Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds

T. Chinburg*, E. Hamilton, D. D. Long†, and A. W. Reid‡

June 19, 2008

Abstract

We show that if M is an arithmetic hyperbolic 3-manifold, the set $\mathbb{Q}L(M)$ of all rational multiples of lengths of closed geodesics of M both determines and is determined by the commensurability class of M. This implies that the spectrum of the Laplace operator of M determines the commensurability class of M. We also show that the zeta function of a number field with exactly one complex place determines the isomorphism class of the number field.

1 Introduction

Let M be a closed, orientable Riemannian manifold of negative curvature. The *rational length spectrum* $\mathbb{Q}L(M)$ of M is the set of all rational multiples of lengths of closed geodesics of M. The commensurability class of M is the set of all manifolds M' for which M and M' have a common finite unramified cover. Our main result is:

Theorem 1.1 *If M is an arithmetic hyperbolic 3-manifold, then the rational length spectrum and the commensurability class of M determine one another.*

This sharpens [12], where it was shown that the complex length spectrum of M determines its commensurability class.

Suppose M' is an arithmetic hyperbolic 3-manifold which is not commensurable to M. Theorem 1.1 implies $\mathbb{Q}L(M) \neq \mathbb{Q}L(M')$, though by Example 2.4 below it is possible that one of $\mathbb{Q}L(M')$ or $\mathbb{Q}L(M)$ contains the other. By the length formulas recalled in §2.1 and §2.2, each element of $\mathbb{Q}L(M) \cup \mathbb{Q}L(M')$ is a rational multiple of the logarithm of a real algebraic number. As noted by Prasad and Rapinchuk in [11], the Gelfond Schneider Theorem [1] implies that a ratio of such logarithms is transcendental if it is irrational. Thus if $\ell \in \mathbb{Q}L(M) - \mathbb{Q}L(M')$ then ℓ/ℓ' is transcendental for all non-zero $\ell' \in \mathbb{Q}L(M')$.

Recently Prasad and Rapinchuk have shown in [11] that if M is an arithmetic hyperbolic manifold of even dimension, then $\mathbb{Q}L(M)$ and the commensurability class of M determine one another. In addition, they have shown that this is not always true for arithmetic hyperbolic 5-manifolds. However, they have announced a proof that for all locally symmetric spaces associated to a specified absolutely simple real Lie group, there are only finitely many commensurability classes of arithmetic lattices giving rise to a given rational length spectrum. Their results do not apply to the case considered in this paper, however, because the real Lie group $\mathrm{PSL}_2(\mathbb{C})$ is not absolutely simple. It is a natural problem to develop a common generalization of this paper and [11].

*Partially supported by N. S. F.
†Partially supported by N. S. F.
‡Partially supported by N. S. F.

It is known (see [4] pp. 415–417) that for closed hyperbolic manifolds, the spectrum of the Laplace-Beltrami operator action on $\mathrm{L}^2(M)$, counting multiplicities, determines the set of lengths of closed geodesics on M (without counting multiplicities). Hence Theorem 1.1 implies:

Corollary 1.2 *The spectrum of the Laplacian of an arithmetic hyperbolic* 3*-manifold* M *determines the commensurability class of* M*.*

This result was claimed but not proved in [12] where the corresponding result was proved for arithmetic hyperbolic surfaces. There have been many constructions over the years of manifolds with the same Laplace-Beltrami spectrum which are not isometric; see [9], [14], [15], [7], [13] and [3]. Apart from [7] the methods of these papers all provide commensurable manifolds.

We now describe the organization of this paper. Some preliminary results concerning arithmetic Kleinian groups are recalled in §2. Suppose that $\Gamma \subset \mathrm{PSL}_2(\mathbb{C})$ is a torsion-free arithmetic Kleinian group associated to an arithmetic hyperbolic three-manifold M. The invariant trace field of Γ is the number field k_Γ generated over $\mathbb{Q}$ by squares of traces of pre-images of elements of Γ in $\mathrm{SL}_2(\mathbb{C})$. It is clear that the commensurability class of M determines $\mathbb{Q}L(M)$. The first step in proving the converse is to show in Theorem 6.1(a) that k_Γ is determined by $\mathbb{Q}L(M)$. We then determine the commensurability class of M from $\mathbb{Q}L(M)$ following ideas similar to those in [12] (see Theorem 6.1(b)).

The main technical work in the proof of Theorem 1.1 is contained in §3 - §5 and concerns Galois theory. One by-product in §3 is the following result:

Theorem 1.3 *Suppose that* k *and* k' *are global fields which are finite separable extensions of a global field* F *and which have the same Galois closure* k^{cl} *over* F*. Suppose there is a place* v *of* F *which splits into exactly* $[k:F]-1$ *places in* k *and into exactly* $[k':F]-1$ *places in* k'*. Then after replacing* k' *by an isomorphic field, either* $k = k'$*, or* k *and* k' *are quadratic non-isomorphic extensions of a common subfield* k^+ *in which* v *splits completely. In the latter case, if* $F = \mathbb{Q}$ *then the zeta functions* $\zeta_k(s)$ *and* $\zeta_{k'}(s)$ *are not equal.*

This theorem is a consequence of a group theoretic result (Lemma 3.3) concerning finite groups G for which there are subgroups H and T and an element $c \in G$ which acts as a transposition on the faithful left G-sets G/H and G/T. We show that a conjugate gHg^{-1} of H by some $g \in G$ is either equal to T or generates with T a group which contains both T and gHg^{-1} with index 2, and we give a complete analysis of how the latter exceptional case can occur. In Remark 3.6 we mention a generalization of Theorem 1.3 to finite étale Galois covers of schemes.

Since number fields with the same zeta function have the same Galois closure over $\mathbb{Q}$, Theorem 1.3 implies:

Corollary 1.4 *If* k *is a number field in which some place of* $\mathbb{Q}$ *splits into exactly* $[k:\mathbb{Q}]-1$ *places, then* k *is determined up to isomorphism by its zeta function. In particular, this conclusion holds if* k *has exactly one complex place.*

This Corollary contrasts with the fact that that there are many examples of number fields which are not determined up to isomorphism by their zeta functions (see [10] and [2]).

2 Preliminaries

In this section we recall some facts about arithmetic Kleinian groups $\Gamma \subset \mathrm{PSL}_2(\mathbb{C})$; see [8] for details.

2.1 Length spectra and eigenvalues

Let Γ be a torsion free discrete finite covolume Kleinian group, so that $M = \mathbf{H}^3/\Gamma$ is a hyperbolic 3-manifold. For $\gamma \in \Gamma$, let λ be an eigenvalue of a pre-image of γ in $\mathrm{SL}_2(\mathbb{C})$ for which $|\lambda| > 1$. Then λ is well-defined up to multiplication by ± 1, and we will refer to $\lambda = \lambda(\gamma)$ as an eigenvalue of γ. The axis of γ in $\mathbf{H}^3$ projects to a closed geodesic $c(\gamma)$ in M which depends only on the conjugacy class of γ in Γ. This defines a bijection between the conjugacy classes of hyperbolic elements of Γ and the set of closed geodesics of $\mathbf{H}^3/\Gamma$. The length of $c(\gamma)$ is $\mathrm{l}(\gamma) = 2\ln|\lambda| = \ln|\lambda\overline{\lambda}|$ where $\lambda\overline{\lambda}$ is algebraic over $\mathbb{Q}$.

2.2 Arithmetic Kleinian groups

Let k be a number field with one complex place, and fix a non-real embedding $\rho_k : k \to \mathbb{C}$. Let B/k be a quaternion algebra which is ramified at all real places of k, and let $\rho_B : B \to \mathrm{Mat}_2(\mathbb{C})$ be an embedding extending the embedding ρ_k. Let O_k be the integers of k, and let $\mathcal{O}$ be an O_k-order of B. Define $\mathcal{O}^1$ to be the multiplicative group of elements of $\mathcal{O}$ of reduced norm 1 to k. Then $\rho_B(\mathcal{O}^1)$ is a subgroup of $\mathrm{SL}(2,\mathbb{C})$ whose projection $\overline{\rho}_B(\mathcal{O}^1)$ to $\mathrm{PSL}(2,\mathbb{C})$ is discrete and of finite covolume. A Kleinian group Γ is called arithmetic if it is commensurable with a group of the form $\overline{\rho}_B(\mathcal{O}^1)$ for some k, B, ρ_B and $\mathcal{O}$ of the above kind. If Γ is a subgroup of some $\overline{\rho}_B(\mathcal{O}^1)$, then Γ is called *derived from a quaternion algebra*. It can be shown (see [8, Theorem 8.3.1 and Cor. 8.3.6]) that a Kleinian group Γ of finite covolume is arithmetic if and only if the group $\Gamma^{(2)}$ generated by the squares of elements of Γ is derived from a quaternion algebra, and in this case

$$k = \mathbb{Q}(\{\mathrm{tr}(\gamma^2) : \gamma \in \Gamma\}) = \mathbb{Q}(\{\mathrm{tr}(\eta) : \eta \in \overline{\rho}_B(\mathcal{O}^1)\}). \tag{2.1}$$

The orbifold $M = \mathbf{H}^3/\Gamma$ is a manifold if and only if Γ has no elliptic elements, and this orbifold is compact if and only if B is a division algebra. Our analysis of the commensurability class of M hinges on the following fact (c.f. [8, Thm. 8.4.1]).

