature $(0; 2, 2, 2, 2, 2, 2)$ has a unique subgroup Γ of signature $(2; -)$ by [Greenberg 63]. Using Magma, we find that if $\Gamma^1_{\mathcal{O}}$ is presented in the form

$$\big\langle X_2X_1, X_3X_1, X_4X_1, X_5X_1 \mid X_1^{-1}X_2X_3^{-1}X_4X_1X_2^{-1}X_2X_4^{-1}\big\rangle,$$

then the subgroup Γ is generated by

$$\langle X_2X_1, X_3X_1, X_4X_1, X_5X_1\rangle.$$

	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 9. Generators for $\Gamma^1_{\mathcal{O}}$ in Example 6.2.

Putting these generators in the standard form

$$\langle a_1, b_1, c_1, d_1 | [a_1, b_1][c_1, d_1] \rangle$$

yields the set of generators for Γ listed in Table 10. $\square$

Our last example is defined over a quartic number field in which the Hilbert symbol of A does not satisfy the hypotheses of Proposition 5.4. We will show that a "nice" symbol does not exist for A. We remark that the technique for finding a maximal order is similar to that of the previous examples, except that in this case we cannot take r to be a rational integer.

Example 6.3. Let $k = \mathbb{Q}(\alpha)$ be the totally real quartic field of discriminant 4752, where α is a root of the polynomial $f(x) = x^4 - 2x^3 - 3x^2 + 4x + 1$. The group $\Gamma^1_{\mathcal{O}}$ of signature $(2; -)$ defined over k with quaternion algebra A satisfying $\mathrm{Ram}_f(A) = \{\mathcal{P}_2\}$ and unramified at the infinite place corresponding to the root α_1, where $-2 < \alpha_1 < -1$, has the generators listed in Table 11.

Here $a = 1 + \alpha$ and $b = (1 - \alpha)(-1 + \alpha + \alpha^2)$.

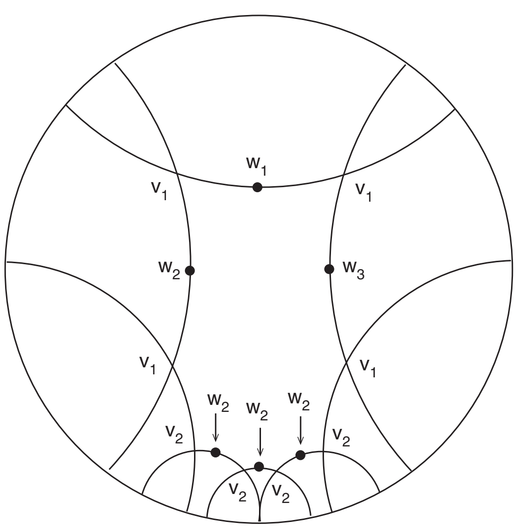

FIGURE 2. Fundamental region for $\Gamma^1_{\mathcal{O}}$ in Example 6.2.

Proof: Let $\alpha_1 < -1 < \alpha_2 < 0 < 1 < \alpha_3 < 2 < \alpha_4$ denote the four real roots of $f(x)$. A fundamental system for R^* is $\langle \alpha, \alpha - 1, \alpha^2 - 2 \rangle$. 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 as follows:

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

From the table of embeddings, it is evident that there does not exist a Hilbert symbol for A such that the only primes dividing abR are in $\mathrm{Ram}_f(A)$. In this case, the algebra

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

is unramified at the place σ_1. The element $1 + \alpha$ is a uniformizer for $\mathcal{P}_3$ in R (since $f(x) \equiv (x+1)^4 \bmod 3$, $\mathcal{P}_3$ 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 mod 3. Thus, A corresponds to one of the two conjugacy classes of $\Gamma^1_{\mathcal{O}}$ defined over k.

