Distribution Agreement

In presenting this thesis or dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis or dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis or dissertation. I retain all ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Signature:

Sean Thomas — Date

Complex iso-length-spectrality in arithmetic hyperbolic 3-manifolds

By

Sean Thomas
Doctor of Philosophy

Mathematics

Emily Hamilton
Advisor

Aaron Abrams
Committee Member

Eric Brussel
Committee Member

Accepted:

Lisa A Tedesco, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

Complex iso-length-spectrality in arithmetic hyperbolic 3-manifolds

By

Sean Thomas
B.A., Rollins College 2006

Advisor: Emily Hamilton, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2011

Abstract

Complex iso-length-spectrality in arithmetic hyperbolic 3-manifolds

By Sean Thomas

The (real-)length spectrum of a compact hyperbolic 3-manifold is the set of lengths of all closed geodesics along with the multiplicity of each length. A closed geodesic also has an imaginary part that represents the twist encountered by traveling once around the closed geodesic. So, the complex length of a closed geodesic is $\ell + it$, where ℓ is the length of the closed geodesic and t is the twist with $0 \leq t < 2\pi$. The complex length spectrum of a compact hyperbolic 3-manifold is the set of complex lengths of all closed geodesics along with the multiplicity of each length. Two compact hyperbolic 3-manifolds are called iso-length-spectral if their length spectra are the same. Also, two compact hyperbolic 3-manifolds are called complex iso-length-spectral if their complex length spectra are the same. The aim of this paper is to investigate if iso-length-spectral arithmetic hyperbolic 3-manifolds are complex iso-length-spectral. Arithmetic hyperbolic 3-manifolds are a class of hyperbolic 3-manifolds where arithmetic data about the manifolds tells us a great deal of information about the manifolds.

Complex iso-length-spectrality in arithmetic hyperbolic 3-manifolds

By

Sean Thomas
B.A., Rollins College 2006

Advisor: Emily Hamilton, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2011

Acknowledgements: First of all, I would like to thank my advisor Emily Hamilton for letting me be her student. Also, she taught my favorite graduate school class: algebraic topology. I knew on the very first day of class that it was the subject I wanted to specialize in, and I do not think I have ever completed a more enjoyable presentation of a very interesting subject. Next, I would like to thank my committee members Aaron Abrams and Eric Brussel for agreeing to be a part of the process by putting in time and effort into my dissertation. Also, I would like to thank my complex analysis professor, Shanshuang Yang, and algebra professor, Raman Parimala. Little did I know that those classes would cover important material with respect to my dissertation, and I was very fortunate to have them as professors. Furthermore, I would not be in this position if not for the professors at my undergraduate institution who introduced me to formal mathematics: Mark Anderson, Gloria Child, Richard Vitray, and Jay Yellen. Also, I would like to thank my parents Glenn and Barbara Thomas for giving me the opportunity to have this opportunity. Lastly, I would like to thank my wife, Mary Thomas, for her support and encouragement throughout the entire process.

Contents

1 Introduction

An interesting question concerning manifolds is, to what extent does an invariant associated with a manifold determine the manifold? A famous paper entitled *Can one hear the shape of a drum?* [9] tried to determine whether the sounds a drum could make uniquely determine the shape of the drum. The frequencies at which the drum vibrates are determined by the shape of the drum. If we know the set of frequencies and their multiplicities, then can we deduce the shape of the drum? It turns out that these frequencies are eigenvalues of the Laplacian operator, i.e., there exists an L^2 function, f, on our drum such that $\Delta f = \lambda f$ where Δ is the Laplacian operator and λ is the eigenvalue. The answer turned out to be 'no,' which was not shown until 1992 [7], but the drums would share certain characteristics such as equal surface area. Two such manifolds that share the same eigenvalues along with their multiplicities are called isospectral. Iso- means same and spectral comes from the fact that the λ are the spectra of the Laplacian. However, this problem had been asked before the 1966 paper. We can generalize this problem by replacing our drum with a Riemannian manifold. Examples of non-isometric, isospectral manifolds were constructed by Milnor in 1964 [15] and later by Vignéras in 1980 [26]. Later in 1985, Sunada formulated a method that gave rise to many examples of non-isometric, isospectral manifolds [21], which have equal volume.

We can ask a similar question about the geodesic length spectrum of a manifold. This is the set of all lengths of closed geodesics along with multiplicities. Two manifolds are called iso-length-spectral if they share the same length spectrum. These spectra are related by the following theorem [6]:

Theorem 1.1 *Two compact negatively curved Riemannian manifolds which are isospectral are iso-length-spectral.*

Although, in a more specific setting where the manifold is a hyperbolic 2-manifold, the relationship is stronger. The following result can be found in [14]:

Theorem 1.2 *Two compact hyperbolic 2-manifolds are isospectral if and only if they are iso-length-spectral.*

For a hyperbolic 3-manifold, closed geodesics have a real length along with a purely imaginary part representing the twist encountered after traveling once along the geodesic. If we define the complex length spectrum of a hyperbolic 3-manifold as the set of all complex lengths of closed geodesics along with multiplicities, then we have the following result [2] [6]:

Theorem 1.3 *Two compact hyperbolic 3-manifolds are isospectral if and only if they are complex iso-length-spectral.*

One might wonder whether iso-length-spectral hyperbolic 3-manifolds are isospectral. If one could show that iso-length-spectral manifolds are complex iso-length-spectral, then the question would be settled. Many non-isometric, isospectral manifolds that have been constructed are commensurable. Two manifolds are commensurable if they share a finite-sheeted covering space. Whether all isospectral hyperbolic 2-manifolds and hyperbolic 3-manifolds are commensurable is still an open problem. However, it is known that iso-length-spectral arithmetic hyperbolic 2-manifolds and arithmetic hyperbolic 3-manifolds are commensurable [20] [4]. Furthermore, a more general result was proven for arithmetic hyperbolic 3-manifolds: two arithmetic hyperbolic 3-manifolds are commensurable if and only if they have equal rational length sets [4], where the rational length set is the set of all rational multiples of lengths of closed geodesics without multiplicity. In this paper, we restrict our viewpoint to arithmetic hyperbolic 3-manifolds, which are a particularly tractable class of hyperbolic 3-manifolds. Our aim is to investigate the following question:

Question 1.4 *Let M_1 and M_2 be iso-length-spectral arithmetic hyperbolic 3-manifolds. Are M_1 and M_2 complex iso-length-spectral?*

It should be noted that the multiplicities of the lengths do matter. In [13], it was proven that there exist hyperbolic 3-manifolds with equal complex length sets but different volumes. Complex iso-length-spectral hyperbolic manifolds have equal volumes. So, the manifolds have equal complex length sets but unequal complex length spectra, which necessary implies the multiplicities do not match. Furthermore, these manifolds can be chosen to be arithmetic.

To give an idea of what to expect, the following correspondence exists in hyperbolic 3-manifolds. Let γ be a closed geodesic in a hyperbolic 3-manifold. Then, the geodesic corresponds to a matrix in $PSL_2(\mathbb{C})$. Furthermore, after an appropriate conjugation we can make the matrix have the form as below.

$$\gamma \longleftrightarrow \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$$

The complex length of the closed geodesic can be calculated from the correspondence above. Let $\lambda = re^{i\theta}$, then

$$\ell(\gamma) = 2ln|\lambda| + 2i\theta$$

where $2ln|\lambda|$ is the (real) length of the closed geodesic and 2θ is the twist encountered by traveling once around the geodesic. In our approach, we forget the purely imaginary part of the complex length, and determine how much the real length determines the purely imaginary part. Or, equivalently, for a fixed value of r such that $\lambda = re^{i\theta}$ is an eigenvalue of a matrix corresponding to a closed geodesic, how many other values on the unit circle, $e^{i\phi}$, make $re^{i\phi}$ an eigenvalue of a matrix corresponding to a closed geodesic? If we could show that there is only one $e^{i\phi}$ that may be paired with a given r, then the problem would be solved for arithmetic hyperbolic 3-manifolds. Although this is not the case, in Section 6.1 we will show that there are only finitely many angles that may be paired with a given r arising from an arithmetic hyperbolic 3-manifold, which is formally stated in the following theorem.

Theorem 1.5 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in a Kleinian group derived from a quaternion algebra A/k. Then, there are only finitely many $e^{i\theta}$ such that $re^{i\theta}$ is a loxodromic eigenvalue from some Kleinian group derived from some quaternion algebra.*

This will be our first result. While this result is promising, it would be nice to pin down exactly how many angles may be paired with a norm of a loxodromic eigenvalue to yield other loxodromic eigenvalues and, also, characterize when multiple angles occur. In Section 6.2, we will look at a "small," tractable case that will be our jumping-off point. Then, we will conjecture about what is required for multiple angles to occur. Following this up, in Section 6.3, we formalize the role of roots of unity, as is seen in the following theorem.

Theorem 1.6 *Let $r = |\lambda|$ be the norm of loxodromic eigenvalues from elements γ_1 and γ_2 in Kleinian groups Γ_1 and Γ_2 derived from a quaternion algebra A/k. If $\lambda_1 = re^{i\theta_1}$, $\lambda_2 = re^{i\theta_2}$, and $\lambda_1 \neq \pm\bar{\lambda}_2$, then λ_1/λ_2 is a root of unity.*

Then, in Section 6.4, we will return to the tractable case to fully characterize what was going on with multiple angles, and, also, we will be able to generalize this to something less restrictive than our "toy" case. Due to restrictions imposed by the fact that $[k : \mathbb{Q}] = 3$, the following degrees for r^2 are the only ones possible.

Theorem 1.7 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in an arithmetic Kleinian group derived from a quaternion algebra A/k over a number field k with $[k : \mathbb{Q}] = 3$. Suppose that the discriminant of the trace field is $-d$, where*

$d > 0$ is a square-free integer. Then, the only possibilities for the degree of r^2 are 3, 6, and 12.

i) If $[\mathbb{Q}(r^2) : \mathbb{Q}] = 12$, then the angle of a loxodromic eigenvalue with norm r is unique.

ii) Suppose $[\mathbb{Q}(r^2) : \mathbb{Q}] = 3$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $d \neq 1, 3$.

iii) Suppose $[\mathbb{Q}(r^2) : \mathbb{Q}] = 6$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $\mathbb{Q}(r^2)$ does not contain $\sqrt{d}$ (if $d \neq 1$) or $\sqrt{3d}$.

While the objects described above have not been formally introduced, the gist is that certain Kleinian groups arise from a quaternion algebra over a number field. If we restrict ourselves to number fields of degree 3, then we have great leverage over the situation and we can characterize exactly when the angle with a loxodromic norm r is unique. More generally, if the degree is a prime $p \neq 2$, then the following theorem holds. The notation N_k refers to the Galois (or, equivalently, normal) closure of a number field k and the notation N_α refers the Galois (or, equivalently, normal) closure of $\mathbb{Q}(\alpha)$, i.e., the minimal degree number field that contains all Galois conjugates of α. Another way to word the latter is that it is a splitting field for the minimal polynomial of α.

Theorem 1.8 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in a Kleinian group derived from a quaternion algebra A/k with $[k : \mathbb{Q}] = p$ where p is a prime not equal to 2. Then, there is a unique quadratic extension contained in the Galois closure of the trace field. If the quadratic extension is $\mathbb{Q}(\sqrt{-d})$, where $d > 0$ is a square-free integer.*

i) If the Galois group of N_{r^2} is not isomorphic to S_p or $S_p \times \mathbb{Z}_2$, then the angle is unique.

ii) If the Galois group of N_{r^2} is isomorphic to S_p. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $d \neq 1, 3$.

iii) If the Galois group of N_{r^2} is isomorphic to $S_p \times \mathbb{Z}_2$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if the Galois closure of r^2 does not contain $\sqrt{d}$ (if $d \neq 1$) or $\sqrt{3d}$.

After discovering the "culprit", in Section 6.5, we leverage our knowledge of the situation to produce infinitely many cases when we have a positive result:

Theorem 1.9 *There exist infinitely many commensurability classes of arithmetic Kleinian groups such that if Γ_1 and Γ_2 are derived and iso-length-spectral, then Γ_1 and Γ_2 are complex iso-length-spectral.*

Theorem 1.10 *Consider a commensurability class of arithmetic Kleinian groups with invariant quaternion algebra A/k where $[k : \mathbb{Q}] = 3$, $k(\sqrt{-1}) \not\hookrightarrow A$, and $k(\sqrt{-3}) \not\hookrightarrow A$. Then, if Γ_1 and Γ_2 are derived and iso-length-spectral, then Γ_1 and Γ_2 are complex iso-length-spectral.*

Then, a natural question is: over all loxodromic eigenvalues, is the number of angles that may be paired with a loxodromic norm unbounded? The answer to this is yes. This is summarized in the following theorem:

Theorem 1.11 *For every $n \geq 2$, there exists a loxodromic norm, r, such that exactly n numbers on the unit circle make $re^{i\theta}$ a loxodromic eigenvalue.*

That is, the angle of a loxodromic eigenvalue can be highly non-unique. Then, in the pursuit of our goal, we prove that a certain number theoretic conjecture is equivalent to a conjecture about a certain class of arithmetic hyperbolic 3-orbifolds. While this is not entirely our doing (see Chapter 12 [16]), we have expanded the equivalence to a certain class of arithmetic hyperbolic 3-orbifolds. While equivalences like these do not directly help solve either conjecture, there are now two settings, algebraic number theory and arithmetic hyperbolic 3-manifolds, to try to solve such problems.

Theorem 1.12 *The Salem conjecture is equivalent to the Short Geodesic conjecture for arithmetic hyperbolic 3-orbifolds with invariant trace field $k = \bar{k}$.*

The Salem conjecture says that certain roots of integral polynomials are uniformly bounded below by a number strictly greater than 1. The Short Geodesic conjecture says that the length of closed geodesics are uniformly bounded below. Both conjectures will be explicitly mentioned in Section 6.6. Finally, in Section 7, we have compiled results that were proven along the way that do not quite line up with the main thrust of the paper. However, they answer some interesting questions and they are included as well.

Now that the results of the paper have been enumerated, we need to outline what background material is necessary to prove these results. In sections 2.1, 2.2, 3, and 4.1, we will introduce the necessary background material from hyperbolic 3-space, hyperbolic 3-manifolds, algebraic number theory, and arithmetic hyperbolic 3-manifolds. After that, in Section 5, we will review some pertinent results that set the stage for our investigation.

2 Geometric Preliminaries

2.1 Hyperbolic 3-Space

Euclid's Fifth Postulate states that given any line, L, and any point, p, not on that line, there is exactly one line, L' such that p lies on L', and L and L' do not intersect. In an attempt to show that the first four postulates implied the fifth postulate, the fifth postulate was proved to be independent of the first four postulates. Changing the fifth postulate to allow infinitely many lines that contain p and do not intersect L yields a consistent geometry. Hyperbolic space is an example of such a space, which is defined below. The following material comes from Chapter 1 of [16].

Definition 2.1 **Upper half space** *is the following subset of 3-dimensional Euclidean space:* $\mathbb{H}^3 = \{(x, y, z) \in \mathbb{R}^3 : z > 0\}$.

Once we choose the appropriate metric, upper half space will serve as a model for hyperbolic 3-space. We use the line element $ds^2 = \frac{dx^2+dy^2+dt^2}{t^2}$. This induces a metric on $\mathbb{H}^3$, which is complete in the sense that every Cauchy sequence converges. The geodesics in $\mathbb{H}^3$ are Euclidean lines perpendicular to the x, y-plane and semi-circles that are orthogonal to the x, y-plane. The volume of regions in $\mathbb{H}^3$ is computed using the volume element $dV = \frac{dxdydt}{t^3}$. The orientation-preserving isometries of $\mathbb{H}^3$ are Möbius transformations. These act on the x, y-plane plus a point at infinity, denoted $\partial\mathbb{H}^3$, and induce a unique map on $\mathbb{H}^3$. As a group, the set of Möbius transformations, $\{z \mapsto \frac{az+b}{cz+d} \mid ad - bc = 1\}$ with $a, b, c, d \in \mathbb{C}$, is isomorphic to $PSL_2(\mathbb{C})$, which is defined below.