Theorem 2.1 *The commensurability class of M determines, and is determined by, the isomorphism class of B as a $\mathbb{Q}$-algebra.*

2.3 Invariant trace fields and quaternion division algebras

In this section we will suppose that k and B satisfy the conditions in §2.2 and that B is a division algebra. We fix an embedding of B into $\mathrm{Mat}_2(\mathbb{C})$, which fixes an embedding of k into $\mathbb{C}$. The following facts are proved in [8, Chapter 12].

Theorem 2.2 *Suppose that Γ is derived from B and that γ is a hyperbolic element of Γ with eigenvalue $\lambda = \lambda(\gamma)$.*

i. The field $k(\lambda)$ generated by λ over k is a quadratic extension field of k which embeds into B. If λ is real, then λ has degree 2 over the field $k \cap \mathbb{R}$.

ii. Let L be a quadratic extension of k. Then L embeds in B/k if and only if $L = k(\lambda(\gamma'))$ for some hyperbolic $\gamma' \in \Gamma$. This will be true if and only if no place of k which splits in L is ramified in B.

iii. Let B_1 and B_2 be quaternion algebras over number fields k_1 and k_2. A field isomorphism $\tau : k_1 \to k_2$ extends to an isomorphism $B_1 \to B_2$ of $\mathbb{Q}$-algebras if and only if $\tau(R_1) = R_2$ when R_i is the set of places of B_i which ramify over k_i.

iv. Let $\eta : k(\lambda) \to \mathbb{C}$ be an embedding. Then $\eta(k) \subset \mathbb{R}$ if and only if $|\eta(\lambda)| = 1$, and $\{\lambda, 1/\lambda, \overline{\lambda}, 1/\overline{\lambda}\}$ is the set of conjugates of λ off the unit circle.

Lemma 2.3 *Let Γ be as in Theorem 2.2. If λ is not real then $k = \mathbb{Q}(\lambda + 1/\lambda)$ and $[\mathbb{Q}(\lambda) : k] = 2$. If λ is real then $k^+ = \mathbb{Q}(\lambda + 1/\lambda)$ is the maximal totally real subfield of k, $[k : k^+] = 2$ and $\mathbb{Q}(\lambda)$ is a degree 2 extension of k^+.*

Proof. Since Γ is derived from a quaternion algebra, $\mathrm{tr}(\gamma) = \lambda + 1/\lambda \in k$ by (2.1). Suppose that $\mathbb{Q}(\lambda + 1/\lambda)$ is a proper subfield of k. A complex place of a proper subfield of k must split completely in k. Since k has just one complex place, this implies all proper subfields of k must be totally real, so $\lambda + 1/\lambda$ is totally real. Because γ is hyperbolic, $|\lambda| \neq 1$, so $\lambda + 1/\lambda \in \mathbb{R}$ implies $\lambda \in \mathbb{R}$. Hence if λ is not real then $k = \mathbb{Q}(\lambda + 1/\lambda)$, and then $[\mathbb{Q}(\lambda) : k] = 2$ by Theorem 2.2(i). For the rest of the proof we suppose that $\lambda \in \mathbb{R}$. Then $F = \mathbb{Q}(\lambda + 1/\lambda)$ is a proper subfield of k, so $\lambda + 1/\lambda$ is totally real. Suppose that $[k : F] \neq 2$. Since k has just two non-real embeddings, the embedding $F \subset \mathbb{R}$ determined by the non-real embedding $k \subset \mathbb{C}$ we have fixed can be extended to an embedding $\eta : k(\lambda) \hookrightarrow \mathbb{C}$ such that $\eta(k) \subset \mathbb{R}$. Theorem 2.2(iv) now implies implies $2 < |\lambda + 1/\lambda| = |\eta(\lambda + 1/\lambda)| = |\eta(\lambda) + \eta(\lambda)^{-1}| \leq 2$ so the contradiction shows $[k : F] = 2$. The last sentence of the lemma now follows from this, Theorem 2.2(i) and the fact that k is not totally real. □

We finish this section by showing how Theorem 1.1 can be used to provide proper inclusion of rational length sets.

Example 2.4 *Let B and k be as in §2.2, and let B' be a quaternion algebra over k which is not isomorphic to B but which ramifies over every place of k where B ramifies. Let M_1 (resp. M_2) be the manifold defined by a Kleinian group Γ_1 (resp. Γ_2) without elliptic elements which is derived from B (resp. B'). Then by Theorem 2.1, M_1 and M_2 are not commensurable. By Theorem 2.2, if γ is a hyperbolic element of Γ_2 then $L = k(\lambda(\gamma))$ embeds into B over k, where $\lambda(\gamma)$ is a unit of O_L having norm 1 to k. Since O_L embeds into some maximal order $\mathcal{O}$ of B, we conclude that there is a hyperbolic element $\gamma' \in \overline{\rho}_B(\mathcal{O}^1)$ such that $\lambda(\gamma) = \lambda(\gamma')$. A positive integral power of γ' lies in a conjugate of Γ_1, so we conclude from the length formulas of §2.1 that $\mathbb{Q}L(M_2) \subset \mathbb{Q}L(M_1)$. Note that Theorem 1.1 will imply that because M_1 and M_2 are not commensurable, $\mathbb{Q}L(M_1)$ must properly contain $\mathbb{Q}L(M_2)$.*

3 Galois theoretic results

The object of this section is to prove Theorem 1.3. As in the Theorem, let k and k' be finite separable extensions of a global field F which have the same Galois closure k^{cl} over F. Suppose there is a place v of F which splits into exactly $[k : F] - 1$ places in k and into exactly $[k' : F] - 1$ places in k'. Define $G = \mathrm{Gal}(k^{\mathrm{cl}}/F)$, $T = \mathrm{Gal}(k^{\mathrm{cl}}/k)$ and $H = \mathrm{Gal}(k^{\mathrm{cl}}/k')$.

Lemma 3.1 *Let $\Gamma = T$ or H and let $m = \#(G/\Gamma)$. The left multiplication action of G on G/Γ embeds G as a transitive permutation group inside $\mathrm{Perm}(G/\Gamma) \cong S_m$. The decomposition group G_w of a place w of k^{cl} over v has order 2 and is generated by a transposition c.*

Proof. We may identify G/Γ with the set of embeddings of $L = (k^{\mathrm{cl}})^{\Gamma}$ into k^{cl} over F, where $L = k$ or k'. The places of L over v correspond to the orbits of G_w on these embeddings. Since there are $[L : F] - 1 = \#(G/\Gamma) - 1$ such orbits, this forces G_w to be generated by a transposition. □

The following Lemma is a slightly more explicit form of a result of Klüners [6, Lemma 2.14]. For the convenience of the reader we will include a proof.

Lemma 3.2 *Suppose G is a transitive subgroup of $S_n = \mathrm{Perm}(\{1,\dots,n\})$ containing a transposition $c = (i,j)$. Let B be the block for the action of G on $\{1,\dots,n\}$ which is the intersection of all blocks which contain $\{i,j\}$. Define $\ell = \#B \geq 2$. Let G_B be the stabilizer of B in G.*

a. The action of G on the n/ℓ disjoint blocks $\mathcal{B} = \{hB\}_{h\in G/G_B}$ defines a surjection $\pi : G \to \overline{G}$ from G to a transitive subgroup $\overline{G}$ of $\mathrm{Perm}(\mathcal{B}) \cong S_{n/\ell}$.

b. The kernel of π is the normal subgroup $N = \prod_{g\in G/G_B} \mathrm{Perm}(gB) \cong S_\ell^{n/\ell}$, where in this product the elements of $\mathrm{Perm}(gB)$ fix each element of $G - gB$. This and part (a) give rise to an isomorphism between G and the wreath product $S_\ell \wr \overline{G}$.

c. The set $\mathcal{C}$ of conjugates of c in G equals $\coprod_{g\in G/G_B}(\mathcal{C} \cap \mathrm{Perm}(gB))$, where $\mathcal{C} \cap \mathrm{Perm}(gB) = \{(a,b) : a,b \in gB\}$ has $\ell(\ell-1)/2$ elements. Thus $\#\mathcal{C} = \#(G/G_B)\ell(\ell-1)/2 = n(\ell-1)/2$.