In this case, we use an intermediate order to find a maximal order $\mathcal{O}$. The order $\mathcal{O}' = R[1, i, \gamma, i\gamma]$, where $\gamma = \frac{1}{2}((1 + \alpha) + (1 + \alpha^2)i + j)$, has discriminant

$$\begin{aligned} d(\mathcal{O}') &= (1 + \alpha)^2 (-1 + \alpha)^2 (-1 + \alpha + \alpha^2)^2 R \\ &= \mathcal{P}_3^2 \mathcal{P}_2^2 R \neq \Delta(A)^2, \end{aligned}$$

and therefore is not maximal. Thus, $\mathcal{O}' \subset \mathcal{O}$, for some maximal order $\mathcal{O}$. Again, by arguments analogous to those in the proof of Proposition 5.1, one can argue that there exists an element $\beta \in \mathcal{O} \cap \frac{1}{\alpha+1}\mathcal{O}' \backslash \mathcal{O}'$. An element in $\mathcal{O}'$ written as an integral vector satisfies the following

	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
a_1	9	−11	−4	3	67	−75	−28	31	−35	39	15	−11	39	−43	−16	12
b_1	2	−4	−1	1	−10	11	4	−3	7	−7	−3	2	−11	14	5	−4
c_1	−12	14	5	−4	26	−28	−11	8	−14	18	6	−5	31	−36	−13	10
d_1	−2	4	1	−1	31	−36	−13	10	−14	18	6	−5	3	−4	−1	1

TABLE 10. Generators for Γ in Example 6.2.

	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	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

TABLE 11. Generators for $\Gamma^1_{\mathcal{O}}$ in Example 6.3.

congruence relations:

$$\begin{aligned}
x_0 + u_0 + u_3 + v_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2,\\
x_1 + u_0 + v_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2,\\
x_2 + u_1 - u_2 + u_3 + v_0 + v_3 &\equiv 0 \bmod 2,\\
x_3 + u_2 + u_3 + v_0 + v_1 &\equiv 0 \bmod 2, \qquad (6\text{–}1)\\
y_0 - u_0 + u_2 + v_0 + v_3 &\equiv 0 \bmod 2,\\
y_1 + u_1 + u_3 + v_0 + v_1 &\equiv 0 \bmod 2,\\
y_2 + u_0 + v_1 + v_2 + v_3 &\equiv 0 \bmod 2,\\
y_3 + u_1 + v_2 + v_3 &\equiv 0 \bmod 2.
\end{aligned}$$

Consider an element of the form

$$\begin{aligned}
\beta &= \frac{1}{2(\alpha+1)}(x + yi + uj + vij) \in I\\
&= \frac{1}{\alpha+1}\mathcal{O}'\backslash\mathcal{O}'.
\end{aligned}$$

Now, β is integral if and only if

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

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

$$\begin{aligned}
x &= (1+\alpha)(r_0 + r_1\alpha + r_2\alpha^2 + r_3\alpha^3)\\
&= (r_0 - r_3) + (r_0 + r_1 - 4r_3)\alpha + (r_1 + r_2 + 3r_3)\alpha^2\\
&\quad + (r_2 + 3r_3)\alpha^3,\\
d &= 4(1+\alpha)^2(s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3) \qquad (6\text{–}2)\\
&= 4(s_0 - s_2 - 4s_3) + 4(2s_0 + s_1 - 4s_2 - 17s_3)\alpha\\
&\quad + 4(s_0 + 2s_1 + 4s_2 + 8s_3)\alpha^2 + 4(s_1 + 4s_2 + 12s_3)\alpha^3,
\end{aligned}$$

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 (6–1), 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,

$$\begin{aligned}
i\beta &= \frac{1}{2(\alpha+1)}\big((1+\alpha+2\alpha^2)(\alpha+1)\\
&\qquad + (1+\alpha+\alpha^2+\alpha^3)i + (\alpha+1)j\big)\\
&= \frac{1}{2}\left((1+\alpha+2\alpha^2) + (1+\alpha^2)i + j\right).
\end{aligned}$$

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

TABLE 12. Norms and traces of sums of the R-basis of $\mathcal{O}$ in Example 6.3.

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

TABLE 13. Norms and traces of products of the R-basis of $\mathcal{O}$ in Example 6.3.