Definition 2.2 *The group* $PSL_2(\mathbb{C})$ *is the quotient group of* $SL_2(\mathbb{C})$ *and the subgroup* $\{\pm I\}$ *where* I *is the* 2×2 *identity matrix and* $SL_2(\mathbb{C})$ *is the set of* 2×2 *matrices with complex entries and determinant equal to* 1.

The isomorphism between these two groups is given by the following correspondence:

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \longleftrightarrow z \mapsto \frac{az+b}{cz+d}$$

where $\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]$ represents the coset containing $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. While isometries of hyperbolic 3-space should be denoted by an element of $PSL_2(\mathbb{C})$, we denote such an element by representative in $SL_2(\mathbb{C})$ from the coset it represents. For us specifically, this will mean that $\begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$ and $\begin{pmatrix} -\lambda & 0 \\ 0 & -1/\lambda \end{pmatrix}$ correspond to the same element of $PSL_2(\mathbb{C})$. Looking at the correspondence with Möbius transformations above, both matrices correspond to $z \mapsto \lambda^2 z$ because the minus signs cancel out. So, these eigenvalues, while unequal, are equivalent because they correspond to the same isometry of hyperbolic 3-space.

Elements of $PSL_2(\mathbb{C})$ are characterized by their trace. That is, the geometry of the isometry is determined by the value of the trace. Since the trace of a matrix is invariant under conjugation, we may conjugate each type of element to a normal form, i.e., Jordan canonical form. An element, γ, falls into one of four categories. Elliptic elements have $tr(\gamma) \in \mathbb{R}$ and $|tr(\gamma)| < 2$. These elements can be conjugated to

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix},$$

which is a rotation about the $z-$axis. Parabolic elements have $tr(\gamma) = 2$. These elements can be conjugated to

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which is a horizontal translation. Hyperbolic elements have $tr(\gamma) \in \mathbb{R}$ and $|tr(\gamma)| > 2$. Loxodromic elements have $tr(\gamma) \in \mathbb{C} \backslash \mathbb{R}$. Both hyperbolic and loxodromic elements can be conjugated to

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix},$$

which is a dilation that sends the $z-$axis to itself by a factor that depends on the eigenvalue of the corresponding element in $PSL_2(\mathbb{C})$. If the element is loxodromic, there is a screw motion that goes along with the dilation. Also, an element of the above form is hyperbolic if and only if $\lambda \in \mathbb{R}$ and loxodromic if and only if $\lambda \in \mathbb{C} \backslash \mathbb{R}$.

Note that isometries of hyperbolic 3-space map $\mathbb{H}^3 \cup \partial \mathbb{H}^3$ to itself. By the Brouwer fixed point theorem, hyperbolic isometries must fix at least one point in $\mathbb{H}^3 \cup \partial \mathbb{H}^3$. Furthermore, we can determine the fixed points of an element by the conjugated form of each trace type. A parabolic element in normal form has one fixed point at infinity. An elliptic element in normal form fixes the $z-$axis. A hyperbolic element in normal form has two fixed points at 0 and ∞. Lastly, a loxodromic element in normal form also has two fixed points at 0 and ∞. Thus respectively, isometries that are not necessarily in normal form correspond to fixing a line in hyperbolic space with endpoints on the sphere at infinity, fixing one point on the sphere at infinity, and fixing two points on the sphere at infinity. We will frequently refer to a group of isometries that defines our manifold. In order to do that, we require the following definitions.

Definition 2.3 *A subgroup, Γ, of $PSL_2(\mathbb{C})$ is* **discrete** *if the induced topology on Γ as a subspace of $PSL_2(\mathbb{C})$ is the discrete topology.*

Proposition 2.4 *A subgroup, Γ, is discrete if and only if $\gamma_n \to Id$, where $\gamma_n \in \Gamma$ implies $\gamma_n = Id$ for sufficiently large values of n.*

Definition 2.5 *A* **Kleinian group** *is a discrete subgroup of $PSL_2(\mathbb{C})$.*

A Kleinian group, Γ, acts properly discontinuously on $\mathbb{H}^3$. That is, for any $\gamma \in \Gamma$ and and compact subset $K \subset \mathbb{H}^3$, the cardinality of the set $\gamma K \cap K$ is finite. Then, we may make the following definition of a fundamental domain.

Definition 2.6 *A* **fundamental domain** *for a Kleinian group Γ is a closed set $F \subset \mathbb{H}^3$ such that $\bigcup_{\gamma\in\Gamma} \gamma F = \mathbb{H}^3$, $int(\gamma F) \cap int(F) = \varnothing$, and the boundary of F has measure zero, where int denotes the interior of a set.*

Remark 2.7 *As a side note: after an appropriate conjugation, an elliptic element in a Kleinian group must have eigenvalues that are roots of unity. If they were not roots of unity, then the group would not be discrete. This is easily seen by taking successive powers of the element, noting that any power of such element will have eigenvalues of norm 1, and the fact that the set $\{e^{ni\theta} \mid n \in \mathbb{Z}\}$ is dense in the unit circle precisely when $e^{i\theta}$ is not a root of unity. In that case, we could produce a sequence of elements that converged to the identity element and yet there would be infinitely many elements in the sequence which were not the identity. This would violate an equivalent condition for discreteness in Proposition 2.4. However, this does not prohibit loxodromic elements from having an eigenvalue of $re^{i\theta}$ where $e^{i\theta}$ is not a root of unity. The same argument does not apply since $|r| \neq 1$.*

2.2 Hyperbolic 3-Manifolds

First, we give an informal review of covering spaces and their correspondence with subgroups of the fundamental group of the space. A covering space is a topological space along with a continuous map that surjects onto the “covered” space. Every point in the covered space has a neighborhood whose inverse image under the covering map consists of disjoint open sets that map homeomorphically onto the specified neighborhood. An elementary result is that the fundamental group of the covering space injects into the fundamental group of the covered space by the group homomorphism induced by the covering map. Thus, the fundamental group of the covering space is isomorphic to a subgroup of the covered space. Furthermore, the index of the injected subgroup is the cardinality of the inverse image of a point in the covered space. If the cardinality is finite, then we call the covering space finite-sheeted. The classification of covering spaces theorem states that after fixing a base-point in the covered space, conjugacy classes of subgroups of the fundamental group are in direct correspondence with covering spaces up to isometry. Simply put, we may use conjugacy classes of subgroups of the fundamental group and covering spaces interchangeably. Specifically, we will be concerned about covering spaces that are finite-sheeted. Shortly, we will use this terminology to develop an equivalence relation between two covering spaces (or subgroups). The following material comes from Chapter 1 of [16].

A hyperbolic 3-manifold is a manifold which locally looks like hyperbolic 3-space, i.e., the manifold is equipped with a Riemannian metric such that every point has a neighborhood that is isometric to a ball in $\mathbb{H}^3$. If Γ is a torsion-free Kleinian group, then Γ acts freely and properly discontinuously on $\mathbb{H}^3$. So, the quotient $\mathbb{H}^3/\Gamma$ is an orientable hyperbolic 3-manifold. For the converse, we have a theorem below, but, first we require a few definitions.

Definition 2.8 *Let g be an element of a group G. Then, g is a* **torsion element** *if g has finite order in G.*

Definition 2.9 *A group G is said to be* **torsion-free** *if the only torsion element in G is the identity element.*

Theorem 2.10 *Let M be a hyperbolic 3-manifold. Then, M is isometric to $\mathbb{H}^3/\Gamma$ where Γ is a torsion-free Kleinian group.*

Sometimes, our Kleinian group may not be torsion-free, i.e., it contains an elliptic element, and Remark 2.7 shows that the eigenvalues are roots of unity. Therefore, a Kleinian group is torsion-free if and only if it contains no elliptic elements. In the case a Kleinian group is not torsion-free, we have the following definition.

Definition 2.11 *A* **hyperbolic 3-orbifold** *is a quotient of $\mathbb{H}^3$ by a Kleinian group Γ. Note that an orbifold is more general than a manifold because Γ may not be torsion-free. Torsion elements have fixed points in hyperbolic 3-space.*

Hyperbolic orbifolds are closely related to hyperbolic manifolds by the following result of Selberg.

Theorem 2.12 *(***Selberg, 1960***) Any finitely generated subgroup of $SL_2(\mathbb{C})$ has a torsion-free subgroup of finite index.*

Corollary 2.13 *Every hyperbolic 3-orbifold of finite volume is finitely covered by a hyperbolic 3-manifold.*

We may use Kleinian group and hyperbolic 3-orbifold interchangeably, and we may pass to a finite-sheeted covering space that is a hyperbolic 3-manifold. Group terminology will generally be used in favor of manifold terminology. This is convenient because we will see that properties of the manifold are reflected in characteristics of elements of the Kleinian group, which are quite tangible as elements of $PSL_2(\mathbb{C})$.

A natural way to separate manifolds is via commensurability classes, which are determined by finite-sheeted covering spaces. Throughout much of this paper, we will investigate commensurability class invariants of arithmetic hyperbolic 3-manifolds.

Definition 2.14 *Two manifolds are* **commensurable** *if they share a common finite-sheeted covering space. Two Kleinian groups,* Γ_1 *and* Γ_2*, are* **commensurable** *if* $[\Gamma_1 : \Gamma_1 \cap \Gamma_2]$ *and* $[\Gamma_2 : \Gamma_1 \cap \Gamma_2]$ *are finite. More generally, two Kleinian groups are* **commensurable in the wide sense** *if some conjugate of one of them is commensurable with the other.*

Something very special about hyperbolic 3-manifolds (and more generally for any dimension greater than or equal to 3) is that they are rigid. This is summed up in the following theorem known as Mostow-Prasad Rigidity.

Theorem 2.15 *Let* Γ_1 *and* Γ_2 *be finite covolume Kleinian groups and let* $\phi : \Gamma_1 \to \Gamma_2$ *be a group isomorphism. Then there exists an isometry of* $\mathbb{H}^3$*,* g*, such that for any* $\gamma_1 \in \Gamma_1$

$$\phi(\gamma_1) = g\gamma_1 g^{-1}$$

This is a very strong result. It says that isomorphic Kleinian groups are actually conjugate, which is certainly not true for all groups. An equivalent statement given in [16] is that if a compact orientable 3-manifolds has a hyperbolic structure, then that structure is unique. This leads to the result that the volume of a hyperbolic manifold is actually a topological invariant, which reinforces the idea that hyperbolic 3-manifolds are quite rigid.

Although there are orbifolds that are not manifolds, Selberg's Lemma gives us that every orbifold is covered by a hyperbolic 3-manifold. Also, commensurability gives us a way of relating two hyperbolic manifolds. If two hyperbolic 3-manifolds, or two Kleinian groups, are commensurable then we will see that they have isomorphic invariant quaternion algebras and equal invariant trace fields. At this point, we mention that commensurability is an equivalence relation (which we have been assuming for a little while). Later, we will isolate certain types of commensurability classes that contain certain kinds of nice hyperbolic 3-manifolds. These will be arithmetic hyperbolic 3-manifolds. Much can be said about this subclass of hyperbolic 3-manifolds.

We have mentioned what happens when our Kleinian group contains elliptic elements. Below is a theorem that summarizes parabolic elements' effect on the geometry of the manifold. But first, note that any familiar term with the prefix co- means that the fundamental domain has the property that follows the prefix. So, covolume refers to the volume of the fundamental domain, F, which equals $\int_F dV$ where dV is the hyperbolic volume element.

Theorem 2.16 *Let Γ be a finite covolume Kleinian group. Then Γ is cocompact if and only if Γ contains no parabolic elements.*

Lastly, what effect do loxodromic elements have on the hyperbolic 3-manifold? They correspond to closed geodesics. Let γ be a loxodromic or hyperbolic element of $PSL_2(\mathbb{C})$. As mentioned earlier, these elements have precisely two fixed points, $z, w \in \mathbb{C}^\infty$. The geodesic between z and w is called the axis of γ. The translation length of γ is defined as $\ell(\gamma) = inf_{z\in\mathbb{H}^3}\{d(z, \gamma(z))\}$. This quantity is invariant under conjugation by an isometry. Thus, we may conjugate γ to look like $\begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$. The closed geodesic that arises from this isometry comes from the identification of two points on the axis of γ, and, furthermore, $\ell(\gamma) = 2 \cdot ln|\lambda|$.

Definition 2.17 *The* **length** *of a loxodromic element, γ, (conjugated as above) is $2ln|\lambda|$.*

Definition 2.18 *The* **complex length** *of a loxodromic element, γ, (conjugated as above) is $2ln|\lambda| + 2i\theta$ where $0 \leq \theta < 2\pi$.*

Recall in Section 1, we defined the length spectrum and the complex length spectrum. Now, we will restate those definitions.

Definition 2.19 *Let M be a compact hyperbolic 3-manifold. The* **length spectrum** *of M is the collection of all real lengths of closed geodesics in M counted with their multiplicities.*

Definition 2.20 *Let M be a compact hyperbolic 3-manifold. The* **complex length spectrum** *of M is the collection of all complex lengths of closed geodesics in M counted with their multiplicities.*

Definition 2.21 *Two compact hyperbolic 3-manifolds are* **iso-length-spectral** *if their length spectra are identical.*

Definition 2.22 *Two compact hyperbolic 3-manifolds are* **complex iso-length-spectral** *if their complex length spectra are identical.*

Now, assume we have an hyperbolic 3-orbifold, $\mathbb{H}^3/\Gamma$, instead of a hyperbolic 3-manifold. The length spectrum of Γ is defined identically, and we define the complex length spectrum of Γ by changing it to a statement about the number conjugacy classes of loxodromic elements of a given length.

Definition 2.23 *Let Γ be a non-elementary Kleinian group. The* **multiplicity** *of a complex length, $\ell + i\theta$, is the number of conjugacy classes of loxodromic elements in Γ that share the same length.*

Definition 2.24 *Let Γ be a non-elementary Kleinian group. The* **complex length spectrum** *of Γ is the collection of complex lengths of loxodromic elements counted with their multiplicities.*

Many theorems in Section 1 suppose we have a Kleinian group. The important part to note is a Kleinian group, Γ, determines an orbifold, $\mathbb{H}^3/\Gamma$. Thus, our results refer to orbifolds.

While we will later highlight the benefits of investigating arithmetic hyperbolic

3-manifolds, some number theoretic results still hold for hyperbolic manifolds that are not arithmetic. In order to prepare for this, we will now delve into the necessary algebraic background.

3 Algebraic Preliminaries

Algebraic number theory generalizes the concept of integer to arbitrary finite degree extensions of the rational numbers. The inspiration for the definition of an algebraic integer comes from the fact that the integral closure of the integers in the rational numbers is precisely the integers, i.e., if a monic polynomial with integral coefficients has a rational root, then the root is an integer. Another generalized concept is a prime number. Since ideals are not necessarily principal, a prime in a number field, or more specifically in the ring of algebraic integers, refers to a prime ideal. While these concepts seem far from the realm of hyperbolic manifolds, we will see that the relative tangibility of algebraic integers enables us to produce examples of eigenvalues of loxodromic elements (along with help from the number theoretic software PARI), and studying prime ideals in number fields will allow us to construct some particularly nice quaternion algebras. These quaternion algebras can be used to construct commensurability classes of arithmetic hyperbolic 3-manifolds.