Proof. The action of G_B on B defines a primitive transitive subgroup of $\mathrm{Perm}(B)$ which contains a transposition. By Jordan's theorem (c.f. [5]), this group must contain all the permutations of B. Hence the orbit of the conjugation $c = (i,j)$ under the conjugation action of G_B is the set of all transpositions defined by pairs of elements of B, and the rest of the Lemma is clear from this. □

Lemma 3.3 *Suppose G is a finite group and that H and T are subgroups of G such that some element c of G acts as a transposition on the faithful left G-sets G/H and G/T. Then $n = [G:T]$ equals $n' = [G:H']$. Identify the cosets of G/T with $\{1,\dots,n\}$, so that G becomes a transitive subgroup of $\mathrm{Perm}(\{1,\dots,n\}) = S_n$ and c is identified with a transposition (i,j) for some $i \neq j$. Let B, G_B, $\mathcal{B}$, $\mathcal{C}$ and $\pi : G \to \overline{G}$ be as in Lemma 3.2. Then T is conjugate to the stabilizer G_i of i, and after replacing H by a conjugate of H in G, either H equals the G_i, or all of the following statements hold:*

i. The block B equals $\{i,j\}$, so that $\ell = 2$.

ii. B is the unique element of $\mathcal{B} = \{gB\}_{g\in G/G_B}$ fixed by H.

iii. The product set $H \cdot G_i$ is the group given by the inverse image $\pi^{-1}(\overline{G}_B)$ of the stabilizer $\overline{G}_B \subset \overline{G}$ of $B \in \mathcal{B}$ under the action of $\overline{G}$ on $\mathcal{B}$. Furthermore $H \cdot G_i$ is the direct product of $G_i = G_j$ with the order two group $\{e,c\}$, where $c = (i,j)$.

iv. The index of each of G_i and H in $H \cdot G_i = \pi^{-1}(\overline{G}_B)$ is 2, and $H \cap N = G_i \cap N$ is the group $N_0 \cong (\mathbb{Z}/2)^{n/\ell-1}$ generated by the set $\mathcal{C} - \{c\}$ of commuting transpositions. There is a unique quadratic character $\chi : \pi^{-1}(\overline{G}_B) \to \{\pm 1\}$ inflated from a character of $\overline{G}_B$ such that $H = \ker(\chi \cdot \xi)$ when $\xi : \pi^{-1}(\overline{G}_B) \to \{\pm 1\}$ is the quadratic character with kernel G_i.

v. H is not conjugate to T, and the characters of G defined by the left action of G on G/H and on G/T are not equal.

Conversely, suppose $\ell = 2$ in Lemma 3.2. Suppose H is a subgroup of index 2 in $\pi^{-1}(\overline{G}_B) = G_i \times \{e,c\}$ which is not equal to G_i, does not contain c and which contains $G_i \cap N$. Then c acts as a transposition on the cosets G/H, and (i) - (v) hold. Via (iv), these H correspond to bijectively to quadratic characters $\chi : \pi^{-1}(\overline{G}_B) \to \{\pm 1\}$ which are inflated from quadratic characters of $\overline{G}_B$.

Proof. Since T is the subgroup of G stabilizing the trivial coset T of G/T, and G acts transitively on G/T, T is conjugate to G_i. To prove $n = n'$ we may suppose by symmetry that $n' \geq n$. Let $Z_G(c)$ be the centralizer of c in G. The map $Z_G(c)\backslash G \to \mathcal{C}$ which sends $Z_G(c)g$ to $g^{-1}cg$ is bijective, where $\mathcal{C}$ is the conjugacy class of c. Since c acts as a transposition on the set of cosets G/H, there are

$\#G - 2\#H$ elements $g \in G$ such that $cgH = gH$. These g are exactly those for which $g^{-1}cg \in H \cap \mathcal{C}$. We conclude that

$$\frac{\#(H \cap \mathcal{C})}{\#\mathcal{C}} = \frac{\#(H \cap \mathcal{C}) \cdot \#Z_G(c)}{\#\mathcal{C} \cdot \#Z_G(c)} = \frac{\#G - 2\#H}{\#G} = 1 - \frac{2}{n'} \tag{3.2}$$

since $n' = [G : H]$. Lemma 3.2(c) now gives that

$$\#\mathcal{C} - \#(H \cap \mathcal{C}) = \#\mathcal{C} \cdot \frac{2}{n'} = \frac{n}{n'}(\ell - 1) \leq (\ell - 1). \tag{3.3}$$

Since $\ell \geq 2$ this proves $\mathcal{C} \not\subset H$. Hence there is a $g \in G/G_B$ such that $H' = H \cap \mathrm{Perm}(gB)$ is a proper subgroup of $\mathrm{Perm}(gB)$ in the notation of Lemma 3.2(c).

Suppose first that $\ell > 2$. Then there are $\ell(\ell-1)/2 > \ell - 1$ elements of $\mathcal{C}$ in $\mathrm{Perm}(gB)$ by Lemma 3.2(c), so (3.3) shows H' contains a transposition. Thus Jordan's theorem implies H' cannot be a primitive subgroup of $\mathrm{Perm}(gB)$, since $H' \neq \mathrm{Perm}(gB)$. We can therefore assume there is a block Z for the action of H' on gB such that $1 \leq \#Z \leq \#(gB)/2$. If $\#Z \geq 2$ then H cannot contain any transposition (i', j') with $i' \in Z$ and $j' \in gB - Z$. There are at least $2(\ell/2) = \ell$ such transpositions, contradicting (3.3). Hence $Z = \{i'\}$ for some $i' \in \{1, \ldots, n\}$ and H does not contain the $\ell - 1$ transpositions (i', j') for which $j' \in gB - Z$. This shows that $n = n'$ in (3.3) and that the elements of $\mathcal{C}$ not in H are exactly these (i', j'). The description of G and $\mathcal{C}$ in Lemma 3.2 now shows that i' is the unique element of $\{1, \ldots, n\}$ such that H contains no transposition of the form (i', j') in $\mathcal{C}$ for some j'. Thus H is contained in the stabilizer $G_{i'}$ of i' in G. Since $[G : H] = n' = n = [G : G_{i'}]$ we conclude that $H = G_{i'}$. Since $G_{i'}$ is conjugate to G_i in G, this completes the proof if $\ell > 2$.

For the rest of the proof we now suppose $\ell = 2$, so that the block B equals $\{i, j\}$ and $\mathcal{C}$ consists of $n/\ell = n/2$ commuting transpositions. Since $n \leq n'$ and $\frac{n}{n'}(\ell - 1) = \frac{n}{n'}$ is integral by (3.3), one has $n = n'$ and there is a unique element $(i', j') = c' \in \mathcal{C}$ not in H. Thus the block $B' = \{i', j'\}$ must be fixed by H. After replacing H by a conjugate of H in G, we can assume $B' = B = \{i, j\}$. Then H and G_i are contained in $\pi^{-1}(\overline{G}_B)$, and these groups both contain the subgroup $N_0 \cong (\mathbb{Z}/2)^{n/2-1}$ of $N \cong (\mathbb{Z}/2)^{n/2}$ which is generated by the $n/2-1$ commuting transpositions in $G_i \cap \mathcal{C} = H \cap \mathcal{C} = \mathcal{C} - \{c\}$. Every element of $\pi^{-1}(\overline{G}_B)$ either fixes i and j or interchanges them, and every element of G which fixes i and j commutes with $c = (i, j)$. We conclude that $\pi^{-1}(\overline{G}_B)$ is the direct product of $G_i = G_j$ with $\{e, c\}$ and $\pi^{-1}(\overline{G}_B) \cap N = N_0$. Thus $[\pi^{-1}(\overline{G}_B) : G_i] = 2$, so since $n = [G : G_i]$ equals $n' = [G : H]$, we see that H is an index 2 subgroup of $\pi^{-1}(\overline{G}_B)$ containing $N_0 = N \cap G_i$. Thus H and G_i are normal subgroups of $\pi^{-1}(\overline{G}_B)$ and are the kernels of quadratic characters τ and ξ, respectively, from $\pi^{-1}(\overline{G_B})$ to $\{\pm 1\}$.

If $H = G_i$ then Lemma 3.3 holds. So we suppose from now on that $H \neq G_i$. Then τ and ξ are distinct, trivial on $N_0 \subset H \cap G_i$ and $\tau(c) = \xi(c) = -1$ since c is in neither H nor G_i. Thus $\chi = \tau\xi^{-1}$ is a quadratic character of $\pi^{-1}(\overline{G}_B)$ which is trivial on c as well as on N_0. Since N is generated by c and N_0, we conclude that χ is inflated from a quadratic non-trivial character of $\pi^{-1}(\overline{G}_B)/N = \overline{G}_B$, and $H = \ker(\tau) = \ker(\chi \cdot \xi)$.