This implies $j = 2i\beta - (1+\alpha+2\alpha^2) - (1+\alpha^2)i \in I$. The integrality of the elements of I is verified using (6–2), and the traces and norms of the R-basis are listed in Tables 12 and 13.

Since $R[1, i, \beta, i\beta]$ has discriminant $\mathcal{P}_2^2 = \Delta(A)^2$, it is a maximal order, and hence $\mathcal{O} = R[1, i, \beta, i\beta]$. Finally, we determine the congruence relations for $\mathcal{O}$ written as a $\mathbb{Z}$-module:

$$4x_0 - x_1 + x_2 - x_3 + u_0 + 2u_1 - 2u_2 + 2u_3 - 3v_0 + 3v_2 \equiv 0 \bmod 6,$$
$$x_0 - x_1 + x_2 - x_3 - 2u_0 + 2u_1 - 8u_2 - 7u_3 - 3v_1 \equiv 0 \bmod 6,$$
$$4y_0 - y_1 + y_2 - y_3 - u_0 - 2u_1 + 2u_2 + u_3 + v_0 + 2v_1 - 2v_2 + 2v_3 \equiv 0 \bmod 6,$$
$$y_0 - y_1 + y_2 - y_3 + 2u_0 - 2u_1 - u_2 + u_3 - 2v_0 + 2v_1 - 2v_2 - v_3 \equiv 0 \bmod 6,$$
$$-u_0 + u_1 - u_2 + u_3 \equiv 0 \bmod 3,$$
$$x_2 + x_3 + u_1 + v_1 + v_3 \equiv 0 \bmod 2,$$
$$x_0 + x_1 + x_2 + u_2 + v_0 \equiv 0 \bmod 2,$$
$$y_2 + y_3 + u_0 + u_1 + v_1 \equiv 0 \bmod 2,$$
$$y_0 + y_1 + y_2 + u_1 + u_2 + u_3 + v_2 \equiv 0 \bmod 2.$$

Here we use $b_1 = \pm b_2 = \pm\sqrt{(\alpha - 1)(\alpha^2 - \alpha + 1)}$ and $\epsilon = 0.1$ in (5–5) and (5–6). The fundamental region for $\Gamma^1_{\mathcal{O}}$ is shown in Figure 3, and the corresponding generators are those listed in Table 11. □

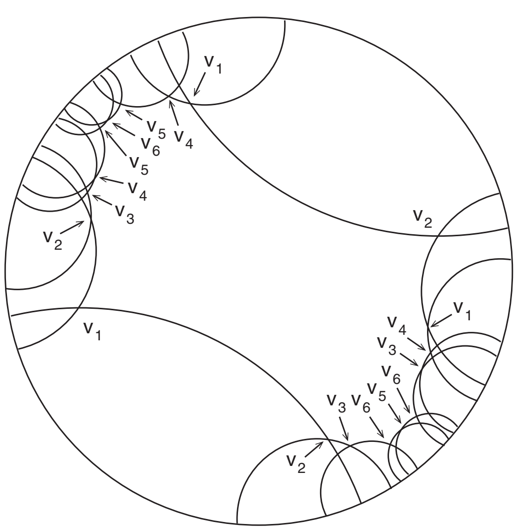

FIGURE 3. Fundamental region for $\Gamma^1_{\mathcal{O}}$ in Example 6.3.

ACKNOWLEDGMENTS

This work comprises a large part of the author's doctoral thesis, and as such, the author is sincerely grateful and indebted to her advisor, Alan W. Reid, and would like to thank him

him for suggesting the problem and for the many enlightening conversations concerning it. The author would also like to thank Felipe Voloch for pointing out the connection between solutions to the quadratic form in Lemma 5.2 and the Chinese remainder theorem and Fernando Rodriguez-Villegas for helpful comments regarding the ramification of quaternion algebras at dyadic primes (cf. [Macasieb 05, Chapter5]). Lastly, the author thanks the referee for many helpful comments and suggestions that contributed to the improvement of this paper. This research was partially supported by an NSF VIGRE fellowship at the University of Texas at Austin.