3.1 Dedekind Domains

In order to extend the concept of an integer, some provisions must be made. It is a well known fact that the unique factorization of the integers does not necessarily hold in finite degree extensions of the rational numbers. This is due specifically to the fact that the concepts of prime and irreducible are equivalent under certain circumstances, but they are not equivalent in general. Fortunately, Dedekind domains provide a different kind of unique factorization if we are willing to replace the idea of a prime number with that of a prime ideal.

We assume the reader knows the definitions of the most basic terms: ring, subring, and ideal. But, we will take some time to review the following terms in order to stress completeness. Also, we assume that our rings are commutative and contain a multiplicative identity denoted as 1. The following material comes from the references [5] and [21].

Definition 3.1 *An ideal P is* **prime** *if P is properly contained in R and if whenever the product $ab \in R$, then $a \in P$ or $b \in P$. Also, an element p of a ring R is called prime if the ideal generated by p is a prime ideal.*

Later we will construct invariants (quaternion algebras and number fields) of arithmetic hyperbolic 3-manifolds. Some classic results in algebraic number theory provide a recipe for a quaternion algebra. We need a number field and a set of prime ideals. (There are more specifications, but we will not elaborate yet.) Given a certain kind of quaternion algebra we will be able to construct an arithmetic hyperbolic 3-manifold. So, while these concepts may be from an introductory algebra class, they form the basis of material to be used later.

Definition 3.2 *An element u of a ring R is called a* **unit** *if there exists a v in R such that $uv = 1$.*

Lengths of closed geodesics in arithmetic hyperbolic 3-manifolds are of the form $2ln|\lambda|$ where λ is a specific type of unit.

Definition 3.3 *Let r be an element of a ring R that is non-zero and not a unit. Then, r is* **irreducible** *if whenever $r = ab$, then a or b is a unit in R.*

Definition 3.4 *An integral domain R is a* **unique factorization domain** *if every element of R that is non-zero and not a unit has a decomposition into irreducible elements that is unique up to multiplication by units.*

Definition 3.5 *An ideal M is* **maximal** *if the only ideals containing M are M and R.*

Definition 3.6 *An* **integral domain***, R, is a ring such that if $ab = 0$, then $a = 0$ or $b = 0$.*

Definition 3.7 *Let $R \subset S$ be a containment of rings. The* **integral closure** *of R is the set of all elements of S that satisfy a monic polynomial with coefficients in*

Definition 3.8 *Let $R \subset S$ be a containment of rings. A ring R is* **integrally closed** *if R is equal to the integral closure of R in S.*

If we wanted full generality, one usually defines an object called a module, then proceeds to define a Noetherian module. The generality is eventually removed when we observe that a ring is an R-module. As these definitions seem superfluous, we will tailor our definitions to our situation.

Definition 3.9 *A* **chain** *of sets is a sequence of subsets, $S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq \ldots$ A chain is said to stabilize if there are only finitely many distinct sets in the chain, i.e., there exists an N such that if $m, n \geq N$, then $S_m = S_n$.*

Definition 3.10 *A ring R is called* **Noetherian** *if every chain of subrings stabilizes.*

Definition 3.11 *An integral domain R is a* **Dedekind domain** *if it is Noetherian, integrally closed, and every non-zero prime ideal is maximal.*

Theorem 3.12 *Let R be a Dedekind domain, P be the set of non-zero prime ideals of R, and $\mathcal{I}$ be an ideal in R. Then, $\mathcal{I}$ can be uniquely expressed as follows:*

$$\mathcal{I} = \prod_{\wp \in P} \wp^{n_\wp(\mathcal{I})}$$

where $n_\wp(\mathcal{I}) \in \mathbb{Z}$ and $n_\wp(\mathcal{I}) = 0$ for all but finitely many prime ideals.

Here are some properties of the function $n_\wp$, which are valid for any ideals $\mathcal{I}, \mathcal{J}$ and any prime ideal $\wp$:

$$n_\wp(\mathcal{I}\mathcal{J}) = n_\wp(\mathcal{I}) + n_\wp(\mathcal{J})$$

$$\mathcal{I} \subset R \Leftrightarrow n_{\wp}(\mathcal{I}) \geq 0$$

$$\mathcal{I} \subset \mathcal{J} \Leftrightarrow n_{\wp}(\mathcal{I}) \geq n_{\wp}(\mathcal{J})$$

$$n_{\wp}(\mathcal{I} + \mathcal{J}) = min(n_{\wp}(\mathcal{I}), n_{\wp}(\mathcal{J}))$$

$$n_{\wp}(\mathcal{I} \cap \mathcal{J}) = max(n_{\wp}(\mathcal{I}), n_{\wp}(\mathcal{J}))$$

We have completed the set up for generalizing the concept of an integer. Now, we need to flesh out some definitions specifically dealing with finite degree field extensions of the rational numbers.

3.2 Number Fields

These will be the most tangible invariants of hyperbolic manifolds. By use of PARI, we will be able to produce polynomials whose roots are eigenvalues of matrices in $PSL_2(\mathbb{C})$ that correspond to geodesics in arithmetic hyperbolic 3-manifolds and other polynomials that can be used to construct fields that are invariant trace fields of arithmetic hyperbolic 3-manifolds. The following material comes from Chapter 0 of [16] and [21].

Definition 3.13 *A* **number field***, K, is a field extension of $\mathbb{Q}$ such that $[K : \mathbb{Q}] < \infty$.*

Definition 3.14 *A complex number, α, is an* **algebraic number** *if there exists a monic polynomial, $f(x) \in \mathbb{Q}[x]$, such that $f(\alpha) = 0$.*

Definition 3.15 *A complex number, α, is an* **algebraic integer** *if there exists a monic polynomial, $f(x) \in \mathbb{Z}[x]$, such that $f(\alpha) = 0$.*

Definition 3.16 *A* **conjugate** *of an algebraic number is a root of the minimal polynomial of the algebraic number.*

Theorem 3.17 *Let K be a field of characteristic zero or a finite field, let K' be an extension of degree n of K, and let C be an algebraically closed field containing K. Then, there exist n distinct $K-$isomorphisms of K' into C.*

Corollary 3.18 *For an algebraic number, α, there are n complex $\mathbb{Q}$-embeddings of $\mathbb{Q}(\alpha)$, where n is the degree of the minimal polynomial of α over $\mathbb{Q}$.*

Note that complex-conjugate pairs refer to $x + iy$ and $x - iy$ in Cartesian coordinates or $re^{i\theta}$ and $re^{-i\theta}$ in polar coordinates.

Definition 3.19 *Let α be an algebraic number. The* **signature** *of α is (r, c) where r is the number of real conjugates and c is the number of complex-conjugate pairs of conjugates. When the roots (or complex-conjugate pairs of roots) denote an embedding, they are referred to as real or complex places.*

Definition 3.20 *An extension field K of the field F is* **simple** *if there exists an element $\alpha \in K$ such that $K = F(\alpha)$. Furthermore, α is called a* **primitive element** *of K/F.*

Theorem 3.21 *If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.*

Corollary 3.22 *Any primitive element of a given number field has the same signature. Thus, we may speak of the signature of the number field as well.*

We will be most interested in number fields with signature $(n - 2, 1)$ and totally imaginary quadratic extensions of such fields, which have signature $(0, n)$. In less opaque language, we are interested in number fields with exactly one complex place (or exactly one pair of complex-conjugate embeddings) and quadratic extensions of these fields in which all places are complex places.

The following theorem may be included with the previous section, but we wish to emphasize the result for number fields. So, it is included here.

Theorem 3.23 *Let R be a ring ($\mathbb{Q}$ for example), A a subring of R ($\mathbb{Z}$ for example), and x and y elements of R, which are integral over A. Then, $x+y$, $x-y$, and xy are integral over A.*

Theorem 3.24 *The ring of integers of an algebraic number field is a Dedekind domain.*

Therefore, we may speak of the ring of (algebraic) integers in a number field in the same way that the ring of (algebraic) integers in the rational numbers is precisely the integers. Something else to note is that all elements (besides 0) in a number field are units. While this is true, we will use the term units to refer to the algebraic integers that are units. Soon we will be able to connect the structure of the group of units in an algebraic number field to the field's signature using Dirichlet's Unit Theorem. Note that roots of unity, i.e. solutions to $z^n = 1$ are an example of units. However, units do not necessarily have finite multiplicative order. For example, $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ has $x^2 - x - 1$ as its minimal polynomial over $\mathbb{Q}$. Then, $\frac{1+\sqrt{5}}{2} \cdot -\frac{1-\sqrt{5}}{2} = 1$, but $\lim_{n\to\infty}\left(\frac{1+\sqrt{5}}{2}\right)^n = \infty$. We are interested in units because, later, we will see that the eigenvalue of loxodromic and hyperbolic elements of $PSL_2(\mathbb{C})$ are units in some number field, and we have already seen that eigenvalues of elliptic elements in a Kleinian group must be roots of unity.

Theorem 3.25 *(Dirichlet's Unit Theorem) Let K be a number field, n its degree, and let (r, c) be the signature of K. Set $m = r + c - 1$. The group of units of K is isomorphic to $\mathbb{Z}^m \times G$, where G is a finite cyclic group comprised of the roots of unity contained in K.*

What follows below illustrates the fact that we need to generalize the concept of a prime number. Unique factorization of elements may fail in the ring of integers of a finite extension of the rational numbers.

Example 3.26 *It is a well known fact that the rational integers factor uniquely into a product of prime integers. For example,* $24 = 2^3 \cdot 3$*. But, this nice quality may be forfeited if one ventures up to a finite degree extension of the rational numbers. Consider the field* $\mathbb{Q}(\sqrt{-5})$ *where the ring of integers is* $\mathbb{Z}[\sqrt{-5}]$*. The element* 6 *has two factorizations into irreducible elements:* $2 \cdot 3$ *and* $(1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$*. This is seen by noting that if the norm of an algebraic integer is* $\pm$ *a prime in* $\mathbb{Z}$*, then the element is an irreducible element in the ring of integers. Also, the norm of an element,* $a + b\sqrt{D}$*, in a quadratic extension of* $\mathbb{Q}$ *is* $a^2 - b^2 D$*. Thus, we do not have unique factorization. The work above shows a bypass around this difficulty. If we pass to prime ideals, then this is no longer an issue and we can recover a property that is close to the unique factorization characteristic of the rational integers. The reason why this would remain unnoticed is that for the rational integers, the concept of prime and irreducible are identical.*

We mentioned that the eigenvalues of elements of arithmetic Kleinian groups will be algebraic units. Something that will be useful as an invariant of the fields they live in will be Galois groups. Before moving on with our current goal of generalizing the concept of an integer, we will give the fundamental theorem of Galois theory.

Theorem 3.27 *(Fundamental Theorem of Galois Theory) Let* K/F *be a Galois extension and set* $G = Gal(K/F)$*. Then, there is a bijection between subfields* E *of* K *containing* F *and subgroups* H *of* G*. More specifically,* E *corresponds to the elements of* G *fixing* E*, and* H *corresponds to the fixed field of* H*. These correspondences are inverses of each other. Under this correspondence,*

i) If E_1*,* E_2 *correspond to* H_1*,* H_2*, then* $E_1 \subseteq E_2$ *if and only if* $H_2 \leq H_1$*.*

ii) $[K : E] = |H|$ *and* $[E : F] = |G : H|$*, the index of* H *in* G*.*

iii) K/E *is always Galois, with Galois group* $Gal(K/E) = H$*.*

iv) E is Galois over F if and only if H is a normal subgroup in G.

v) If E_1, E_2 correspond to H_1, H_2, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence, the field lattice is the subgroup lattice turned upside down.

Proposition 3.28 *If $K/\mathbb{Q}$ is a Galois extension, then K has all real places or all complex places.*

Proof: This follows from the fact that each place corresponds to an embedding of K into $\mathbb{R}$ or $\mathbb{C}$ determined by sending α such that $K = \mathbb{Q}(\alpha)$ to a conjugate root β. Since K is assumed to be Galois, all embeddings are actually automorphisms of K. $\square$

Corollary 3.29 *Fields with at least one complex place and at least one real place are not Galois extensions of $\mathbb{Q}$.*

3.3 A Bridge and a Brief Aside

Example 3.26 demonstrates that we have to make some concessions in order to generalize the fact that integers factor uniquely. We will show this is Section 3.4. However, first we require a few more definitions.

Definition 3.30 *The (field)* **norm** *of an algebraic number, α, is defined as $N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma_i} \sigma_i(\alpha)$ where the product is taken over all $\mathbb{Q}$-embeddings, $\sigma_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.*

Definition 3.31 *The (field)* **trace** *of an algebraic number, α, is $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{\sigma_i} \sigma_i(\alpha)$ where the sum is taken over all $\mathbb{Q}$-embeddings, $\sigma_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.*

Proposition 3.32 *Let K be a number field and $\mathcal{O}_K$ the ring of integers. If α is a non-zero element of $\mathcal{O}_K$, then $|N_{K/\mathbb{Q}}(\alpha)|$ is equal to the cardinality of $\mathcal{O}_K/(\alpha)$.*

The proposition above justifies the following definition after we notice that if an integral ideal $\mathcal{I}$ contains a non-zero element α, then the ideal generated by α is contained in $\mathcal{I}$. Thus, the cardinality of $\mathcal{O}_K/\mathcal{I}$ is less than or equal to the cardinality of $\mathcal{O}_K/(\alpha)$.

Definition 3.33 *The* **norm** *of a non-zero integral ideal $\mathcal{I} \subset \mathcal{O}_K$ is the cardinality of $\mathcal{O}_K/\mathcal{I}$.*

Now, we define the Dedekind zeta function which is a generalization of the well-known Riemann zeta function. This function is involved in determining the volume of arithmetic hyperbolic 3-manifolds.

Definition 3.34 *Let K be a number field. The* **Dedekind zeta function** *is*

$$\zeta_K(s) = \sum_{\mathcal{I} \subset \mathcal{O}_K} \frac{1}{N(\mathcal{I})^s}$$

The function is defined for complex numbers, s, with real part greater than 1. If we take $K = \mathbb{Q}$, then the definition reduces to the Riemann zeta function.

3.4 Factorization of Prime Ideals

Now consider the situation where we have a finite extension, L, of a number field K. The ring of integers in K, denoted $\mathcal{O}_K$, is a Dedekind domain. Given a prime ideal $\wp \subset \mathcal{O}_K$, we know that $\wp\mathcal{O}_L$ is an ideal contained in $\mathcal{O}_L$. Since $\mathcal{O}_L$ is also a Dedekind domain, $\wp\mathcal{O}_L = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$ where $\mathcal{P}_i$ are prime ideals contained in $\mathcal{O}_L$.

Proposition 3.35 *In the discussion above, $\mathcal{P}_i$ where $i = 1, \ldots, n$ are the only prime ideals contained in $\mathcal{O}_L$ such that $\mathcal{P} \cap \mathcal{O}_K = \wp$.*

Now we are ready to define what it means for a prime ideal to ramify in a field extension and characterize which prime ideals ramify.