We must now show that the characters χ_T and χ_H of G defined by the actions of G on $G/T = \{1, \ldots, n\}$ and G/H, respectively, are not equal. Suppose $\chi_T = \chi_H$. By Mackey's formula, the multiplicity of the trivial representation of T in the restriction of χ_T (resp. χ_H) to T equals $\#(T\backslash G/T)$ (resp. $\#(T\backslash G/H)$). Hence $\chi_T = \chi_H$ implies $\#(H\backslash G/T) = \#(T\backslash G/H) = \#(T\backslash G/T) = \#(T\backslash G/T)$, so the numbers of orbits of H and of T acting on $G/T = \{1, \ldots, n\}$ are equal. However, this is not the case, for the following reason. We have shown that H and T have the same image $\overline{G}_B$ in $\overline{G} = G/N$, where N is the normal subgroup of G generated by the $n/2$ pairwise disjoint transpositions in $\mathcal{C}$. Each such transposition (i', j') defines a block $\{i', j'\}$ for the action of G on $G/T = \{1, \ldots, n\}$. Furthermore, both H and T contain the subgroup N_0 of N generated by $\mathcal{C} - \{c\}$ where $c = (i, j)$. Thus if $i' \notin \{i, j\}$ then i' has the same orbit under the actions of H and of T,

namely union of the blocks of G given by the orbit of $\overline{G}_B$ acting on the block $\{i', j'\}$. On the other hand, if $i' \in \{i, j\}$ then $\{i', j'\} = \{i, j\}$ and both i' and j' are fixed by $T = G_i = G_j$. Because H is not G_i or G_j but H fixes the block $\{i, j\}$, there must be an element of H which permutes i' and j'. Thus there is one fewer orbit for the action of H on $\{1, \ldots, n\}$ than for the action of T. The contradiction shows $\chi_T \neq \chi_H$. The proof of the final converse statement in Lemma 3.3 consists of reversing the above arguments. □

We can now prove a more detailed version of Theorem 1.3 concerning fields F, k and k' satisfying the hypotheses stated at the beginning of this section.

Theorem 3.4 *The group $G = \mathrm{Gal}(k^{\mathrm{cl}}/k)$ satisfies the hypotheses of Lemma 3.3 when we let $T = \mathrm{Gal}(k^{\mathrm{cl}}/k)$, $H = \mathrm{Gal}(k^{\mathrm{cl}}/k')$ and when we let c be the transposition generating the decomposition group of a place w of k^{cl} over k. Suppose ℓ and N are as in Lemma 3.3, and let k^+ (resp. k'^+) be the maximal extension of F in k (resp. in k') in which v splits completely. Let $(k^+)^{\mathrm{cl}}$ be the Galois closure of k^+ over F.*

i. The field $(k^+)^{\mathrm{cl}}$ is the maximal extension $(k^{\mathrm{cl}})^N$ of F in k^{cl} in which v splits completely.

ii. The fields k^+ and k'^+ are isomorphic and their isomorphism class is determined by F, v, $(k^+)^{\mathrm{cl}}$ and k^{cl}.

iii. If $\ell > 2$ then k and k' are isomorphic, and $[k : k^+] > 2$.

iv. Suppose $\ell = 2$. After replacing k' by one if its conjugate fields over F inside k^{cl}, either $k' = k$ or the fields k and k' are non-isomorphic quadratic extensions of k^+. In the latter case, if $F = \mathbb{Q}$ then the zeta functions $\zeta_k(s)$ and $\zeta_{k'}(s)$ are not equal.

Proof. The fact that G, T, H and c satisfy the hypotheses of Lemma 3.3 is a consequence of Lemma 3.1. Letting c be the transposition (i, j) we may replace k by a conjugate field in such a way that T is identified with the stabilizer G_i. Since N is the normal subgroup generated by the conjugacy class of c, $(k^{\mathrm{cl}})^N$ is the maximal extension of F in k^{cl} in which v splits completely. The subfield k^+ is the fixed field for the action on k^{cl} of the group $\langle G_i, N\rangle$ generated by $G_i = T = \mathrm{Gal}(k^{\mathrm{cl}}/k)$ and by N. By Lemmas 3.2 and 3.3, the quotient group $\langle G_i, N\rangle/N$ is the stabilizer $\overline{G}_B$ of the block B containing i, where $\overline{G} = G/N$ acts transitively and faithfully on the set $\mathcal{B}$ of blocks for the action of G on $G/T = \{1, \ldots, n\}$ defined in Lemma 3.2. The intersection of the conjugates of $\overline{G}_B$ in $\overline{G}$ is therefore trivial, so the intersection of the conjugates of $\langle G_i, N\rangle$ in G is N and $(k^+)^{\mathrm{cl}} = (k^{\mathrm{cl}})^N$.

Suppose now that F, k^{cl} and $(k^+)^{\mathrm{cl}}$ are given. The groups $G = \mathrm{Gal}(k^{\mathrm{cl}}/k)$ and $N = \mathrm{Gal}(k^{\mathrm{cl}}/(k^+)^{\mathrm{cl}})$ are then determined. Lemma 3.3 shows that in all cases, after replacing k' by a conjugate field, the groups $\langle T, N\rangle$ and $\langle H, N\rangle$ are equal. Since the fixed fields of these groups acting on k^{cl} are k^+ and k'^+, respectively, this proves part (ii) of Theorem 3.4.

Suppose $\ell > 2$. Lemma 3.3 k and k' are isomorphic. By Lemma 3.1, $N \cong S_\ell^{n/\ell}$, and $N \cap G_i \cong S_{\ell-1} \times S_\ell^{n/\ell-1}$ is the stabilizer of i in N. We thus have

$$[k : k^+] = [\langle G_i, N\rangle : G_i] \geq [N : N \cap G_i] = [S_\ell : S_{\ell-1}] = \ell > 2.$$

We now suppose that $\ell = 2$. Part (iv) of Theorem 3.4 follows directly in this case from Lemmas 3.1, 3.2, 3.3 and the fact that when $F = \mathbb{Q}$, $\zeta_k(s)$ determines the character of the permutation representation $\mathbb{C}[G/T]$ of G via the Cebotarev density theorem. □

Remark 3.5 *The smallest possible degree over F of non-isomorphic fields k and k' as in Theorems 1.3 and 3.4 is* 6. *It is not hard to check that all minimal degree examples can be constructed in the*

following way when $\mathrm{char}(F) \neq 2$. *Let* v *be a place of* F. *Let* k^+ *be a non-Galois cubic extension of* F *in which* v *splits. The Galois closure* $(k^+)^{\mathrm{cl}}$ *is then an* S_3 *extension of* F *in which* v *splits, so it contains a unique quadratic extension* $L = F(\sqrt{d})$ *in which* v *splits, where* $d \in F$. *Suppose that* $\alpha \in k^+$ *is a square at two of the places of* k^+ *over* v *and a non-square at the remaining place over* v. *Then* k *and* k' *can be taken to be isomorphic to* $k^+(\sqrt{\alpha})$ *and* $k^+(\sqrt{d \cdot \alpha})$, *respectively. A numerical example is given by letting* v *be the infinite place of* $F = \mathbb{Q}$ *and by letting* α *be the unique negative real root of* $f(x) = x^3 - 4x + 1$. *Then* $k^+ = \mathbb{Q}(\alpha)$, $k = k^+(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$ *and* $k' = k^+(\sqrt{37 \cdot \alpha}) = \mathbb{Q}(\sqrt{37 \cdot \alpha})$.

Remark 3.6 *One can generalize Theorem 1.3 by replacing the field extensions* k *and* k' *of* F *by finite étale covers* X *and* X' *of a connected scheme* Y *which are quotients of a common finite Galois étale cover of* Y. *One replaces the place* v *of* F *by a point of* Y *which is assumed to lie under exactly* $[X : Y] - 1$ *points of* X *and exactly* $[X' : Y] - 1$ *points of* X'. *The same group theoretic arguments then show that after replacing* X' *by a Galois conjugate over* Y, *either* $X = X'$ *or* X *and* X' *have a common degree two quotient* X'' *over* Y *in which* v *splits completely.*

4 Galois closures of fields generated by eigenvalues and logarithms of lengths.

Throughout this section we assume that Γ is an arithmetic Kleinian group derived from a quaternion algebra B/k. We view k as a subfield of $\mathbb{C}$ via a fixed a non-real embedding $\rho_k : k \to \mathbb{C}$. Let $\gamma \in \Gamma$ be a hyperbolic element with eigenvalue $\lambda = \lambda(\gamma)$, so $|\lambda| > 1$. We assume the notations of §3 concerning k. Let k^+ be the maximal totally real subfield of k.

Proposition 4.1 *If* λ *is real, then* $\mathbb{Q}(\lambda) = \mathbb{Q}(\lambda\overline{\lambda}) = \mathbb{Q}(\lambda^2)$, *so* $\mathbb{Q}(\lambda)^{\mathrm{cl}} = \mathbb{Q}(\lambda\overline{\lambda})^{\mathrm{cl}}$.

Proof. Since γ^2 has eigenvalue λ^2, we conclude from Lemma 2.3 that $k^+ \subset \mathbb{Q}(\lambda^2) \subset \mathbb{Q}(\lambda)$ and that each of $\mathbb{Q}(\lambda^2)$ and $\mathbb{Q}(\lambda)$ have degree 2 over k^+. Hence $\mathbb{Q}(\lambda^2) = \mathbb{Q}(\lambda)$. □

Lemma 4.2 *Suppose that* λ *is not real. Then* $[\mathbb{Q}(\lambda, \overline{\lambda}) : \mathbb{Q}(\lambda\overline{\lambda})] = 2$ *and every* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\lambda)^{\mathrm{cl}}/\mathbb{Q}(\lambda\overline{\lambda}))$ *either fixes or interchanges* λ *and* $\overline{\lambda}$.