REFERENCES

[Ackermann et al. 03] 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)*, pp. 1–9, Res. Exp. Math. 27. Lemgo: Heldermann, 2003.

[Borel 81] A. Borel. "Commensurability Classes and Volumes of Hyperbolic 3-Manifolds." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* 8:1 (1981), 1–33.

[Chinburg and Friedman 99] T. Chinburg and E. Friedman. "An Embedding Theorem for Quaternion Algebras." *J. London Math. Soc. (2)* 60:1 (1999), 33–44.

[Cohen et al. 95] H. Cohen et al. "List of Number Fields of Degree $\leq$ 7." Available online (ftp://pari.math.u-bordeaux.fr/pub/numberfields/), 1995.

[Edmonds et al. 82] A. L. Edmonds, J. H. Ewing, and R. S. Kulkarni. "Torsion Free Subgroups of Fuchsian Groups and Tessellations of Surfaces." *Invent. Math.* 69:3 (1982), 331–346.

[Greenberg 63] L. Greenberg. "Maximal Fuchsian Groups." *Bull. Amer. Math. Soc.* 69 (1963), 569–573.

[Johansson 98] S. Johansson. "Genera of Arithmetic Fuchsian Groups." *Acta Arith.* 86:2 (1998), 171–191.

[Johansson 00] S. Johansson. "On Fundamental Domains of Arithmetic Fuchsian Groups." *Math. Comp.* 69:229 (2000), 339–349.

[Katok 92] S. Katok. *Fuchsian Groups*, Chicago Lectures in Mathematics. Chicago: University of Chicago Press, 1992.

[Macasieb 05] M. L. Macasieb. "Derived Arithmetic Fuchsian Groups of Genus Two." PhD thesis, University of Texas at Austin, 2005.

[Maclachlan and Reid 03] C. Maclachlan and A. W. Reid. *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Mathematics 219. New York: Springer-Verlag, 2003.

[Maclachlan and Rosenberger 83] C. Maclachlan and G. Rosenberger. "Two-Generator Arithmetic Fuchsian Groups." *Math. Proc. Cambridge Philos. Soc.* 93:3 (1983), 383–391.

[Maclachlan and Rosenberger 92] C. Maclachlan and G. Rosenberger. "Two-Generator Arithmetic Fuchsian Groups II." *Math. Proc. Cambridge Philos. Soc.* 111:1 (1992), 7–24.

[Odlyzko 75] A. M. Odlyzko. "Some Analytic Estimates of Class Numbers and Discriminants." *Invent. Math.* 29:3 (1975), 275–286.

[Parry 75] C. J. Parry. "Units of Algebraic Number Fields." *J. Number Theory* 7:4 (1975), 385–388.

[Pohst et al. 90] M. Pohst, J. Martinet, and F. Diaz y Diaz. "The Minimum Discriminant of Totally Real Octic Fields." *J. Number Theory* 36:2 (1990), 145–159.

[Ribenboim 72] P. Ribenboim. *Algebraic Numbers*, Pure and Applied Mathematics 27. New York: Wiley, 1972.

[Schneider 75] V. Schneider. "Die elliptischen Fixpunkte zu Modulgruppen in Quaternionenschiefkörpern." *Math. Ann.* 217:1 (1975), 29–45.

[Takeuchi 77] K. Takeuchi. "Commensurability Classes of Arithmetic Triangle Groups." *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 24:1 (1977), 201–212.

[Takeuchi 83] K. Takeuchi. "Arithmetic Fuchsian Groups with Signature $(1; e)$." *J. Math. Soc. Japan* 35:3 (1983), 381–407.

[Vignéras 80] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics 800. Berlin: Springer, 1980.

[Washington 97] L. C. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83. New York: Springer-Verlag, 1997.

Melissa L. Macasieb, Department of Mathematics, University of British Columbia, Vancouver BC V6T 1Z2, Canada (macasieb@math.ubc.ca)

Received November 27, 2006; accepted in revised form January 26, 2008.