Definition 3.36 *Let $\wp \subset \mathcal{O}_K$ be a prime ideal, L/K a field extension, and $\wp\mathcal{O}_L = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$. Then, $\wp$ is* **ramified** *with respect to a field extension L/K if there exists an e_i greater than 1.*

Definition 3.37 *The* **discriminant** *Δ_K of a number field $K/\mathbb{Q}$ is defined as the ideal generated by $\{det[\sigma_i(\alpha_j)]^2\}$, where σ_i is an embedding of K into $\mathbb{C}$, α_j is a basis of $K/\mathbb{Q}$, and $[\sigma_i(\alpha_j)]$ is an $n \times n$ matrix with $[K : \mathbb{Q}] = n$.*

Definition 3.38 *The* **discriminant** *of L over K, denoted $\Delta_{L/K}$ or $\Delta_{\mathcal{O}_L/\mathcal{O}_K}$ is the ideal of $\mathcal{O}_K$ generated by the discriminants of bases of L over K which are contained in $\mathcal{O}_L$.*

Theorem 3.39 *With the notation as above, a prime ideal $\wp \subset \mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if it contains the discriminant $\Delta_{\mathcal{O}_L/\mathcal{O}_K}$. Note that the discriminant is an ideal and has a factorization that consists of finitely many primes ideals. Thus, only finitely many primes ramify in a given field extension.*

3.5 Non-Archimedean Local Fields

The aim of this section is to informally introduce local fields. They are prerequisite to proving the Chebotarev Density Theorem (though not needed for its statement), and they are needed to fully understand the notation in the section on quaternion algebras. The descriptor, local, refers to the fact that the field is a locally compact topological field with respect to a non-discrete topology. For our purposes, all local fields will have characteristic zero. Local fields are completions of number fields in the sense that every Cauchy sequence converges. This includes the Archimedean number fields $\mathbb{C}$ and $\mathbb{R}$, which are closed under Cauchy sequences when equipped with the usual norms. Given a number field and an embedding into $\mathbb{C}$, one may use the embedding to derive a norm, which is simply $norm(x) = |\sigma(x)|$, where $|\cdot|$ denotes the usual complex norm. Then, the completion of the field with respect to the aforementioned norm will be isomorphic to $\mathbb{C}$ or $\mathbb{R}$ depending on whether the embedding is real or complex. A real embedding or complex-conjugate pair of embeddings are called infinite places. Recall that they were called real and complex places in a previous section. Other completions are the non-archimedean number fields, which arise from prime ideals. Given a prime ideal, we can construct a norm and, then, a completion of that number field. These are called finite places of the number field. Likewise, these fields are complete in the sense that every Cauchy sequence converges. The important point to take away from this section is that this very informal discussion of local fields only serves to inform the reader of the terminology in the section on quaternion algebras. Finally, the completion of a number field K at a place σ (whether finite or infinite) is denoted K_σ, or $K_\wp$ if we want to emphasize that the place is finite.

3.6 Chebotarev Density Theorem

The Chebotarev Density Theorem is a result that specifies the statistical splitting behavior of a prime ideal of number field in a finite-degree extension. Exactly what is meant by statistical splitting behavior will be illuminated in an example following the theorem. First, we give a basic definition of natural density of a set of rational integers in order to put the definition of Dirichlet Density into perspective.

Definition 3.40 *The* **natural density** *of a subset of positive integers, S, is defined as $\lim_{n\to\infty} \frac{S(n)}{n}$, where $S(n)$ is the number of integers in S that are less than or equal to n.*

Now, instead of speaking about the density of a set in relation to the rational integers, now we will introduce a definition that measures how dense a particular set of prime ideals is with respect to the entire set of prime ideals. The counting function $S(n)$ now compares the number of prime ideals that split a certain way with the total number of prime ideals, which lie over the rational prime p less than or equal to n. The density is the ratio of the size of these sets as n goes to infinity. While this definition of density is quite natural, it is harder to compute than the Dirichlet density, which is defined below. See [8] for a reference.

Definition 3.41 *The* **Dirichlet density** *of a subset of primes, A, in a number field is*

$$\lim_{s \to 1^+} \frac{\displaystyle\sum_{\mathcal{P} \in A} N(\mathcal{P})^{-s}}{|log \frac{1}{1-s}|}$$

When the natural density of a set of prime ideals exists, the natural density is equal to the Dirichlet density. Although, the converse is not true.

Remark 3.42 *A simple observation is that there are infinitely many rational primes and, thus, infinitely many prime ideals. Given that the Dirichlet density of a set of prime ideals meshes with the natural density, the Dirichlet density of a finite set of prime ideals must be zero. The contrapositive of this simple observation is that there are infinitely many prime ideals in a set of non-zero density. See Chapter 4 Section 6 of [8] under Properties of Dirichlet Density.*

Now, the following theorem will supply us with a multitude of prime ideals.

Theorem 3.43 *(Chebotarev Density) Let K'/K be a normal extension with Galois group G. Let $\sigma \in G$ and suppose σ has c conjugates in G. The set of primes $\wp$ of K which have a prime divisor $\wp'$ in K' whose Frobenius automorphism is σ has a density $c/|G|$.*

We give the statement of the Chebotarev Density for completeness. However, all we need is the following corollary, which is tailored to our situation. See Chapter 3 Section 2 of [8] for details as to why a prime splits completely if and only if its Frobenius automorphism is the identity element.

Corollary 3.44 *For any finite collection of quadratic extensions of a number field K, there are infinitely many primes of K that split completely in the entire collection of quadratic extensions.*

Proof: Let N be the Galois closure of the collection of quadratic extensions over K. The set, S, of prime ideals of K that split completely has density $1/|G|$, where G is the Galois group of N over K. Recall 3.42, since $1/|G|$ is non-zero, there are infinitely many prime ideals in S. Note that every prime ideal in S factors into exactly $[N : K]$ prime ideals in N. Let L be a quadratic extension of K in the collection and $\wp$ a prime of K that splits completely in N. If $\wp$ remains prime in L, then $\wp$ has $[N : L]$ prime factors in N. Since $2 \cdot [N : L] = [N : K]$, we have a contradiction and $\wp$ must split in L (and, thus, split completely because $[L : K] = 2$).

Example 3.45 *The Chebotarev Density Theorem specifies the likelihood of a prime splitting in a certain way. The quadratic field $\mathbb{Q}(i)$ is a simple example of this phenomenon. The ring of integers in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. Through elementary means, it can be shown that the prime 2 ramifies in $\mathbb{Z}[i]$, primes $p \equiv 3 \bmod 4$ remain prime, and primes $p \equiv 1 \bmod 4$ split completely. Since there are only finitely many ramified primes, their density is zero. Otherwise, a prime either (completely) splits or remains prime. Since the Galois group of $\mathbb{Q}(i)$ over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z}$, the Frobenius automorphism is either the identity element or the nontrivial element of the Galois group. Thus, the density of the set of primes with a given Frobenius automorphism is $1/2$. The elementary method shows that "half" of the primes split and "half" remain prime, and the theorem reinforces this intuitive notion.*

3.7 Quaternion Algebras

Definition 3.46 *A* **quaternion algebra**, *A over F is a four-dimensional F-space with basis vectors $1, i, j$, and k. Multiplication is defined such that $1_A = 1_F$ is the* *multiplicative identity, $i^2 = a1$, $j^2 = b1$, and $ij = -ji = k$ for some $a, b \in F^*$ and by extending multiplication linearly so that A is an associative algebra over F. A quaternion algebra can be specified by $\left(\frac{a,b}{F}\right)$*

Definition 3.47 *The* **reduced norm** *and* **reduced trace** *of an element $x \in A$ are $n(x) = x\bar{x} \in F$ and $tr(x) = x + \bar{x} \in F$. Note that $\bar{x} = a_0 - a_1 i - a_2 j - a_3 k$ is the conjugate of $x = a_0 + a_1 i + a_2 j + a_3 k$.*

Definition 3.48 *An* **integer** *of A is $x \in A$ such that $n(x)$ and $tr(x)$ are integers of F.*

The following definition creates something analogous to the ring of integers in a number field. Unfortunately, the integers of a quaternion algebra do not form a ring, but Definition 3.50 corrects for such an inadequacy. The notion of ramification is introduced and the discriminant of a quaternion algebra is defined. We will see that only finitely many primes of a number field ramify in a quaternion algebra in the same way only finitely many primes of a number field ramify in an algebraic extension of a number field. While these definitions and theorems seem very abstract and without purpose (to a topologist), there are theorems that will make use of these definitions and theorems to produce results that will pertain to our situation, i.e., these number theoretic objects will provide the framework to address the overall goal of this paper.

Remark 3.49 *Previously in this section, F denoted the field over which the quaternion algebra, A, is defined. Now k will represent the number field over which A is defined. We make the distinction because now we are narrowing our perspective to that of a number field and, previously, k was used as one of the basis vectors of the quaternion algebra.*

Definition 3.50 *An order $\mathcal{O}$ is a finitely generated ring of integers in A which contains the ring of integers of k, denoted R_k, and $k\mathcal{O} = A$.*

Note that the symbol $\mathcal{O}$ has previously been used to identify the ring of integers of a number field. To avoid any confusion, $\mathcal{O}$ refers to an order in a quaternion algebra, while $\mathcal{O}_k$ refers to the ring of integers of k. However, when both objects are referred in a very close proximity as above, then R_k will denote the ring of integers of the number field k.

Definition 3.51 *A quaternion algebra A/k is* **ramified** *at a place, ν, of k if $A \bigotimes_k k_\nu$ is the unique division algebra over k_ν. Otherwise, A* **splits** *at ν.*

Now, we will state a theorem that provides equivalent statements dealing with quadratic extensions of the number field, k, which our quaternion algebra lies over. Recall that the ramification set contains places of the number field over which it is defined. These correspond to real embeddings, complex-conjugate pairs of embeddings, or prime ideals of k. For a quadratic extension L/k, an infinite place of k, σ, lifts to an embedding, $\hat{\sigma}$, of L. A real embedding may or may not split and a complex place always splits. A real embedding splits if $[L_{\hat{\sigma}} : k_\sigma] = 1$ and does not split if $[L_{\hat{\sigma}} : k_\sigma] = 2$.

Theorem 3.52 *Let L be a quadratic extension of k, where k is the number field over which the quaternion algebra, A, is defined. Then, the following are equivalent:*

i) L embeds in A.

ii) L splits A.

iii) $L \bigotimes_k k_\nu$ is a field for each $\nu \in Ram(A)$.

iv) Every element of $Ram(A)$ does not split in L.

Definition 3.53 *The discriminant of A/k, denoted $\Delta(A)$ is the product of prime ideals: $\displaystyle\prod_{\nu_\wp \in Ram_f(A)} \wp$, where $Ram_f(A)$ is the set of finite places that ramify A.*

Theorem 3.54 *(Classification of Quaternion Algebras) Let* A_1 *and* A_2 *be quaternion algebras over the number field* k *and let* $Ram(A_1)$ *be the set of places where* A_1 *is ramified. Then,*

i) The cardinality of $Ram(A_1)$ *is even.*

ii) $A_1 \cong A_2$ *if and only if* $Ram(A_1) = Ram(A_2)$

iii) For any finite set, denoted S*, of places of* k *(excluding any complex places) of even cardinality, then there exists a quaternion algebra* A *over* k *such that* $Ram(A) = S$.

4 Combining Geometric and Algebraic Knowledge

4.1 Arithmetic Hyperbolic 3-Manifolds

Hyperbolic 3-manifolds are hard to study. More specifically, producing examples of hyperbolic manifolds is tricky. The benefit of arithmetic hyperbolic 3-manifolds is that they are much easier to produce. If one has a certain kind of quaternion algebra and a certain kind of number field, then one may use these ingredients to construct one. The burden is shifted to existence of a certain kind of number field, and quaternion algebras, but the existence theorem for quaternion algebras greatly lightens this burden to simply finding certain kinds of number fields. Under certain circumstances, we may explicitly construct these types of number fields. Not only is this class of hyperbolic manifolds easier to construct, but this class has a nice characterization of commensurability, which relates to the quaternion algebra and number field from which the groups are constructed.

Before embarking on our tour of arithmetic Kleinian groups, we will first state some results that hold for a more general class of Kleinian groups. All of this material can be found in [16].

Definition 4.1 *Let Γ be a subgroup of $PSL_2(\mathbb{C})$. Then, Γ is* **elementary** *if the action of Γ on $\mathbb{H}^3 \cup \partial\mathbb{H}^3$ has a finite orbit. Otherwise, Γ is* **non-elementary**.

Definition 4.2 *Let Γ be a non-elementary subgroup of $PSL_2(\mathbb{C})$. Let $\hat{\Gamma} = P^{-1}(\Gamma)$, where P is the surjective homomorphism from $SL_2(\mathbb{C})$ to $PSL_2(\mathbb{C})$ that mods out by the subgroup $\{\pm I\}$. Then, the* **trace field** *of Γ, denoted by $\mathbb{Q}(tr\,\Gamma)$ is the field $\mathbb{Q}(tr\,\hat{\gamma} : \hat{\gamma} \in \Gamma)$.*

Theorem 4.3 *Let Γ be a Kleinian group of finite covolume. Then the trace field of Γ is a number field.*

Now we have the first appearance of a connection of hyperbolic 3-manifolds and algebraic number theory. The proof relies on Mostow-Rigidity. Although, the trace field of a finite covolume Kleinian group is always a number field. This is not a commensurability invariant. The following is from [19].

Example 4.4 *Consider the Kleinian group generated by the following two elements*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix}$$

where μ is a third root of unity equal to $(-1+\sqrt{-3})/2$. It is stated without proof that this subgroup is an index 12 subgroup of the arithmetic group $PSL_2(\mathcal{O}_3)$ where $\mathcal{O}_3$ is the set of algebraic integers in the field $\mathbb{Q}(\sqrt{-3})$. Thus, the subgroup above is also of finite covolume. Note, that multiplying the two elements above yields an element with trace equal to $2-\mu$. Also, any product of powers of the two elements above will have traces that are in $\mathbb{Q}(\sqrt{-3})$. Thus, the trace field is $\mathbb{Q}(\sqrt{-3})$. By adding,

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

we get a group such that the 2-generator subgroup above has index 2. By an appropriate multiplication, we get an element with trace i/μ, which is a twelfth root of unity. Hence, we have a commensurable groups with different trace fields.

We would like a notion of the trace field which *is* an invariant of the commensurability class. This is possible if we pass to a certain finite sheeted covering space and take the trace field of that Kleinian group. Given a Kleinian group Γ, consider $\Gamma^{(2)} = \langle \gamma^2 \mid \gamma \in \Gamma \rangle$. This is a finite index normal subgroup of Γ.

Theorem 4.5 *Let Γ be a finitely-generated non-elementary subgroup of $SL_2(\mathbb{C})$. The* *trace field of* $\Gamma^{(2)}$*, denoted* $k\Gamma := \mathbb{Q}(tr\Gamma^{(2)})$*, is an invariant of the commensurability class of* Γ*. The field* $k\Gamma$ *is called the invariant trace field of* Γ*.*

While we are listing invariants of commensurability classes of Kleinian groups, we might as well add to the list. Another invariant is a certain quaternion algebra associated to a Kleinian group. Let Γ be a subgroup of $SL_2(\mathbb{C})$. Then, we define $A_0\Gamma$ as the set $\{\Sigma a_i\gamma_i \mid a_i \in \mathbb{Q}(tr\ \Gamma^{(2)}),\ \gamma_i \in \Gamma^{(2)}\}$.

Theorem 4.6 *Let* Γ *be a non-elementary subgroup of* $SL_2(\mathbb{C})$*. Then,* $A_0\Gamma$ *is a quaternion algebra.*

Similar to the trace field, we must pass to a finite-sheeted covering space and take the quaternion algebra associated to that Kleinian group. This is actually a corollary to Theorem 4.5.