Proof. Since λ is not real, complex conjugation takes λ to $\overline{\lambda} \neq \lambda$ and fixes $\mathbb{Q}(\lambda\overline{\lambda})$. The Lemma now follows from the fact shown in Theorem 2.2(iv) that λ and $\overline{\lambda}$ have larger complex absolute value than any of the other conjugates of λ. □

Lemma 4.3 *Suppose that* $\ell = 2$ *in Theorem 3.4 and that* λ *is not real. Then* $k = \mathbb{Q}(\lambda + \lambda^{-1})$ *is a degree two extension of the totally real field* k^+. *There are two possibilities:*

a. The field $\mathbb{Q}(\lambda) = \mathbb{Q}(\overline{\lambda})$ *is quadratic over* k *and Galois of degree four over* k^+.

b. The extensions $\mathbb{Q}(\lambda)$ *and* $\mathbb{Q}(\overline{\lambda})$ *are distinct quadratic extensions of* k. *The extension* $\mathbb{Q}(\lambda, \overline{\lambda})$ *is a dihedral extension of degree* 8 *of* k^+. *The field* $\mathbb{Q}(\lambda\overline{\lambda})$ *is a non-Galois degree four extension of* k^+ *inside* $\mathbb{Q}(\lambda, \overline{\lambda})$, *and* $\mathbb{Q}(\lambda\overline{\lambda}) \cap k = k^+$.

Proof. We know from Lemma 2.3 that $k = \mathbb{Q}(\lambda + \lambda^{-1})$, so $\lambda + \lambda^{-1}$ is not real. By Theorem 3.4, k is stable under complex conjugation, and $k^+ = k \cap \mathbb{R}$ is the maximal totally real subfield of k, with $[k : k^+] = 2$. By Theorem 2.2(i), $[\mathbb{Q}(\lambda) : k] = [\mathbb{Q}(\lambda) : \mathbb{Q}(\lambda + \lambda^{-1})] = 2$.

If $\mathbb{Q}(\lambda) = \mathbb{Q}(\overline{\lambda})$, complex conjugation defines an automorphism of $\mathbb{Q}(\lambda)$ over k^+ which gives a non-trivial automorphism of k. Then $[\mathbb{Q}(\lambda) : k] = [k : k^+] = 2$ implies $\mathbb{Q}(\lambda)/k^+$ is Galois of degree 4.

Now suppose $\mathbb{Q}(\lambda) \neq \mathbb{Q}(\overline{\lambda})$. Then $\mathbb{Q}(\lambda)/k^+$ is a quartic extension containing the quadratic extension k/k^+. Complex conjugation sends k to k, fixes k^+ and carries $\mathbb{Q}(\lambda)$ to $\mathbb{Q}(\overline{\lambda})$. This implies $\mathbb{Q}(\lambda, \overline{\lambda})$ is a dihedral extension of k^+ of degree 8. By Lemma 4.2, $[\mathbb{Q}(\lambda, \overline{\lambda}) : \mathbb{Q}(\lambda\overline{\lambda})] = 2$. The rest of part (b) follows from this and the fact that $\mathbb{Q}(\lambda\overline{\lambda}) = \mathbb{Q}(\lambda) \cap \mathbb{R} \supset k^+$ is fixed by complex conjugation while k is not. $\square$

Proposition 4.4 *Suppose that λ is not real, and that either $\ell > 2$ or that $\ell = 2$ and that option (b) of Lemma 4.3 holds. Then the Galois closure $\mathbb{Q}(\lambda)^{\mathrm{cl}}$ of $\mathbb{Q}(\lambda)$ over $\mathbb{Q}$ equals $\mathbb{Q}(\lambda\overline{\lambda})^{\mathrm{cl}}$.*

Proof. If $\ell = 2$, Lemma 4.3(b) implies $\mathbb{Q}(\lambda\overline{\lambda})$ is a non-Galois quartic extension of k^+ inside the dihedral degree 8 extension $\mathbb{Q}(\lambda, \overline{\lambda})$ of k^+. Hence the Galois closure of $\mathbb{Q}(\lambda\overline{\lambda})$ over k^+ is $\mathbb{Q}(\lambda, \overline{\lambda})$, and this implies that $\mathbb{Q}(\lambda\overline{\lambda})^{\mathrm{cl}} = \mathbb{Q}(\lambda)^{\mathrm{cl}}$.

The remaining case to consider is when λ is complex and $\ell > 2$. Then $\mathbb{Q}(\lambda)$ is a quadratic extension of $k = \mathbb{Q}(\lambda + \lambda^{-1})$ by Lemma 2.3. The inclusion $k^{\mathrm{cl}} \subset \mathbb{Q}(\lambda)^{\mathrm{cl}}$ gives a surjection $q : \mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\lambda)^{\mathrm{cl}}/\mathbb{Q}) \to \mathrm{Gal}(k^{\mathrm{cl}}/\mathbb{Q}) = G$. Define $\mathcal{H} = \mathrm{Gal}(\mathbb{Q}(\lambda)^{\mathrm{cl}}/\mathbb{Q}(\lambda\overline{\lambda})) \subset \mathcal{G}$. It will suffice to show that the intersection $\mathcal{J}$ of all the conjugates of $\mathcal{H}$ in $\mathcal{G}$ equals the trivial subgroup $\{e\}$.

We know by Lemma 4.2 that every $\tilde{\gamma} \in \mathcal{H}$ either fixes each of λ and $\overline{\lambda}$ or interchanges them. If all $\tilde{\gamma} \in \mathcal{J}$ fix λ, then since $\mathcal{J}$ is normal in $\mathcal{G}$ we will see that $\mathcal{J}$ fixes all of $\mathbb{Q}(\lambda)^{\mathrm{cl}}$, so $\mathcal{J} = \{e\}$ and we are done. We may thus suppose that there is an element $\tilde{\gamma} \in \mathcal{J}$ for which $\tilde{\gamma}(\lambda) = \overline{\lambda}$ and $\tilde{\gamma}(\overline{\lambda}) = \lambda$. Then $\tilde{\gamma}(\lambda + \lambda^{-1}) = \overline{\lambda} + \overline{\lambda}^{-1}$. Since $k = \mathbb{Q}(\lambda + \lambda^{-1})$, we conclude that $\gamma = q(\tilde{\gamma}) \in G$ satisfies $\gamma\sigma_1 = \sigma_2$, where σ_1 and σ_2 are as before the non-real complex conjugate embeddings of k into $\mathbb{C}$. Since $\ell > 2$, the description of the complex conjugations $\mathcal{C}$ in G given in Theorem 3.4 and Lemma 3.2 shows that there is a $j \notin \{1, 2\}$ such that $\tau\sigma_1 = \sigma_1$ and $\tau\sigma_2 = \sigma_j$ for some $\tau \in \mathcal{G}$. Then $\tau\gamma\tau^{-1}\sigma_1 = \sigma_j$.

Let $\tilde{\tau} \in \mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\lambda)^{\mathrm{cl}}/\mathbb{Q})$ be any element for which $q(\tilde{\tau}) = \tau$. By the definition of $\mathcal{J}$ as the intersection of all the conjugates of $\mathcal{H}$ in $\mathcal{G}$, we know that $\tilde{\gamma} \in \mathcal{H}$ and $\tilde{\tau}\tilde{\gamma}\tilde{\tau}^{-1} \in \mathcal{H}$. We have $(\tilde{\tau}\tilde{\gamma}\tilde{\tau}^{-1})(\lambda + 1/\lambda) = \sigma_j(\lambda + 1/\lambda)$. On the other hand, $\tilde{\tau}\tilde{\gamma}\tilde{\tau}^{-1} \in \mathcal{H}$ and Lemma 4.2 show $(\tilde{\tau}\tilde{\gamma}\tilde{\tau}^{-1})(\lambda + 1/\lambda) \in \{\lambda + 1/\lambda, \overline{\lambda} + 1/\overline{\lambda}\}$. This would give $\sigma_j(\lambda + 1/\lambda) = \sigma_i(\lambda + 1/\lambda)$ for some $i \in \{1, 2\}$, which is impossible since $k = \mathbb{Q}(\lambda + 1/\lambda)$ and $j \notin \{1, 2\}$. The contradiction completes the proof of Proposition 4.4. $\square$

5 Cebotarev Results

We will assume the notations of the previous two sections. Let $b : \Gamma \to \mathbb{Z}^+$ be a function on hyperbolic elements of Γ and let $l_b(\gamma) = (\lambda(\gamma)\overline{\lambda(\gamma)})^{b(\gamma)}$ for $\gamma \in \Gamma$.