Corollary 4.7 *If* Γ *is a finitely generated, non-elementary subgroup of* $SL_2(\mathbb{C})$*, then the quaternion algebra* $A\Gamma := A_0\Gamma$ *is an invariant of the commensurability class of* Γ*. The quaternion algebra* $A\Gamma$ *is called the invariant quaternion algebra of* Γ*.*

Now, we finally define arithmetic Kleinian groups, but first we require one more definition. Recall that an order, $\mathcal{O}$, of a quaternion algebra, A/k, is a finitely generated ring of integers in A which contains the ring of integers of k, R_k, and $k\mathcal{O} = A$. This material in Chapter 8.2 of [16]

Definition 4.8 *Let* $\mathcal{O}$ *be an order of* A*. Then, the* **elements of norm 1***, denoted* $\mathcal{O}^1$*, consists of all* $\alpha \in \mathcal{O}$ *such that* $n(\alpha) = 1$ *where* $n(\cdot)$ *is the reduced norm.*

Definition 4.9 *Let* k *be a number field with exactly one complex place and let* A *be a quaternion algebra over* k *which is ramified at all real places. Let* ρ *be an embedding of* A *into* $M_2(\mathbb{C})$ *and let* $\mathcal{O}$ *be an* R_k*-order of* A*. Then, a subgroup* γ *of* $PSL_2(\mathbb{C})$ *is an* **arithmetic Kleinian group** *if it is commensurable with some* $P\rho(\mathcal{O}^1)$*, where*

P refers to projectivizing. Hyperbolic 3-manifolds are called **arithmetic** *when their fundamental groups are arithmetic Kleinian groups.*

Definition 4.10 *An arithmetic Kleinian group is* **derived** *(from a quaternion algebra) if, in addition to the criteria in the previous definition, it is contained in some $P\rho(\mathcal{O}^1)$.*

We note now that groups constructed this way are discrete and have finite covolume. These facts take proof, which are omitted but may be found in *Chapter 8* of [16].

Theorem 4.11 *If Γ is an arithmetic Kleinian group which is commensurable with $\rho(\mathcal{O}^1)$, where $\mathcal{O}$ is an order in a quaternion algebra A/k and ρ is a k-embedding, then $k\Gamma = k$ and $A\Gamma = \rho(A)$.*

What follows here is a characterization when an arithmetic Kleinian group is not cocompact. Notice that an arithmetic Kleinian group's compactness is entirely determined by arithmetic data.

Theorem 4.12 *Let Γ be an arithmetic Kleinian group commensurable with $P\rho(\mathcal{O}^1)$, where $\mathcal{O}$ is an order in a quaternion algebra A/k. The following are equivalent:*

i) Γ is not cocompact.

ii) $k = \mathbb{Q}(\sqrt{-d})$ and $A = M_2(k)$

Similarly, other arithmetic data determine precisely when a Kleinian group is arithmetic.

Theorem 4.13 *Let Γ be a finite-covolume Kleinian group. Then Γ is arithmetic if and only if the following three conditions hold.*

i) $k\Gamma$ is a number field with exactly one complex place.

ii) $tr(\gamma)$ is an algebraic integer for all $\gamma \in \Gamma$.

iii) $A\Gamma$ is ramified at all real places of $k\Gamma$.

And, here we see that an arithmetic Kleinian group has a finite-index subgroup that is a derived Kleinian group, which is a stronger version of arithmeticity.

Theorem 4.14 *Let Γ be a finite-covolume Kleinian group. Then, Γ is arithmetic if and only if $\Gamma^{(2)}$ is derived from a quaternion algebra.*

Another characterization of derived is contained in the following theorem:

Theorem 4.15 *Let Γ be a finite-covolume Kleinian group. Then Γ is derived if and only if the following three conditions hold.*

i) $k\Gamma$ is a number field with exactly one complex place.

ii) $tr(\gamma)$ is an algebraic integer for all $\gamma \in \Gamma$.

iii) $|\sigma(tr\ \gamma)| \leq 2$.

When our Kleinian group is derived from a quaternion algebra, we have a better handle of what algebraic integers may appear as eigenvalues.

Proposition 4.16 *Let Γ be an arithmetic Kleinian group derived from a quaternion algebra A/k.*

1) *Let λ be an eigenvalue for a loxodromic element in Γ. If λ is not real then $k = \mathbb{Q}(\lambda + 1/\lambda)$.*

2) *Let Γ be derived from a quaternion algebra, and $\gamma \in \Gamma$ a loxodromic element with eigenvalues $\{\lambda, 1/\lambda\}$. Then the following possibilities hold for $\lambda = re^{i\theta}$.*

i) λ *is not real and the Galois conjugates off of the unit circle are* $\lambda, 1/\lambda, \bar{\lambda}$, *and* $1/\bar{\lambda}$.

ii) λ *is real and the Galois conjugates off of the unit circle are* λ *and* $1/\lambda$.

Furthermore, λ *is an algebraic integer with palindromic minimal polynomial. If* λ *is not real, then* $k(\lambda) = \mathbb{Q}(\lambda)$, *and* $[k(\lambda) : k] = 2$. *If* λ *is real, then* $\mathbb{Q}(\lambda + 1/\lambda)$, *denoted* k^+ *is the maximal totally real subfield of* k, $[k : k^+] = 2$ *and* $\mathbb{Q}(\lambda)$ *is a degree two extension of* k^+.

Proposition 4.17 *Any* λ *that fulfills the conditions of part 2(i) or 2(ii) of the above proposition occurs as an eigenvalue of an element of some arithmetic Kleinian group derived from a quaternion algebra.*

Something we will need later is a criterion as to when a certain eigenvalue appears in an arithmetic Kleinian group. Recall that Theorem 3.52 gives a list of equivalent criteria for when a quadratic extension embeds into a quaternion algebra.

Theorem 4.18 *Let* Γ *be a Kleinian group derived from a quaternion algebra* A/k. *Let* L *be a quadratic extension of* k. *Then* L *embeds in* A *if and only if* Γ *contains an element* γ *of infinite order with* $L = k(\lambda)$ *where* λ *is the eigenvalue of* γ *with norm greater than 1.*

4.2 Why *Arithmetic* Hyperbolic 3-Manifolds?

Constructing hyperbolic 3-manifolds is hard in general. As previously mentioned, a good reason for studying arithmetic hyperbolic 3-manifolds is that they are easy to construct. Another motivation is that arithmetic data can tell you something about geometric qualities of the manifold. First, we will provide the volume formula for Kleinian groups arising from maximal orders. Then, a later theorem can be used to construct hyperbolic 3-manifolds in which all geodesics are simple. Note that the following two discussion points will not be used later, but are included to highlight the ease of working with arithmetic hyperbolic 3-manifolds and the utility of arithmetic data with respect to hyperbolic 3-manifolds.

Theorem 4.19 *Let k be a number field with exactly one complex place, A/k be a quaternion algebra ramified at all real places of k, $\mathcal{O}$ be a maximal order in A, P be a prime ideal of k, and $\Delta(A)$ the discriminant of A. Then,*

$$Vol(\mathbb{H}^3/P\rho(\mathcal{O}^1)) = (4\pi^2)^{1-[k:\mathbb{Q}]}|\Delta_k|^{3/2}\zeta_k(2)\prod_{P|\Delta(A)}(N(P)-1)$$

The covolume of an arithmetic Kleinian group is entirely determined by arithmetic information. The degree of k over $\mathbb{Q}$, discriminant of k, value of the Dedekind zeta function at 2, and norms of prime ideals which ramify in A entirely determine the volume of such a group. While not all arithmetic Kleinian groups arise this way, they will share a finite-sheeted cover and, therefore, the covolume of any arithmetic Kleinian group will be a rational multiple of the volume formula given in the theorem above.

The following theorem and corollary give a method to produce arithmetic Kleinian groups that only contain simple closed geodesics. Simple closed geodesics are closed geodesics that do not self intersect.

Theorem 4.20 *If M has a non-simple closed geodesic, then $A\Gamma \cong (\frac{a,b}{k\Gamma})$ for some $a \in k\Gamma$ and $b \in k\Gamma \cap \mathbb{R}$.*

Corollary 4.21 *Suppose that there are no elements $a \in k\Gamma$ and $b \in k\Gamma \cap \mathbb{R}$ such that $A\Gamma \cong (\frac{a,b}{k\Gamma})$. Then, all of the closed geodesics of the closed hyperbolic 3-manifold $M = \mathbb{H}^3/\Gamma$ are simple.*

While the corollary above does not necessarily need an arithmetic hyperbolic 3-manifold, the construction of such Kleinian groups in [16] uses arithmetic Kleinian groups because they are easier to deal with than general Kleinian groups.

Another instance of algebraic data being able to describe geometric phenomena deals with the lengths of closed geodesics in arithmetic hyperbolic 3-manifolds. Recall Proposition 4.16 says the lengths of closed geodesics are highly related to certain roots of integral polynomials which have most roots on the unit circle. Unlike the volume formula and manifolds with only simple geodesics, the section will be used later in this paper.

5 Previous Results

These results provide the basis and theme for further investigation and can be found in [4]. Recall our main goal is to see how many angles may be paired with the norm of a loxodromic eigenvalue and yield a loxodromic eigenvalue. The main result from [4] states that two arithmetic hyperbolic 3-manifolds are commensurable if and only if their rational length sets are equal. Now, we are assuming that we have two iso-length spectral arithmetic hyperbolic 3-manifolds, which implies their rational length sets are equal. Thus, they are commensurable, and then they have equal invariant trace fields. Furthermore, if we have two loxodromic eigenvalues of equal norm from the pair of iso-length-spectral manifolds, then the loxodromic eigenvalues must be quadratic extensions of the same trace field. This discussion sparks our interest in the trace field.

Definition 5.1 *Let k be a number field. Then the* **conjugate** *of k, denoted $\bar{k}$, is the field consisting of the complex conjugates of all elements in k.*

Example 5.2 *Let k be a number field. If k is a Galois field, then $k = \bar{k}$. So, for a positive, square-free integer D, $\mathbb{Q}(\sqrt{-D}) = \overline{\mathbb{Q}(\sqrt{-D})}$.An example is that is not a Galois extension is $\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}(-i\sqrt{2}) = \overline{\mathbb{Q}(i\sqrt{2})}$. Furthermore, it is possible for $k \neq \bar{k}$. For example, $\mathbb{Q}(\mu\sqrt{3}) \neq \mathbb{Q}(\bar{\mu}\sqrt{3}) = \overline{\mathbb{Q}(\mu\sqrt{3})}$*

Recall that we would like to fix the norm, r, of a loxodromic eigenvalue and determine how many $e^{i\theta}$ may be paired with r such that $re^{i\theta}$ is a loxodromic eigenvalue. Previous work was done in the case that $k = \bar{k}$. The following theorems, proved in [4], give us information about what we can glean from this case.

Proposition 5.3 *Let $\lambda = re^{i\theta}$ be an eigenvalue of a loxodromic element in an arithmetic Kleinian group derived from a quaternion algebra A/k. Suppose that $k = \bar{k}$, and let $m = [k : \mathbb{Q}]$.*

i) *If* $k(\lambda) = k(\bar{\lambda})$, *then* $e^{i\theta}$ *is a root of unity of degree less than or equal to* $4m$ *over* $\mathbb{Q}$. *In this case,* $[\mathbb{Q}(r^2) : \mathbb{Q}] < 2m$.

ii) *If* $k(\lambda) \neq k(\bar{\lambda})$, *then* r^2 *and* $e^{2i\theta}$ *are roots of the same irreducible monic polynomial over* $\mathbb{Q}$, *and hence* $e^{i\theta}$ *is not a root of unity. In this case,* $[\mathbb{Q}(r^2) : \mathbb{Q}] = 2m$.

Proposition 5.4 *Let* Γ_1 *and* Γ_2 *be arithmetic Kleinian groups derived from quaternion algebras* A_1 *and* A_2 *over* k. *Let* $\gamma_1 \in \Gamma_1$ *and* $\gamma_2 \in \Gamma_2$ *be loxodromic isometries with corresponding eigenvalues* $\lambda_1 = re^{i\theta_1}$ *and* $\lambda_2 = re^{i\theta_2}$, *with* $|\lambda_1|, |\lambda_2| > 1$.

i) *If* $k(\lambda_1) \neq k(\lambda_2)$, *then* ${\lambda_1}^2 = \bar{\lambda}_2^2$.

ii) *If* $k(\lambda_1) = k(\lambda_2)$ *and* r^2, $e^{2i\theta_1}$, *and* $e^{2i\theta_2}$ *are roots of the same irreducible monic polynomial over* $\mathbb{Q}$, *then* ${\lambda_1}^2 = {\lambda_2}^2$.

So, under the circumstances of part *ii*), the angle is unique. (Recall that λ and $-\lambda$ correspond to a geodesic of the same complex length) Under the circumstances of part *i*), the angle can have two values.

Remark 5.5 *Later it will be proved that the second statement above has an analogue if we remove the requirement on the conjugates of* r^2. *That is, if* $k(\lambda_1) = k(\lambda_2)$, *then* ${\lambda_1}^n = {\lambda_2}^n$ *for some* n. *Stated in another way, the first eigenvalue is equal to the product of the second eigenvalue and an* n^{th} *root of unity. Also, it will be shown that for every* n, *we can find a pair of eigenvalues such that* n *is the smallest power fulfilling the aforementioned equation. We do have a bound for* n. *Adjoining the root of unity,* μ, *to* k *is necessarily a quadratic extension of* k. *As such,* $\mu + 1/\mu \in k$. *So,* $\phi(n)/2 \leq [k : \mathbb{Q}]$ *where* ϕ *is Euler's totient function.*

The following theorem helps us partially determine $e^{i\theta}$ for a given r in the case that $k = \bar{k}$.

Corollary 5.6 *In addition to the supposition of Proposition 5.4, suppose* $k = \bar{k}$, *then* *i) If* $[\mathbb{Q}(r^2) : \mathbb{Q}] < 2m$*, then both* $e^{2i\theta_1}$ *and* $e^{2i\theta_2}$ *are roots of unity of degree less than or equal to* $4m$ *over* $\mathbb{Q}$*.*

ii) If $[\mathbb{Q}(r^2) : \mathbb{Q}] = 2m$*, then either* ${\lambda_1}^2 = {\lambda_2}^2$ *or* ${\lambda_1}^2 = \bar{\lambda}_2^2$*.*

Definition 5.7 *Let* Γ *be a Kleinian group and let* γ *be a loxodromic element of* Γ *with eigenvalue* λ*, meaning that* $tr(\gamma) = \lambda + 1/\lambda$*, with* $|\lambda| > 1$*. Then,* γ *is* **generic** *if no power of* λ *is real.*

An equivalent definition of a generic loxodromic eigenvalue, $\lambda = re^{i\theta}$, is that $e^{i\theta}$ is not a root of unity. Note if $e^{i\theta}$ were a root of unity, then some power of λ would be real, and, thus, the corresponding normal form of the element in $PSL_2(\mathbb{C})$ would have real trace.

Recall that a loxodromic eigenvalue, $\lambda = re^{i\theta}$, is generic if $e^{i\theta}$ is not a root of unity. So, for a given r that comes from a trace field that is fixed under complex conjugation, norms of generic loxodromic elements may only be paired with two possible angles. This creates a problem that will be discussed after 5.12. However, norms of non-generic loxodromic elements are roots of unity and it is less clear as to which roots of unity may be paired with these norms, but we will have a characterization of such roots with Theorem 7.8.

The following is a standard result for invariant trace fields of arithmetic Kleinian groups. Recall that Theorem 4.12 states if an arithmetic Kleinian group with invariant quaternion algebra A/k is not cocompact then $[k : \mathbb{Q}] = 2$.

Proposition 5.8 *Let* Γ *be an arithmetic Kleinian group with invariant trace field* k *such that* $[k : k \cap \mathbb{R}] > 2$*. Then,* Γ *does not contain a hyperbolic element.*

Proof: If $[k : k \cap \mathbb{R}] > 2$, then $[k : \mathbb{Q}] > 2$, which implies k has a real place. Suppose $\gamma \in \Gamma$ is a hyperbolic element with eigenvalue λ. Then, $\gamma^{2m} \in \Gamma^{(2)}$ for any $m \geq 1$ and $\lambda^{2m} + 1/\lambda^{2m} \in k \cap \mathbb{R}$. Since $[k : k \cap \mathbb{R}] > 2$, there exists an embedding

$\sigma : k \hookrightarrow \mathbb{R}$ such that $\sigma|_{k\cap\mathbb{R}}$ is the identity map. Therefore, for some value of m, $|\sigma(tr\ \gamma^{2m})| = |tr\ \gamma^{2m}| > 2$. However, by Theorem 4.15 part 3), it must be the case that $|\sigma(tr\ \gamma^{2m})| \leq 2$. Hence, Γ cannot contain a hyperbolic element. $\square$

Note that this also implies that Γ only contains generic loxodromic elements if $[k : k \cap \mathbb{R}] > 2$. Since otherwise, some power of a non-generic loxodromic element is hyperbolic. The next proposition is a standard result for number fields and holds as long as k has at least one complex place. However, we state it here as it is relevant to our specific setting.

Proposition 5.9 *Let k be the invariant trace field of an arithmetic Kleinian group Γ. Then, $[k : k \cap \mathbb{R}] = 2$ if and only if $k = \bar{k}$.*

Proof: Suppose $[k : k \cap \mathbb{R}] = 2$. Then, k is a Galois extension of $k \cap \mathbb{R}$. Thus, any non-trivial isomorphism that fixes $k \cap \mathbb{R}$ must be an automorphism of k and, furthermore, generate the Galois group. Conjugation fixes $k \cap \mathbb{R}$ but does not fix $\lambda + 1/\lambda$ since $\lambda \notin \mathbb{R}$ and $|\lambda| > 1$. Hence, conjugation is an automorphism of k. So, we may conclude $k = \bar{k}$.

Now, suppose $k = \bar{k}$. By Proposition 4.16, $\mathbb{Q}(\lambda + 1/\lambda) = \mathbb{Q}(\bar{\lambda} + 1/\bar{\lambda})$ for any loxodromic eigenvalue of γ. Then, $x^2 - (\alpha + \bar{\alpha})x + \alpha \cdot \bar{\alpha}$ where $\alpha = \lambda + 1/\lambda$ is the minimal polynomial of $\lambda + 1/\lambda$ over $k \cap \mathbb{R}$. The coefficients are real and elements of k, since $k = \bar{k}$. Since $k \not\subset \mathbb{R}$, it must be that $[k : k \cap \mathbb{R}] = 2$. $\square$

Corollary 5.10 *Let k be the invariant trace field of of an arithmetic Kleinian group Γ. If $[k : \mathbb{Q}]$ is odd, then $k \neq \bar{k}$.*

Proof: If $[k : \mathbb{Q}]$ is odd, then $2 \nmid [k : \mathbb{Q}]$. Since $[k : k \cap \mathbb{R}] \mid [k : \mathbb{Q}]$, this implies that $[k : k \cap \mathbb{R}] \neq 2$. By Proposition 5.9, this implies that $k \neq \bar{k}$. $\square$

For the moment, suppose that a derived Kleinian group, Γ, contains loxodromic elements with eigenvalues of λ and $\bar{\lambda}$. Then, by Theorem 4.16 part 1), $k = \mathbb{Q}(\lambda + 1/\lambda) = \mathbb{Q}(\bar{\lambda} + 1/\bar{\lambda}) = \bar{k}$. So, if $k \neq \bar{k}$, then Γ cannot contain generic loxodromic elements with eigenvalues that are conjugate. Conjugate eigenvalues may be a serious problem for isospectrality. There is no way to control the number of times an eigenvalue and its conjugate occur in the length spectrum. (Although number theoretic methods exist to compute multiplicities in certain cases. These can be found in [26].) So, the case where $k \neq \bar{k}$ is nicer. Also, if $k \neq \bar{k}$, then this does get rid of purely hyperbolic elements and their angles which are roots of unity, but we will see that the roots of unity do manifest themselves and create another problem. The following result may be found in [24].

Theorem 5.11 *Let K be a Galois extension of $\mathbb{Q}$ with Galois group $G := G(K/\mathbb{Q})$, and let k_1 and k_2 be subfields of K corresponding to subgroups H_1 and H_2 of G respectively. Then, the following conditions are equivalent:*

i) Each conjugacy class of G meets H_1 and H_2 in the same number of elements.

ii) The same primes p are ramified in k_1 and k_2, and, for the non-ramified p, the decomposition of p in k_1 and k_2 is the same.

iii) The zeta functions of k_1 and k_2 are the same.

The following corollary follows either from the observation that isomorphic fields have the same zeta function (it is a number field invariant) so *iii*) holds, or that subgroups of the Galois group corresponding to isomorphic subfields of a Galois extension are conjugate subgroups and, thus, *i*) holds. (For the curious reader, the converse is not true. There exist number fields with identical zeta functions that are not isomorphic number fields. See [18].)

Corollary 5.12 *Let k_1 and k_2 be quadratic extensions of the number field k. If k_1 and k_2 are isomorphic as fields, then any prime in k has identical splitting behavior in k_1 and k_2.*

In the case where $k = \bar{k}$, the only solace we may offer is that if $k(\lambda) = \mathbb{Q}(\lambda)$ embeds in a quaternion algebra where λ is a generic loxodromic eigenvalue, then $k(\bar{\lambda}) = \mathbb{Q}(\bar{\lambda})$ also embeds in the same quaternion algebra. Consider the following argument. Since λ and $\bar{\lambda}$ are roots of the same integral polynomial, the corresponding fields, $\mathbb{Q}(\lambda) = k(\lambda)$ and $\mathbb{Q}(\bar{\lambda}) = k(\bar{\lambda})$, are isomorphic. By Corollary 5.12, both fields have identical prime splitting behavior, which determines whether or not the field embeds in a given quaternion algebra by Theorem 3.52. However, this gives us no control over the multiplicity of the eigenvalue and just because $k(\lambda)$ embeds into a quaternion algebra does not imply we have an element in a Kleinian group with an eigenvalue of λ. It only implies that an element in our Kleinian group has a power of λ as its eigenvalue. While this is not a definite obstruction, we do not have the tools necessary to investigate this.

6 New Results

6.1 Angles of Loxodromic Eigenvalues

In this section, we prove:

Theorem 1.5 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in a Kleinian group derived from a quaternion algebra A/k. Then, there are only finitely many $e^{i\theta}$ such that $re^{i\theta}$ is a loxodromic eigenvalue in a Kleinian group derived from A/k.*

Previous work was done to make progress on the possible equivalence of real-length and complex-length isospectrality in arithmetic hyperbolic 3-manifolds. We will see how much the algebraic restrictions on the lengths of geodesics determine the angle. For example, if the angle corresponding to the length of the geodesic were unique, then we would have a positive solution to Question 1.4. From an algebraic perspective, the angle is not unique, i.e., there do exist loxodromic eigenvalues of equal norm but different angles. We will give examples of such polynomials (if you believe the output of PARI). Even though this is the case, important information can still be obtained from this perspective.

Note that an eigenvalue of a loxodromic element is equivalent to the complex length of the loxodromic element (the length is the complex logarithm of the eigenvalue). Since the eigenvalues are algebraic integers, it is more convenient to deal with the eigenvalues as opposed to the actual length of a closed geodesic. In this section $\lambda = re^{i\theta}$ is an eigenvalue of a loxodromic eigenvalue in an arithmetic Kleinian group Γ derived from a quaternion algebra A/k where k is a number field with exactly one complex place such that $[k : \mathbb{Q}] = m$. The first thing we will show is that the number of angles that may be paired with a given length is finite. A frequently-used fact is that the conjugates of λ have norm equal to r, $1/r$, or 1, which follows from Theorem 4.16 part 3 i). Furthermore, this implies that any product of conjugates of λ has norm equal to r^2, $1/r^2$, r, $1/r$, or 1.

Lemma 6.1 *Let $\lambda = re^{i\theta}$ be a loxodromic eigenvalue from a Kleinian group derived from A/k such that $|\lambda| = r > 1$. Then, the conjugates of $r^2 = \lambda \cdot \bar{\lambda}$ and $e^{2i\theta} = \lambda/\bar{\lambda}$ are r^2, $1/r^2$, $re^{i\tau}, 1/re^{i\tau}$, or $e^{i\tau}$ where τ varies depending on the given product.*

Proof: Recall from Theorem 4.16 part 3 i) that the conjugates of λ look like λ, $\bar{\lambda}$, $1/\lambda$, $1/\bar{\lambda}$ or $e^{i\phi}$. Note, to exactly determine the conjugates of the product, we need to know all elements in the Galois group of N_λ. (Recall that N_λ is the splitting field for the minimal polynomial of λ or, equivalently, the Galois closure of $\mathbb{Q}(\lambda)$.) However, what we desire is to know all of the possibilities. There are eight possible products of the aforementioned quantities when we exclude products such as $\lambda \cdot 1/\lambda = 1$, which does not give a possible conjugate of r^2. The possible valid products with λ are $r^2 = \lambda \cdot \bar{\lambda}$, $e^{2i\theta} = \lambda \cdot 1/\bar{\lambda}$, and $re^{i\tau} = \lambda \cdot e^{i\phi}$. The remaining valid products of $\bar{\lambda}$ are $e^{-2i\theta} = \bar{\lambda} \cdot 1/\lambda$ and $re^{i\tau} = \bar{\lambda} \cdot e^{i\phi}$. The remaining valid products of $1/\lambda$ are $1/r^2 = 1/\lambda \cdot 1/\bar{\lambda}$ and $1/re^{i\tau} = 1/\lambda \cdot e^{i\phi}$. Lastly, the remaining valid products of $e^{i\phi_1}$ are $e^{i\tau} = e^{i\phi_1} \cdot e^{i\phi_2}$. $\square$

The following proof relies on the fact that if a set of algebraic integers has uniformly bounded degree and the norms of the conjugates are uniformly bounded away from 0 and ∞, then the set has finite cardinality. To see this, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates corresponding to a degree n polynomial f. Then, $f(x)$ equals

$$\prod_{i=1}^{n} (x - \alpha_i)$$

and the coefficients of f are symmetric polynomials in α_i. Furthermore, we are looking at algebraic integers. So, the coefficients of the polynomial are integers. By bounding the degree and norm of α_i, the norm of the symmetric polynomials are bounded. Hence, this implies there are only finitely many polynomials with integer coefficients that correspond to the prescribed bounds.

Finally, we state some notation. Let α be an algebraic number. Then, we denote the Galois (or normal) closure of $\mathbb{Q}(\alpha)$ as N_α. The Galois closure is simply the splitting field for a polynomial that defines the field. Let K/F be a Galois extension. We denote the Galois group of K/F by $G(K/F)$. Also, note that for a loxodromic eigenvalue $\lambda = re^{i\theta}$, $e^{i\theta} \neq \pm 1$.

Proof of Theorem 1.5: By Proposition 4.16, λ is an algebraic integer, and, thus, all conjugates of λ are algebraic integers, since they satisfy the same monic, integral polynomial. Recall that $1/\lambda$ is a conjugate of λ. By Theorem 3.23, algebraic integers form a ring. So, $r^2 = \lambda \cdot \bar{\lambda}$ and $1/r^2 = 1/\lambda \cdot 1/\bar{\lambda}$ are also algebraic integers. Since r and $1/r$ satisfy the polynomials $x^2 - r^2$ and $x^2 - 1/r^2$, r and $1/r$ are algebraic integers as well. Furthermore, algebraic integers are closed under multiplication. So, $e^{i\theta} = 1/r \cdot re^{i\theta}$ is also an algebraic integer. Let $\sigma \in G(N_{r,e^{i\theta}}/\mathbb{Q})$. We will consider all σ that fix r. (The set of all such automorphisms is nonempty, since the identity map is an automorphism that fixes r.) Note that from Theorem 4.16 the conjugates of λ are known. If we assume that r is fixed under some embedding into $\mathbb{C}$, then we can determine the image of $e^{i\theta}$ under the embedding as well.

Claim: If $\sigma(r) = r$, then $\sigma(e^{i\theta}) = e^{\pm i\theta}$.

Suppose by way of contradiction, there exists σ such that $\sigma(r) = r$ and $\sigma(re^{i\theta}) = 1/\lambda$, $1/\bar{\lambda}$, or $e^{i\phi}$. First, assume $\sigma(\lambda) = 1/\bar{\lambda}$. (If $\sigma(\lambda) = 1/\lambda$, then compose σ with conjugation. Note that $\sigma(r)$ will still equal r.) Then, $\sigma(re^{i\theta}) = r \cdot \sigma(e^{i\theta})$, which implies $\sigma(e^{i\theta}) = 1/r^2 \cdot e^{i\theta}$ and also $\sigma(e^{2i\theta}) = 1/r^4 \cdot e^{2i\theta}$. Thus, $e^{2i\theta}$ has a conjugate with norm $1/r^4$, which is a contradiction by Lemma 6.1. Second, assume $\sigma(re^{i\theta}) = e^{i\phi}$. Then, $\sigma(e^{i\theta}) = 1/r \cdot e^{i\phi}$ and, furthermore, $\sigma(e^{2i\theta}) = 1/r^2 \cdot e^{2i\phi}$. By Lemma 6.1, the only possible conjugate of $e^{2i\theta}$ with norm equal to $1/r^2$ is precisely $1/r^2$. But, this implies $e^{i\phi} = \pm 1$, which is a contradiction.

By Theorem 3.27, $\mathbb{Q}(e^{i\theta} + e^{-i\theta})$ is a subset of $\mathbb{Q}(r)$, which implies $[\mathbb{Q}(e^{i\theta}) : \mathbb{Q}]$ is bounded because $[\mathbb{Q}(r) : \mathbb{Q}]$ is fixed and $\mathbb{Q}(e^{i\theta})$ is a degree 2 extension of $\mathbb{Q}(e^{i\theta} + e^{-i\theta})$. Therefore, the degree of the minimal polynomial of $e^{i\theta}$ is bounded. In this case, since $|\sigma(e^{i\theta})| = |\sigma(re^{i\theta})|/|\sigma(r)|$ and the norm of the conjugates of $re^{i\theta}$ and r are bounded, the norm of the conjugates of $e^{i\theta}$ are bounded. Therefore, the set of loxodromic angles with a corresponding loxodromic eigenvalue of norm equal to r has bounded degree and all its conjugates have bounded norm. Hence, there are only finitely many such values. $\square$

Now, there is a natural discussion that follows the proof of Theorem 1.5. However, it does not address the main goals outlined in the introduction. As a result, we have move this discussion to Section 7.2.

Remark 6.2 *Consider an algebraic integer, $\alpha \neq 1$, such that $1/\alpha$ is a root of the same minimal polynomial. Let σ be any embedding of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$, and notice that σ induces an embedding of $\mathbb{Q}(\alpha+1/\alpha)$ into $\mathbb{C}$. Then, $\mathbb{Q}(\alpha+1/\alpha)$ is fixed by an embedding if and only if $\alpha \mapsto \alpha^{\pm 1}$. One implication is clear. To show the other implication, assume that $\mathbb{Q}(\alpha + 1/\alpha)$ is fixed by an embedding. Then, $\alpha + 1/\alpha = \sigma(\alpha + 1/\alpha) = \sigma(\alpha) + 1/\sigma(\alpha)$. There are at most two solutions to the equation $z + 1/z = \beta$. To see this, multiply both size by z and subtract βz from both sides, which yields the quadratic equation $z^2 - \beta z + 1$. Therefore, if $\mathbb{Q}(\alpha + 1/\alpha)$ is fixed by an embedding, then $\alpha \mapsto \alpha^{\pm 1}$.*

Before we prove the corollary, consider a loxodromic eigenvalue with $\lambda = ri$. Then, $\mathbb{Q}(i + 1/i) = \mathbb{Q} \subset \mathbb{Q}(r)$. Therefore, in the following corollary we do not consider the case where $e^{i\theta} = i$. This corollary will be used in Section 6.6, which contains some results that are not central to our investigation and may be skipped if so desired.