5.1 The intersection of Galois closures

Lemma 5.1 *The intersection $\cap_{\gamma\in\Gamma}\mathbb{Q}(l_b(\gamma))^{\mathrm{cl}}$ is equal to k^{cl} unless k is a quadratic extension of a totally real field k^+, and in the latter case this intersection equals $(k^+)^{\mathrm{cl}}$. These two alternatives correspond to $\ell > 2$ and $\ell = 2$ in the notation of Theorem 3.4.*

Proof. Suppose first that $\ell > 2$. Then the maximal totally real subfield k^+ of k has $[k : k^+] > 2$ by Theorem 3.4(iii). On applying Lemma 2.3 to $\gamma^{b(\gamma)}$ we see that $\lambda(\gamma)^{b(\gamma)}$ is not real. Lemma 2.3 and Proposition 4.4 now show

$$\mathbb{Q}(\lambda(\gamma)^{b(\gamma)}) = k(\lambda(\gamma)) \quad \text{and} \quad \mathbb{Q}(l_b(\gamma))^{\mathrm{cl}} = \mathbb{Q}(\lambda(\gamma)^{b(\lambda)})^{\mathrm{cl}} \supset k^{\mathrm{cl}}. \tag{5.4}$$

Theorem 2.2(i) also shows that $\mathbb{Q}(\lambda(\gamma)^{b(\lambda)})$ is a quadratic extension of k, so $\mathbb{Q}(\lambda(\gamma)^{b(\lambda)})^{\mathrm{cl}}$ is an elementary abelian two-extension of k^{cl}. Hence to show that $\cap_{\gamma\in\Gamma}\mathbb{Q}(l_b(\gamma))^{\mathrm{cl}}$ is equal to k^{cl}, it will be enough to show that for each quadratic extension L of k^{cl} there is a hyperbolic element $\gamma \in \Gamma$ such that $\mathbb{Q}(\lambda(\gamma)^{b(\lambda)})^{\mathrm{cl}} \cap L = k^{\mathrm{cl}}$.

By the Cebotarev density Theorem, we can find a rational prime p which splits completely in k^{cl}, does not lie under a prime of k which ramifies in B, and for which some prime P over p in k^{cl} is inert to L. By the approximation theorem for absolute values of k, we can construct a quadratic extension F of k which is ramified at each place of k which ramifies in B, and such that each prime over p in k splits in F. By Theorem 2.2(ii) there is a hyperbolic element $\gamma \in \Gamma$ such that $k(\lambda(\gamma))$ is isomorphic to F. Then $\mathbb{Q}(\lambda(\gamma)^b) = k(\lambda(\gamma)^b) = k(\lambda(\gamma)) = F$ for all positive integers b by (5.4). Since p splits completely in F by construction, we conclude that p splits in $\mathbb{Q}(\lambda(\gamma)^{b(\lambda)})^{\mathrm{cl}} = (F)^{\mathrm{cl}}$. Since p does not split in the quadratic extension L of k^{cl}, this forces $\mathbb{Q}(\lambda(\gamma)^{b(\lambda)})^{\mathrm{cl}} \cap L = k^{\mathrm{cl}}$ as required.

Suppose now that $\ell = 2$. Then $[k : k^+] = 2$ by Theorem 3.4, and $\mathbb{Q}(l_b(\gamma)) \supset k^+$ by Lemma 4.3, so

$$(k^+)^{\mathrm{cl}} \subset \cap_{\gamma\in\Gamma}\mathbb{Q}(l_b(\gamma))^{\mathrm{cl}}. \tag{5.5}$$

Since $k^{\mathrm{cl}}/(k^+)^{\mathrm{cl}}$ is a two-extension, the right side of (5.5) is also a two-extension of $(k^+)^{\mathrm{cl}}$. Hence it will suffice to show for each quadratic extension L of $(k^+)^{\mathrm{cl}}$ it is possible to find a hyperbolic $\gamma \in \Gamma$ such that such that $\mathbb{Q}(l_b(\gamma))^{\mathrm{cl}} \cap L = (k^+)^{\mathrm{cl}}$. This can be done by a Cebotarev argument similar to the one for $\ell > 2$. $\square$

5.2 The case $\ell = 2$.

Throughout this section we will assume all the notation of the previous section and that $\ell = 2$. Thus k is a quadratic extension of a totally real field k^+.

Lemma 5.2 *There are infinitely many $\gamma \in \Gamma$ for which $\lambda = \lambda(\gamma)^{b(\gamma)}$ has the following properties.*

a. λ satisfies the conditions in option (b) of Lemma 4.3.

b. All embeddings of the field k^+ into $\mathbb{Q}(\lambda\overline{\lambda})$ over $\mathbb{Q}$ have the same image.

Proof. By the Cebotarev density theorem, we can find infinitely many primes p of $\mathbb{Q}$ which split completely in k and do not lie under any place of k ramified in B. Fix such a prime, and let q_1 and q_2 be primes of O_k over a prime q^+ of k^+ which lies over p. We can find a quadratic extension F/k which is ramified over each place of k which ramifies in B and such that q_1 is ramified in F, and q_2 splits in F. We then have $q_1O_F = \mathcal{Q}_1^2$ and $q_2O_F = \mathcal{Q}_2\mathcal{Q}_2'$ where $\mathcal{Q}_j$ is a prime ideal of F. By Theorem 2.2, there is an element $\gamma \in \Gamma$ such that $F = k(\lambda')$ where $\lambda' = \lambda(\gamma)$. By Theorem 2.2(i) we have $F = k(\lambda'^b)$ for all integers $b \geq 1$. Thus $F = k(\lambda)$ when $\lambda = (\lambda')^{b(\gamma)} = \lambda(\gamma)^{b(\gamma)}$. The extension F/k^+ cannot be Galois, since $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are primes of F over the same prime q^+ of k^+ which have different ramification degrees. If λ were real, then by Lemma 2.3, the extension $\mathbb{Q}(\lambda)$ would be quadratic over k^+, so $k(\lambda)$ would be Galois over k^+, which is not the case. Thus λ is not real, so either option (a) or option (b) of Lemma 4.3 holds. However, option (a) is impossible, since then $k(\lambda)$ would again again be Galois over k^+. So option (b) holds.

Note that by Lemma 4.3 there is an embedding $s_1 : k^+ \to \mathbb{Q}(\lambda\overline{\lambda})$. Suppose that there is another embedding $s_2 : k^+ \to \mathbb{Q}(\lambda\overline{\lambda})$ such that $s_1(k^+) \neq s_2(k^+)$. Regarding k^+ as a subfield of $\mathbb{Q}(\lambda\overline{\lambda})$ via s_1, the composite field $L = k^+s_2(k^+)$ is now a totally real non-trivial extension of k^+ inside $\mathbb{Q}(\lambda\overline{\lambda})$. By option (b) of Lemma 4.3, L must be the fixed field $\mathbb{Q}(\lambda, \overline{\lambda})^{\tilde{J}}$ of the order 4 subgroup $\tilde{J}$ generated by the conjugates of $J = \mathrm{Gal}(\mathbb{Q}(\lambda, \overline{\lambda})/\mathbb{Q}(\lambda\overline{\lambda}))$ in $\mathrm{Gal}(\mathbb{Q}(\lambda, \overline{\lambda})/k^+)$. Let $\mathcal{A}$ be a prime of

$\mathbb{Q}(\lambda,\overline{\lambda})$ lying over the prime $\mathcal{Q}_2$ of F. Recall that $\mathcal{Q}_2$ is unramified over k^+, since the prime q_2 of k under $\mathcal{Q}_2$ is split from k to F, and q_2 is unramified over the prime q^+ of k^+ which is unramified over $\mathbb{Q}$. However, since $\mathbb{Q}(\lambda,\overline{\lambda})$ is a Galois extension of k^+, $\mathcal{A}$ must be conjugate to a prime of $\mathbb{Q}(\lambda,\overline{\lambda})$ lying over the prime $\mathcal{Q}_1$, which is quadratically ramified over k. So it follows that $\mathcal{A}$ must be quadratically ramified over F, i.e. $\mathcal{A}^2 = \mathcal{Q}_2 O_{\mathbb{Q}(\lambda,\overline{\lambda})}$. By considering the ramification indices of primes lying below $\mathcal{A}$ in the tower of extensions $k^+ \subset F \subset \mathbb{Q}(\lambda,\overline{\lambda})$ it follows that the inertia group $I(\mathcal{A})$ of $\mathcal{A}$ in $H = \mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/k^+)$ equals $\mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/F) = \mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/\mathbb{Q}(\lambda))$. No conjugate of $I(\mathcal{A})$ lies in the group $\tilde{J}$, since $\tilde{J}$ is generated by the conjugates of J and J is a non-central group of order 2 in H which intersects $\mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/k)$ trivially. (Note that $\mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/k)$ is the Klein four subgroup generated by the conjugates of $I(\mathcal{A}) = \mathrm{Gal}(\mathbb{Q}(\lambda,\overline{\lambda})/\mathbb{Q}(\lambda))$.) Thus q^+ must ramify in the extension $L = k^+ s_2(k^+) = \mathbb{Q}(\lambda,\overline{\lambda})^{\tilde{J}}$ since no prime over q^+ in L can ramify in $\mathbb{Q}(\lambda,\overline{\lambda})$. However, we chose q^+ to be a prime over the rational prime p which splits completely in k^+. Thus p splits completely in $s_2(k^+)$ and thus also in L, which is impossible if q^+ ramifies from k^+ to L. The contradiction shows that there could not have been a second embedding $s_2 : k^+ \to \mathbb{Q}(\lambda\overline{\lambda})$ such that $s_2(k^+) \neq k^+$. □

6 Proof of Theorem 1.1

Clearly the commensurability class of M determines the rational length spectrum $\mathbb{Q}L(M)$. Hence Theorem 1.1 will follow immediately from the next result and Theorem 2.1.