Corollary 6.3 *Let $\lambda = re^{i\theta}$ with $e^{i\theta} \neq \pm i, \pm 1$. If $1/r$ is a conjugate of r, then $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r + 1/r)$. Otherwise, if $1/r$ is not a conjugate of r, then $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) = \mathbb{Q}(r)$.*

Proof: From the proof of Proposition 1.5, we see that $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r)$. Recall, an automorphism of N_λ sends λ to some element of $\{\lambda, 1/\lambda, \bar{\lambda}, 1/\bar{\lambda}, e^{\pm i\phi_k}\}$. Let $\sigma \in G(N_{r,e^{i\theta}}/\mathbb{Q})$. Now, the proof breaks down into two cases.

Case 1: $1/r$ is a conjugate of r.

By Remark 6.2, we must show $\sigma(r) = 1/r$ implies $\sigma(e^{i\theta}) = e^{\pm i\theta}$. Suppose $\sigma(\lambda) = \lambda$. Then, $1/r \cdot \sigma(e^{i\theta}) = \sigma(re^{i\theta}) = re^{i\theta}$. Multiplication by r yields $\sigma(e^{i\theta}) = r^2 e^{i\theta}$, which implies $\sigma(e^{2i\theta}) = r^4 e^{2i\theta}$. But, a conjugate of $e^{2i\theta}$ cannot have norm exceeding r^2 by Lemma 6.1. Thus, we have a contradiction. If $\sigma(\lambda) = \bar{\lambda}$, then compose with conjugation to achieve the previous contradiction. If $\sigma(\lambda) = 1/\lambda$, then, $1/r \cdot \sigma(e^{i\theta}) = \sigma(re^{i\theta}) = 1/r \cdot e^{-i\theta}$. Multiplication by $1/r$ yields $\sigma(e^{i\theta}) = e^{-i\theta}$. If $\sigma(\lambda) = 1/\bar{\lambda}$, then $1/r \cdot \sigma(e^{i\theta}) = \sigma(re^{i\theta}) = 1/r \cdot e^{i\theta}$. Canceling $1/r$ from both sides, we see $\sigma(e^{i\theta}) = e^{i\theta}$. Finally, if $\sigma(\lambda) = e^{i\phi}$, another similar argument shows $\sigma(e^{2i\theta}) = r^2 e^{2i\phi}$. But, the only possible conjugate of $e^{2i\theta}$ of norm r^2 is precisely the real number r^2 by Lemma 6.1. This implies that $e^{i\phi} = \pm 1$, which is a contradiction.

Case 2: $1/r$ is not a conjugate of r.

The proof of Proposition 1.5 shows that $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r)$. Then, $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) = \mathbb{Q}(r)$ if we show any automorphism sending $e^{i\theta}$ to $e^{\pm i\theta}$ fixes r. We can assume that $\sigma(e^{i\theta}) = e^{i\theta}$ because, otherwise, we may compose with conjugation. Using the assumption that $\sigma(e^{i\theta}) = e^{i\theta}$, we can show the following. If λ is sent to λ, $\bar{\lambda}$, $1/\lambda$, $1/\bar{\lambda}$, or $e^{i\phi}$, then we can conclude $\sigma(r) = r$, $\sigma(r^2) = r^2 e^{-4i\theta}$,

$\sigma(r^2) = 1/r^2 \cdot e^{-4i\theta}$, $\sigma(r) = 1/r$, or $\sigma(r) = e^{i(\phi-\theta)}$, respectively. By Lemma 6.1, the second and third possibility implies that $e^{i\theta}$ is a fourth root of unity. The fourth possibility directly implies that $1/r$ is a conjugate of r. Finally, the fifth possibility implies that $1/r$ is a conjugate of r by Lemma 7.7. Both of these possibilities cannot occur. Hence, r is fixed under σ. $\square$

6.2 Trace Fields of Degree 3

Thus far, the known results give us a fairly clear picture of how much a length of a geodesic determines the twist of a geodesic when the trace field is closed under complex conjugation. Naturally, one may ask what happens when the trace field is not closed under complex conjugation. Now, we will investigate a particularly manageable and enlightening case when the degree of the trace field is equal to 3.

Proposition 6.4 *Let k be a number field with one complex place. If $[k : \mathbb{Q}] = 3$, then $k \neq \bar{k}$.*

Proof: Suppose $k = \mathbb{Q}(\alpha)$. Let $\bar{\alpha} \in \mathbb{C}$ and $\beta \in \mathbb{R}$ be the conjugates of α. If $k = \bar{k}$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\bar{\alpha}) = \mathbb{Q}(\beta)$. This is impossible since $\mathbb{Q}(\beta) \subseteq \mathbb{R}$. $\square$

Furthermore, the Galois group of the Galois closure of a trace field with $[k : \mathbb{Q}] = 3$ is isomorphic to S_3. To see this fact, considering the following. The only other possibility is $\mathbb{Z}_3$ (see Chapter 14.6 of [5] for an explanation), which would imply that k is Galois. Although, if $G(N_k/\mathbb{Q}) \cong \mathbb{Z}_3$, then $k = \bar{k}$, which contradicts Proposition 6.25.

Proposition 6.5 *Let λ be a loxodromic eigenvalue where $[k : \mathbb{Q}] = m$. Then, $[N_\lambda : \mathbb{Q}] \leq 2^m m!$. Note that $k = \mathbb{Q}(\lambda + 1/\lambda)$. So, $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2m$.*

Proof: The Galois group of the closure of k has order at most $m!$. By Lemma 7.7, we know that if α is a conjugate of λ, then $1/\alpha$ is a conjugate of λ. Hence adjoining

α to the Galois closure of k adds at least two roots because fields are closed under division. $\square$

We can begin to see why this case is such an asset. All fields with exactly one complex place and degree equal to 3 are not closed under complex conjugation. This specific case will help us make conjectures about trace fields of any degree with $k \neq \bar{k}$. Now, we turn to PARI to aid the investigation. Pari will help us compute the Galois groups of polynomials. The Galois groups are a good starting point. When the trace field is closed under complex conjugation, the angle of the loxodromic eigenvalue was partially determined by certain Galois conjugates of $r^2 = \lambda \cdot \bar{\lambda}$.

Now, the reader may either assume that the minimal polynomial of a loxodromic eigenvalue must be palindromic, i.e., the i^{th} coefficient a_i equals the $(n-i)^{th}$ coefficient a_{n-i} where n is the degree of the polynomial and $0 \leq i \leq n$, or (s)he may look at Section 7.2 for an in-depth explanation of this fact. A census of polynomials of the form $x^6 + ax^5 + bx^4 + cx^3 + bx^2 + ax + 1$ where $|a|$, $|b|$, $|c| \leq 10$ was taken using PARI. Note that this polynomial is palindromic. First, all reducible polynomials were filtered out of the census. Then, all polynomials with at least one real root were filtered out of the census. All polynomials that remained were minimal polynomials of loxodromic eigenvalues (with the exception of any cyclotomic polynomials that were removed as well). An irreducible, palindromic polynomial of degree six with all complex roots must have at least one pair of conjugate roots with norm 1, since roots with norm not equal to 1 occur in quadruplets, i.e., α, $1/\alpha$, $\bar{\alpha}$, and $1/\bar{\alpha}$. By Proposition 4.17, all of the polynomials in the census are minimal polynomials of loxodromic eigenvalues. Furthermore, by Proposition 5.8 and Proposition 5.9, these are generic loxodromic eigenvalues.

By Proposition 6.5 and [3], the only possible Galois groups for the Galois closure of $\mathbb{Q}(\lambda)$ with trace fields of degree 3 are $\mathbb{Z}_6$, S_3, D_6, A_4, S_4, $A_4 \times \mathbb{Z}_2$, and $S_4 \times \mathbb{Z}_2$.

Multiple polynomials in the census had Galois group S_3, D_6, S_4, and $S_4 \times \mathbb{Z}_2$. Using group theoretic arguments, one can show that $\mathbb{Z}_6$, A_4, and $A_4 \times \mathbb{Z}_2$ cannot occur as Galois groups of loxodromic eigenvalues. By the comment after Proposition 6.25, the trace field of a degree 3 extension must have Galois group that is isomorphic to S_3. This would require $\mathbb{Z}_6$, A_4, and $A_4 \times \mathbb{Z}_2$ to have normal subgroups whose quotient is isomorphic to S_3, which is not the case. A quotient of an abelian group is abelian, so $\mathbb{Z}_6$ is impossible. A_4 is impossible because it has no normal subgroups of order 2. Finally $A_4 \times \mathbb{Z}_2$ is impossible because mod-ing out by a normal subgroup must annihilate the $\mathbb{Z}_2$ factor, but again A_4 has no normal subgroup of order 2.

This section deals with the enumeration of the Galois groups of loxodromic eigenvalues that arise from trace fields of degree 3. The possible Galois groups are isomorphic to S_3, D_6, S_4, and $S_4 \times \mathbb{Z}_2$. First of all, recall that a loxodromic eigenvalue that arises from a trace field of degree 3 has a degree of 6. Furthermore, $\lambda = re^{i\theta}$ has conjugates λ, $1/\lambda$, $\bar{\lambda}$, $1/\bar{\lambda}$, $e = e^{i\phi}$, and $1/e = e^{-i\phi}$. The motivation for the discussion that follows is that Theorem 1.7 is stated in terms of the degree of r^2 and Theorem 1.8 is stated in terms of the Galois group of N_{r^2}. We will eventually use Theorem 1.8 to prove Theorem 1.7 as a corollary, but we need to establish a correspondence between the degree of r^2 and the Galois group of N_{r^2} in order to translate a statement about the Galois group of N_{r^2} into a statement about the degree of r^2.

Group 1: $S_4 \times \mathbb{Z}_2$

When the Galois group is $S_4 \times \mathbb{Z}_2$, any map that preserves the relation $\sigma(1/z) = 1/\sigma(z)$ is valid. This follows from simple counting principles. There are 6 choices for λ. Once you decide where λ maps, then the image of $1/\lambda$ is determined. Then, there are 4 choices for $\bar{\lambda}$. Once you decide where $\bar{\lambda}$ maps, then the image of $1/\bar{\lambda}$ is determined. Finally, there are 2 choices for e. Once you decide where e maps, then the image of $1/e$ is determined. Furthermore, $6 \cdot 4 \cdot 2 = 48$, which is the order of $S_4 \times \mathbb{Z}_2$. Therefore, any valid map is an element of $S_4 \times \mathbb{Z}_2$.

Then, the degree of r^2 in this case is 12 because $r^2 = \lambda\bar{\lambda}$, the images of λ and $\bar{\lambda}$ are independent of each other, and this gives us $6 \cdot 4/2 = 12$ conjugates. Thus, the conjugates (reciprocals are not listed) of r^2 are $r^2, e^{2i\theta}, \lambda e^{i\phi}, \lambda e^{-i\phi}, \bar{\lambda} e^{i\phi}$, and $\bar{\lambda} e^{-i\phi}$. Hence, $[\mathbb{Q}(r^2) : \mathbb{Q}] = [\mathbb{Q}(e^{2i\theta}) : \mathbb{Q}] = 12$. Notice that r^2 and $e^{2i\theta}$ share the same minimal polynomial over $\mathbb{Q}$. Thus by Proposition 5.4, $|\lambda|$ has a unique argument.

Group 2: S_4

While it is possible to enumerate all the elements of S_4, this is tedious and the motivation is to determine the conjugates of r^2. This can be avoided by showing that the degree of r^2 is 12. Also, note that r^2 can have at most 12 conjugates from the description of the Galois group when it is isomorphic to $S_4 \times \mathbb{Z}_2$. This case requires the most ingenuity to discovering the conjugates of r^2. The key idea is that the group of all valid maps from the set of conjugates to itself is isomorphic to $S_4 \times \mathbb{Z}_2$. What we need to do is sift through these elements and only select those that are contained in S_4. Note that there is only one subgroup of $S_4 \times \mathbb{Z}_2$ that is isomorphic to S_4. A convenient fact is that $S_4 \times \mathbb{Z}_2$ contains a nontrivial center. So, our approach is either an element of $S_4 \times \mathbb{Z}_2$ is contained within S_4, or if not, maybe we can find the only nontrivial element of the center of $S_4 \times \mathbb{Z}_2$, then the product of this nontrivial element and the element not contained in $S_4 \times \mathbb{Z}_2$ is contained in $S_4 \times \mathbb{Z}_2$.

The element of order two in the center is the map $\sigma : z \mapsto 1/z$ where z is any conjugate of λ. Notice this is true because if we have an automorphism $\tau : x \mapsto y$, then

$$(\sigma \circ \tau)(x) = \sigma(y) = 1/y$$

and

$$(\tau \circ \sigma)(x) = \tau(1/x) = 1/\tau(x) = 1/y$$

Therefore, $z \mapsto 1/z$ is the element of order two in the center of $S_4 \times \mathbb{Z}_2$. Now, consider an element, τ, of $S_4 \times \mathbb{Z}_2$ that maps λ to x and $\bar{\lambda}$ to y. By a previous argument, we may choose x and y to be any distinct conjugates. If τ is an element of the subgroup S_4, then xy is a conjugate of $r^2 = \lambda\bar{\lambda}$. However, if τ is not an element of S_4, then we may represent it as a product of τ' that lies in S_4 and σ the element of order two in the center. Post-composing with σ yields an element of S_4 such that λ maps to $1/x$ and $\bar{\lambda}$ maps to $1/y$. So, r^2 maps to $1/xy$. Therefore, for all possible conjugates of r^2 either xy or $1/xy$ is a conjugate. However, recall that $e^{2i\theta}$ is a possible conjugate. So, this says that r^2 has at least six conjugates with no two being reciprocals of one another and either $e^{2i\theta}$ or $e^{-2i\theta}$ is one of the six conjugates. By Lemma 7.7, we know that if r^2 has a conjugate of norm 1, then all reciprocals of roots are also roots. This implies that the degree of r^2 is 12, which means r^2 has the maximum number of conjugates.

The conjugates (reciprocals are not listed) of r^2 are $r^2, e^{2i\theta}, \lambda e^{i\phi}, \lambda e^{-i\phi}, \bar{\lambda}e^{i\phi}$, and $\bar{\lambda}e^{-i\phi}$. Hence, $[\mathbb{Q}(r^2) : \mathbb{Q}] = [\mathbb{Q}(e^{2i\theta}) : \mathbb{Q}] = 12$. Notice that r^2 and $e^{2i\theta}$ share the same minimal polynomial over $\mathbb{Q}$. Thus by Proposition 5.4, $|\lambda|$ has a unique argument.

Group 3: $D_6 \cong \mathbb{Z}_6 \rtimes \mathbb{Z}_2$

An explicit set of maps for the Galois group D_6 must respect the set of rigid isometries of a regular hexagon. So, we must label the vertices of a hexagon in such a way that respects: $\sigma(1/z) = 1/\sigma(z)$. First, the hexagon must be labeled such that z and $1/z$ are on opposite corners of the hexagon. Otherwise, there would exist a map that fixed z and did not fix $1/z$. To see this, look at the isometry that reflects about the line between the vertex labeled z vertex and the vertex opposite z, which we have assumed is not labeled $1/z$. Second, complex conjugation is an element of order 2 that does not fix any of the conjugates since they are all non-real. The rotation of order 2 cannot be complex conjugation because we have already labeled the opposite vertex to z as $1/z$. This means that conjugation has to be a reflection that moves all the vertices. Therefore, λ has to be adjacent to $\bar{\lambda}$. The remaining two vertices must be labeled e and $1/e$. These two requirements uniquely determine the labeling up to a rigid isometry of the hexagon. One such reading of the vertices in a counter-clockwise fashion yields the following list: λ, e, $1/\bar{\lambda}$, $1/\lambda$, $1/e$, and $\bar{\lambda}$.