Theorem 6.1 *Suppose that $M_1 = \mathbf{H}^3/\Gamma_1$ and $M_2 = \mathbf{H}^3/\Gamma_2$ are arithmetic hyperbolic 3-manifolds with the same rational length spectrum. Let k_i (resp. B_i) be the invariant trace field (resp. the invariant quaternion algebra) of M_i.*

a. There is an field isomorphism $\phi : k_1 \to k_2$.

b. The isomorphism ϕ in (a) can be extended to an isomorphism $B_1 \to B_2$.

To begin the proof of Theorem 6.1, note that by (2.1), we can replace Γ_i by $\Gamma_i^{(2)}$ so as to be able to assume that Γ_i is derived from B_i. Since M_1 and M_2 have the same rational length spectrum there are functions $b_i : \Gamma_i - \{e\} \to \mathbb{Z}^+$ for $i = 1, 2$ with the following property. Suppose $i = 1, 2$ and that $j = 3 - i$ is the other element of $\{1, 2\}$. Then for each $\gamma \in \Gamma_i - \{e\}$, the product $b_i(\gamma) \cdot \mathrm{l}(\gamma)$ lies in the set $\mathcal{L}(M_j)$ of lengths of closed geodesics of M_j, where $\mathrm{l}(\gamma)$ is the length of the closed geodesic on M_i associated to γ.

Define

$$\ell_{b_i}(\gamma) = \left(\lambda(\gamma)\overline{\lambda(\gamma)}\right)^{b_i(\gamma)} = e^{b_i(\gamma)\mathrm{l}(\gamma)}$$

where $\lambda(\gamma)$ is the eigenvalue of γ. Let $S(\Gamma_i, b_i) = \{\ell_{b_i}(\gamma) : \gamma \in \Gamma_i - \{e\}\}$. Since $b_i(\gamma)\mathrm{l}(\gamma) = \mathrm{l}(\gamma') \in \mathcal{L}(M_j)$ for some $\gamma' \in \Gamma_j - \{e\}$, we conclude that

$$S(\Gamma_i, b_i) \subset S(\Gamma_j, 1_j) \tag{6.6}$$

when $1_j : \Gamma_j - \{e\} \to \mathbb{Z}^+$ is the function which takes the value 1 on all elements of $\Gamma_j - \{e\}$.

6.1 Proof of Theorem 6.1(a)

By Lemma 5.1,

$$\cap\{\mathbb{Q}(\tau)^{\mathrm{cl}} : \tau \in S(\Gamma_i, b_i)\} = (k_i')^{\mathrm{cl}} \tag{6.7}$$

where $k_i' = k_i$ except when k_i is a quadratic extension of its maximal totally real subfield k_i^+, in which case $k_i' = k_i^+$. This result is independent of b_i. So by (6.6),

$$(k_1')^{\mathrm{cl}} = (k_2')^{\mathrm{cl}} \tag{6.8}$$

It was shown in Theorem 3.4 that the isomorphism class of k_i' can be determined from that of $(k_i')^{\mathrm{cl}}$. So (6.8) implies Theorem 6.1(a) if $k_i = k_i'$ for $i = 1, 2$. We thus reduce to the case in which $[k_i : k_i^+] = 2$ for at least one of $i = 1, 2$. Then (6.8) gives $[k_i : k_i^+] = 2$ and $\ell = 2$ for $i \in \{1, 2\}$.

By Lemma 5.1,

$$\cap\{\mathbb{Q}(\tau) : \tau \in S(\Gamma_i, b_i)\} = (k_i^+)^{\mathrm{cl}}.$$

The containments in (6.6) now show $(k_1)^{\mathrm{cl}} = (k_2)^{\mathrm{cl}}$. By Theorem 3.4, this forces k_1^+ and k_2^+ to be isomorphic.

In Lemma 5.2 we showed there is an element $\gamma \in \Gamma_1$ such that $\lambda = \lambda(\gamma)^{b_1(\gamma)}$ satisfies all the conditions in option (b) of Lemma 4.3 and for which all embeddings of the field k_1^+ into $\mathbb{Q}(\lambda\overline{\lambda})$ over $\mathbb{Q}$ have the same image, where $\lambda\overline{\lambda} = \ell_{b_1}(\gamma)$. Fixing one such embedding, the field $\mathbb{Q}(\ell_{b_1}(\gamma))$ is a non-Galois quartic extension of k_1^+, and the Galois closure F of $\mathbb{Q}(\ell_{b_1}(\gamma))$ over k_1^+ is a dihedral extension of k_1^+ of degree 8. Now Lemma 4.3 forces k_1 to be isomorphic to F^D where D is the unique Klein four subgroup of $\mathrm{Gal}(F/k_1^+)$ which does not contain $\mathrm{Gal}(F/\mathbb{Q}(\ell_{b_1}(\gamma)))$.

We now use the fact described above that $\ell_{b_1}(\gamma) = \ell_1(\gamma')$ for some $\gamma' \in \Gamma_2$ (see 6.6). Since we have shown $(k_1)^+$ is isomorphic to $(k_2)^+$, all embeddings of $(k_2)^+$ into $\mathbb{Q}(\ell_1(\gamma')) = \mathbb{Q}(\ell_{b_1}(\gamma))$ have the same image because of condition (b) of Lemma 5.1. This image is the same as that of $(k_1)^+$ under the embedding discussed above. Running the above arguments through now with Γ_2 replacing Γ_1, we conclude that $\ell_1(\gamma') = \ell_{b_1}(\gamma)$ implies k_2 is isomorphic to the field $F^D = k_1$.

6.2 Proof of Theorem 6.1(b)

We adopt the notations and assumptions of §6.1. By Theorem 6.1(a) we can assume that B_1 and B_2 are quaternion division algebras over the same number field k. Let R_i be the set of places of k which ramify in B_i.

Proposition 6.2 *There is an automorphism $c' : k \to k$ such that $c'(R_1) = R_2$.*

Before proving this Lemma, we note that it implies B_1 and B_2 are isomorphic as $\mathbb{Q}$-algebras by Theorem 2.2(iii), so this and Theorem 2.1 will show Theorem 6.1(b).

To begin the proof of Proposition 6.2, note that since the two non-real embeddings of k into $\mathbb{C}$ are taken to each other by complex conjugation, we can apply complex conjugation to the image of one of the embeddings $\rho_{B_i} : B_i \to \mathrm{Mat}_2(\mathbb{C})$ used to define Γ_i to be able to assume that the ρ_{B_i} define the same embedding $\rho : k \to \mathbb{C}$.

Lemma 6.3 *Suppose that $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$ are hyperbolic elements such that the lengths $\mathrm{l}(\gamma_1)$ and $\mathrm{l}(\gamma_2)$ are (non-zero) rational multiples of one another. Define $\lambda_i = \lambda(\gamma_i)$ to be the eigenvalue associated to γ_i, so that $|\lambda_i| > 1$. Then either $k(\lambda_1) = k(\lambda_2)$ or $k(\overline{\lambda_2}) = k(\lambda_1)$, and if $k(\lambda_1) \neq k(\lambda_2)$ then k is stable under complex conjugation.*

Proof. By Theorem 2.2(i), $k(\lambda_i^n) = k(\lambda_i)$ is quadratic over k for all integers $n \geq 1$. Since $\mathrm{l}(\gamma_i) = \ln|\lambda_i\overline{\lambda}_i|$ and $\mathrm{l}(\gamma_1)$ and $\mathrm{l}(\gamma_2)$ are non-zero rational multiples of one another, we can replace γ_1 and γ_2 by suitable positive powers of themselves so that the following is true. There is a real number $r > 0$ such that $\lambda_j = re^{i\theta_j}$ for some $\theta_j \in \mathbb{R}$ and $j = 1, 2$. The assumption that $k(\lambda_1) \neq k(\lambda_2)$ implies there is an automorphism $\eta \in \mathrm{Gal}(k(\lambda_1, \lambda_2)/k(\lambda_1))$ such that $\eta(\lambda_2) = 1/\lambda_2$.

Let F be the smallest Galois extension of $\mathbb{Q}$ containing k and all Galois conjugates of λ_1 and λ_2. Consider a lift τ to F of η. We have

$$\left|\frac{\tau(\overline{\lambda_2})}{\tau(\overline{\lambda_1})}\right| = |\lambda_1\lambda_2| \cdot \left|\frac{\lambda_2^{-1}\tau(\overline{\lambda_2})}{\lambda_1\tau(\overline{\lambda_1})}\right| = r^2\left|\frac{\tau(\lambda_2\overline{\lambda_2})}{\tau(\lambda_1\overline{\lambda_1})}\right| = r^2\left|\frac{\tau(r^2)}{\tau(r^2)}\right| = r^2.$$

By considering the Galois conjugates of the λ_j (see Theorem 2.2(iv)), this implies

$$|\tau(\overline{\lambda_2})| = r = 1/|\tau(\overline{\lambda_1})| \quad \text{and} \quad \tau(\overline{\lambda_1}) \in \{1/\lambda_1, 1/\overline{\lambda_1}\} \quad \text{and} \quad \tau(\overline{\lambda_2}) \in \{\lambda_2, \overline{\lambda_2}\}.$$

If $\tau(\overline{\lambda_1}) = 1/\lambda_1$ then $\tau(\lambda_1) = \lambda_1$ would imply $\overline{\lambda_1} = 1/\lambda_1$ which is impossible since λ_1 is not on the unit circle. Similarly, $\tau(\overline{\lambda_2}) \neq \lambda_2$ because $\tau(\lambda_2) = 1/\lambda_2$. Hence

$$\tau(\overline{\lambda_1}) = 1/\overline{\lambda_1} \quad \text{and} \quad \tau(\overline{\lambda_2}) = \overline{\lambda_2}.$$

Therefore

$$e^{-2i\theta_2} = \overline{\lambda_2}/\lambda_2 = \tau(\lambda_2\overline{\lambda_2}) = \tau(r^2) = \tau(\lambda_1\overline{\lambda_1}) = \lambda_1/\overline{\lambda_1} = e^{2i\theta_1}$$

so $\overline{\lambda_2}^2 = r^2e^{-2i\theta_2} = r^2e^{2i\theta_1} = \lambda_1^2$. Hence Theorem 2.2(i) shows the desired equality of fields $k(\overline{\lambda_2}) = k(\overline{\lambda_2}^2) = k(\lambda_1^2) = k(\lambda_1)$.

Suppose finally that $k(\lambda_1) \neq k(\lambda_2)$. Then $k(\lambda_1) = k(\overline{\lambda_2})$, $k(\overline{\lambda_1}) = k(\lambda_2)$ and neither λ_1 nor λ_2 can be real. By Lemma 2.3, $\mathbb{Q}(\lambda_i) = k(\lambda_i)$ is quadratic over $k = \mathbb{Q}(\lambda_i + 1/\lambda_i)$ for $i = 1, 2$. If $\overline{\lambda_2} + 1/\overline{\lambda_2} \in k = \mathbb{Q}(\lambda_2 + 1/\lambda_2)$ then k is stable under complex conjugation. Otherwise $\overline{\lambda_2} + 1/\overline{\lambda_2} \notin k$ so

$$\mathbb{Q}(\lambda_1) = k(\lambda_1) = k(\overline{\lambda_2}) = k(\overline{\lambda_2} + 1/\overline{\lambda_2}) = \mathbb{Q}(\lambda_2 + 1/\lambda_2, \overline{\lambda_2} + 1/\overline{\lambda_2})$$

is stable under complex conjugation. But then $k(\overline{\lambda_1}) = k(\lambda_2)$ and $k(\lambda_1) = \mathbb{Q}(\lambda_1)$ show

$$k(\lambda_2) = k(\overline{\lambda_1}) = \mathbb{Q}(\lambda_1, \overline{\lambda_1}) = \mathbb{Q}(\lambda_1) = k(\lambda_1)$$

contrary to hypothesis. This shows k must be stable under complex conjugation. □

Proof of Proposition 6.2.

We regard k, B_1 and B_2 as subalgebras of $\mathrm{Mat}_2(\mathbb{C})$ via our fixed embedding $\rho : k \to \mathbb{C}$ and fixed extensions of this embedding to B_1 and B_2. Since $\mathbf{H}^3/\Gamma_1$ and $\mathbf{H}^3/\Gamma_2$ are length commensurable, for each $\gamma_1 \in \Gamma_1 - \{e\}$ there is an element $\gamma_2 \in \Gamma_2 - \{e\}$ for which the conclusions of Lemma 6.3 hold, and the same is true if Γ_1 and Γ_2 are interchanged.

Suppose first that for all such pairs γ_1 and γ_2 one has $k(\lambda_1) = k(\lambda_2)$ in Lemma 6.3. In view of Theorem 2.2(ii), this implies that the quadratic field extensions of k which embed into B_1 are exactly those which embed into B_2. Therefore Theorem 2.2(iii) shows B_1 and B_2 are isomorphic over k, so we can let c' be the identity isomorphism in Proposition 6.2.

For the rest of the proof we assume that there is at least one pair γ_1 and γ_2 as above such that $k(\lambda_1) = k(\overline{\lambda_2}) \neq k(\lambda_2)$. We can also assume $R_1 \neq R_2$, since otherwise the proof can be completed as before, with c' the identity isomorphism. By Lemma 6.3, complex conjugation on $\mathbb{C}$ induces an order two automorphism $c' : k \to k$. If $c'(R_1) = R_2$, then c extends to a $\mathbb{Q}$-automorphism $c' : B_1 \to B_2$ by Theorem 2.2(iii), and Proposition 6.2 follows. We therefore assume that $c'(R_1) \neq R_2$.

By exchanging B_1 and B_2 if necessary, we may suppose that $|R_2| \geq |R_1|$. Since $c'(R_1) \neq R_2 \neq R_1$, we may choose places $\mathcal{P} \in R_2 - R_1$ and $\mathcal{Q} \in R_2 - c'(R_1)$. Note that then $c'(\mathcal{Q}) \notin R_1$.

By Theorem 2.2(ii), a quadratic extension L/k embeds into B_1 if and only if no place in R_1 splits in L/k. Since $\mathcal{P}$ and $c'(\mathcal{Q})$ do not lie in R_1, we may by Theorem 2.2(ii) choose a hyperbolic element $\delta \in \Gamma_1$ with eigenvalue $\lambda(\delta)$ so that $\mathcal{P}$ and $c'(\mathcal{Q})$ both split in $k(\lambda(\delta))$. Since $\mathbf{H}^3/\Gamma_1$ and $\mathbf{H}^3/\Gamma_2$ are length commensurable, Lemma 6.3 implies that there is a $\delta' \in \Gamma_2$ with eigenvalue $\lambda(\delta')$ such that

$k(\lambda(\delta')) = k(\lambda(\delta))$ or $k(\overline{\lambda(\delta')})$. If $k(\lambda(\delta')) = k(\lambda(\delta))$ then $\mathcal{P}$ splits in $k(\lambda(\delta'))$, which contradicts the fact that $k(\lambda(\delta'))$ embeds into B_2 over k and $\mathcal{P} \in R_2$ ramifies in B_2. Similarly, if $k(\lambda(\delta')) = k(\overline{\lambda(\delta)})$, then $\mathcal{Q}$ splits in $k(\lambda(\delta'))$ because $c'(\mathcal{Q})$ splits in $k(\lambda(\delta))$. This is also false since $\mathcal{Q} \in R_2$ ramifies in B_2 and $k(\lambda(\delta'))$ embeds into B_2. The contradiction completes the proof of Proposition 6.2. □

Acknowledgments. The first and second authors would like to thank the University of Texas at Austin for its hospitality during this work, and the last author wishes to thank the Centre Interfacultaire Bernoulli of EPF Lausanne, The University of Pennsylvania and the Institute for Advanced Study. We would also like to thank the referee for very helpful suggestions.

References

[1] A. Baker, *Transcendental Number Theory*, second edition, Cambridge Mathematical Library, Cambridge Univ. Press (1990).

[2] W. Bosma and B. de Smit, *On arithmetically equivalent number fields of small degree*, in Algorithmic number theory (Sydney, 2002), 67–79, Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, 2002.

[3] P. G. Doyle and J. P. Rossetti, *Tetra and Didi, the cosmic spectral twins*, Geom. and Topology **8** (2004), 1227–1242.

[4] R. Gangolli, *The length spectra of some compact manifolds*, J. Diff. Geom. **12** (1977), 403–424.

[5] I. M. Isaacs and T. Zieschang, *Generating symmetric groups*, Amer. Math. Monthly **102** (1995), no. 8, 734–739.

[6] J. Klüners, *Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe*, Shaker Verlag (2005).

[7] A. Lubotzky, B. Samuels and U. Vishne, *Division algebras and non-commensurable isospectral manifolds*, Duke Math. J. **135** (2006), 361–379.

[8] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Mathematics **219**, Springer-Verlag (2003).

[9] J. Milnor, *Eigenvalues of the Laplace operator on certain manifolds*, Proc. Nat. Acad. Sci. USA **51** (1964), 542.

[10] R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342–360.

[11] G. Prasad and A. S. Rapinchuk, *Weakly commensurable arithmetic groups, lengths of closed geodesics and isospectral locally symmetric spaces*, preprint (January 2007).

[12] A. W. Reid, *Isospectrality and commensurability of arithmetic hyperbolic* 2- *and* 3-*manifolds*, Duke Math. J. **65** (1992), 215–228.

[13] M. Salvai, *On the Laplace and complex length spectra of locally symmetric spaces of negative curvature*, Math. Nachr. **239/240** (2002), 198–203.

[14] T. Sunada, *Riemannian coverings and isospectral manifolds*, Annals of Math. **121** (1985), 169–186.

[15] M-F. Vignéras, *Variétiés Riemanniennes isospectrales et non isométriques*, Annals of Math. **112** (1980), 21–32.

Department of Mathematics,
University of Pennsylvania
Philadelphia, PA 19104

Department of Mathematics and Computer Science,
Emory University
Atlanta, GA 30322

Department of Mathematics,
University of California
Santa Barbara, CA 93106

Department of Mathematics,
University of Texas
Austin, TX 78712