By looking at the images of λ and $\bar{\lambda}$ under the same element of the Galois group, we can determine that the conjugates of r^2 are $r^2, 1/r^2, 1/\lambda\cdot e^{i\phi}, 1/\bar{\lambda}\cdot e^{-i\phi}, \lambda e^{-i\phi}$, and $\bar{\lambda}e^{i\phi}$. Hence, $[\mathbb{Q}(r^2):\mathbb{Q}] = 6$. The conjugates of $e^{2i\theta}$ are $e^{2i\theta}, e^{-2i\theta}, 1/\lambda\cdot e^{-i\phi}, 1/\bar{\lambda}\cdot e^{-i\phi}, \lambda e^{i\phi}$, and $\bar{\lambda}e^{-i\phi}$. Hence, $[\mathbb{Q}(e^{2i\theta}):\mathbb{Q}] = 6$. Notice that $e^{2i\theta}$ is a conjugate of another loxodromic eigenvalue with the same norm. At this point, we have found a criterion that allows for non-unique angles.

Group 4: S_3

Now, we will explicitly enumerate the elements of the Galois group when it is S_3. Note in this case the element of the Galois group is entirely determined by the image of any conjugate of λ because $[\mathbb{Q}(\lambda):\mathbb{Q}] = 6$, which is the order of S_3. So, $\mathbb{Q}(\lambda)$ is a Galois extension of $\mathbb{Q}$, and, furthermore, $\mathbb{Q}(z)$ is equal to $\mathbb{Q}(\lambda)$ where z is any conjugate of λ. An explicit set of maps for the Galois group S_3 must include the identity permutation and conjugation represented as $(\lambda,\bar{\lambda})(1/\lambda,1/\bar{\lambda})(e,1/e)$. Also, there must be a permutation, σ, that transposes λ and $1/\lambda$. This permutation must have order 2 because the order of a permutation is the least common multiple of the length of the cycles when written as disjoint cycles and no element of S_3 has order 6 or order 4. Furthermore, σ cannot send e to $1/e$ because conjugation already does that. So, we have $(\lambda, 1/\lambda)(\bar{\lambda}, e)(1/\bar{\lambda}, 1/e)$. Note that there is some ambiguity here. Does $\bar{\lambda} \mapsto e$ or does $\bar{\lambda} \mapsto 1/e$? To resolve this, we realize that one of the two has to occur. If the second occurs rename $1/e$ as e and rename e as $1/e$. Composing with conjugation yields a new element: $(\lambda, 1/\bar{\lambda}, e)(1/\lambda, \bar{\lambda}, 1/e)$, which has order 3. By composing the element of order 3 with itself, we get the following permutation: $(\lambda, e, 1/\bar{\lambda})(1/\lambda, 1/e, \bar{\lambda})$. Finally, composing the previous element with conjugation yields $(\lambda, 1/e)(1/\lambda, e)(\bar{\lambda}, 1/\bar{\lambda})$.

By looking at the images of λ and $\bar{\lambda}$ under the same element of the Galois group, we can determine that the conjugates of r^2 are $r^2, 1/\lambda \cdot e^{i\phi}$, and $1/\bar{\lambda} \cdot e^{-i\phi}$. Hence, $[\mathbb{Q}(r^2) : \mathbb{Q}] = 3$. The conjugates of $e^{2i\theta}$ are $e^{2i\theta}, e^{-2i\theta}, 1/\lambda \cdot e^{-i\phi}, 1/\bar{\lambda} \cdot e^{-i\phi}, \lambda e^{i\phi}$, and $\bar{\lambda} e^{-i\phi}$. Hence, $[\mathbb{Q}(e^{2i\theta}) : \mathbb{Q}] = 6$. Again, notice that $e^{2i\theta}$ is a conjugate of another loxodromic eigenvalue.

Now, we know that the only Galois groups that might impede the uniqueness of the angle are S_3 and D_6. An interesting feature about these groups is that, while r^2 and $e^{2i\theta}$ are not Galois conjugates, $e^{2i\theta}$ is a Galois conjugate of a loxodromic eigenvalue. This is a special feature of degree 3 trace fields. Further investigation produced two loxodromic eigenvalues with equal norms but different minimal polynomials: $x^6 + 3x^5 + 3x^4 - 10x^3 + 3x^2 + 3x + 1$ and $x^6 + 6x^5 + 12x^4 + 10x^3 + 12x^2 + 6x + 1$. Computations suggested that the second eigenvalue was obtained by multiplying the first eigenvalue by a sixth root of unity. Now, we have a possible characterization when the length of a geodesic does not uniquely determine the angle. In the next section, we will see that if $\mathbb{Q}(\lambda)$ contains nontrivial roots of unity, then the angle is not unique.

6.3 Roots of Unity

In this section, we prove:

Theorem 1.6 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ_1 and γ_2 in Kleinian groups Γ_1 and Γ_2 derived from a quaternion algebra A/k. If $\lambda_1 = re^{i\theta_1}$, $\lambda_2 = re^{i\theta_2}$, and $\lambda_1 \neq \pm\bar{\lambda}_2$, then λ_1/λ_2 is a root of unity.*

Now we return to the question, when is the angle of a loxodromic eigenvalue not uniquely determined? As hinted at before and the title of this section it has precisely to do with roots of unity. That is, if the field generated by a loxodromic eigenvalue contains nontrivial roots of unity, then the angle of the loxodromic eigenvalue is not unique. First, we give a useful result of Kronecker [22] from [12] and a lower bound for Euler's totient function from [11], where $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Theorem 6.6 *(**Kronecker, 1857**) Let $\alpha \neq 0$ be an algebraic integer. Then, α is a root of unity if and only if all conjugates of α have norm at most* 1.

Theorem 6.7 *Let ϕ be Euler's totient function. Then, $\phi(n) \geq \sqrt{n}$ for $n \neq 2, 6$.*

The following proposition is a standard result that can be found in [5].

Proposition 6.8 *Let μ be an n^{th} root of unity. Then, the degree of the minimal polynomial of μ is $\phi(n)$.*

Remark 6.9 *There are only finitely many roots of unity in any number field. This follows from the previous proposition and theorem along with the fact that the degree of a subfield of a number field divides the degree of the number field.*

Proof of Theorem 1.6: We do not need to worry about the case where $k = \bar{k}$ because Corollary 5.6 shows that $\lambda_1 = \pm\lambda_2$ or $\lambda_1 = \pm\bar{\lambda}_2$ for generic loxodromic eigenvalues and λ_1/λ_2 is a root of unity for non-generic loxodromic eigenvalues. Furthermore, if $\lambda_1 \neq \pm\bar{\lambda}_2$, then, by the contrapositive of part 1) of Proposition 5.4, we know that $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_2)$. Note that we are assuming that the trace fields are the same, i.e., $\mathbb{Q}(\lambda_1 + 1/\lambda_1) = \mathbb{Q}(\lambda_2 + 1/\lambda_2)$.

Therefore, we have the following quadratic field extension

$$\begin{array}{c} \mathbb{Q}(\lambda_1) = L = \mathbb{Q}(\lambda_2) \\ \Big| \\ \mathbb{Q}(\lambda_1 + 1/\lambda_1) = k = \mathbb{Q}(\lambda_2 + 1/\lambda_2) \end{array}$$

We need to show that for any $\sigma \in G(N_{\lambda_1}/\mathbb{Q})$, $|\sigma(\lambda_1)| = |\sigma(\lambda_2)|$. Then, the norm of any conjugate of λ_1/λ_2 is 1, and, by a result of Kronecker, λ_1/λ_2 is a root of unity. Let $\sigma \in G(N_{\lambda_1}/\mathbb{Q})$. Recall that part $3i$) of Theorem 4.16 states that the only conjugates of λ that are not on the unit circle are $\lambda, \bar{\lambda}, 1/\lambda$, and $1/\bar{\lambda}$.

Case 1: Suppose $\sigma(\lambda_1) = \lambda_1$. Then, σ is the identity map on $\mathbb{Q}(\lambda_1)$, which equals $\mathbb{Q}(\lambda_2)$. So, σ is the identity map on $\mathbb{Q}(\lambda_2)$, and, thus, $\sigma(\lambda_2) = \lambda_2$.

Case 2: Suppose $\sigma(\lambda_1) = 1/\lambda_1$. Then, $\sigma(1/\lambda_1) = \lambda_1$, which implies σ fixes $Q(\lambda_1 + 1/\lambda_1)$, but σ does not fix $\mathbb{Q}(\lambda_1)$. Due to the equalities mentioned above, σ fixes $\mathbb{Q}(\lambda_2 + 1/\lambda_2)$, but σ does not fix $\mathbb{Q}(\lambda_2)$. Since the field extension is degree 2, $\sigma(\lambda_2) = 1/\lambda_2$.

Case 3: Suppose $\sigma(\lambda_1) = \bar{\lambda}_1$. Then, this map is complex conjugation. So, $\sigma(\lambda_2) = \bar{\lambda}_2$.

Case 4: Suppose $\sigma(\lambda_1) = 1/\bar{\lambda}_1$, but $\sigma(\lambda_2) \neq 1/\bar{\lambda}_2$. Composing with complex conjugation yields $\sigma(\lambda_1) = 1/\lambda_1$ and $\sigma(\lambda_2) \neq 1/\lambda_2$, which contradicts Case 2.

Therefore, $\sigma(\lambda_1) = \lambda_1 \Leftrightarrow \sigma(\lambda_2) = \lambda_2$, $\sigma(\lambda_1) = 1/\lambda_1 \Leftrightarrow \sigma(\lambda_2) = 1/\lambda_2$, $\sigma(\lambda_1) = \bar{\lambda}_1 \Leftrightarrow \sigma(\lambda_2) = \bar{\lambda}_2$, and $\sigma(\lambda_1) = 1/\bar{\lambda}_1 \Leftrightarrow \sigma(\lambda_2) = 1/\bar{\lambda}_2$. The only case left to consider is if $\sigma(\lambda_1)$ lies on the unit circle. However, by the four cases above, this implies that $\sigma(\lambda_2)$ also lies on the unit circle. Hence, $|\sigma(\lambda_1)| = |\sigma(\lambda_2)|$. $\square$

Now that we have proved Theorem 1.6, we see that roots of unity play an important role when the angle of a loxodromic eigenvalue is not unique. Recall that Theorem 1.7 and Theorem 1.8 deal with invariant trace fields of prime degree. A question that arises is "what roots of unity, μ, make $k(\mu)$ a quadratic extension of k?" First, we require Lemma 6.10, but after we have Corollary 6.11, which answers this question.

Lemma 6.10 *Let k be a number field with exactly one complex place with $[k : \mathbb{Q}] \neq 2$ (or equivalently k has at least one real embedding). If L is a quadratic extension of k that contains a nontrivial root of unity, then $\mu \notin k$ and $\mu + 1/\mu \in k$.*

Proof: All conjugates of a non-trivial root of unity are not real, and all conjugates of $\mu + 1/\mu \,(= \mu + \bar{\mu})$ are real. Therefore, since k has a real embedding $\mu \notin k$. This implies that $L = k(\mu)$ where μ is a non-trivial root of unity. The minimal polynomial of μ over k must be a degree 2 polynomial with the following form: $x^2-(\mu+\alpha)x+\mu\cdot\alpha$ where α is a conjugate of μ (and, thus, a root of unity) and $\mu + \alpha$, $\mu \cdot \alpha \in k$.

Claim: $\alpha = 1/\mu$

Note that $\alpha = \pm 1/\mu$, since $\mu \cdot \alpha \in k$ has a real embedding and the only real roots of unity are ± 1. Suppose $\alpha = -1/\mu$. Consider the image of μ under τ, a real embedding of k, in which $\tau(\mu - 1/\mu)$ is necessarily real number. Then,

$$\tau(\mu - 1/\mu) = \tau(\mu) - 1/\tau(\mu) = \tau(\mu) - \overline{\tau(\mu)}$$

Note that since the conjugate of a root of unity is a root of unity, $\tau(\mu)$ is a root of unity, and, furthermore, the complex-conjugate of $\tau(\mu)$ is $1/\tau(\mu)$. Now consider $z - \bar{z}$ where z is a complex number. If $z = x + iy$ with $x, y \in \mathbb{R}$, then $\bar{z} = x - iy$. So, $z - \bar{z} = 2iy$. Thus, the difference of a complex number and its conjugate is real if and only if $y = 0$. Therefore, the imaginary part of $\tau(\mu)$ must be zero, which implies $\tau(\mu) = \pm 1$. The only conjugates of ± 1 is ± 1. Therefore, this implies that $\mu = \pm 1$. However, this would contradict the fact that μ is a non-trivial root of unity. Therefore, $\alpha = 1/\mu$.

Therefore, the minimal polynomial of μ over k is $x^2 - (\mu + 1/\mu)x + 1$, which implies $\mu + 1/\mu \in k$. □

Corollary 6.11 *Let $k/\mathbb{Q}$ be a field with exactly one complex place. If $[k : \mathbb{Q}] = p \neq 2$, where p is a prime. Then, λ_1/λ_2 is 1, -1, a primitive third root of unity, a primitive fourth root of unity, or a primitive sixth root of unity.*

We have the following field extension diagram where $L = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_2)$:

$$\begin{array}{c} L \\ \Big| {\scriptstyle 2} \\ k \\ \Big| {\scriptstyle p} \\ \mathbb{Q} \end{array}$$

Proof: Let μ be a non-trivial root of unity. Then, $\mu + 1/\mu = \mu + \bar{\mu}$ is a real number with only real conjugates. This is because for a complex number $z = x + iy$, $z + \bar{z} = 2x$, which is clearly a real number. Furthermore, any conjugate of $\mu + 1/\mu$ is a real number because any embedding of μ sends this number to $\tau(\mu) + 1/\tau(\mu)$, which is a sum of complex conjugates and so is real as well. Therefore, if k has a complex embedding, $[k:\mathbb{Q}] = p$ where p is prime, and $\mu + 1/\mu \in k$, then $\mu + 1/\mu$ must lie in a proper subfield of k. Since the only proper subfield of k is $\mathbb{Q}$, $\mu + 1/\mu \in \mathbb{Q}$. The only such roots of unity, μ, such that $\mu + 1/\mu \in \mathbb{Q}$ are 1, -1, the primitive third roots of unity, the primitive fourth roots of unity, and the primitive sixth roots of unity. $\square$

Remark 6.12 *Now that we have Corollary 6.11 above, it is worth noting what quadratic fields contain the fourth and sixth roots of unity. The former is clearly contained in $\mathbb{Q}(\sqrt{-1})$, since $i := \sqrt{-1}$ is a generator for the fourth roots of unity. The latter is contained in $\mathbb{Q}(\sqrt{-3})$. To see this, a generator for the third roots of unity is $e^{2\pi i/3} = cos(2\pi i/3) + isin(2\pi i/3) = -1/2 + i\sqrt{3}/2 = -1/2 + \sqrt{-3}/2$. Therefore, $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$. Furthermore, $-e^{2\pi i/3}$ is a primitive sixth root of unity contained in $\mathbb{Q}(\sqrt{-3})$.*

Up to this point, we see that what may obstruct the equivalence of real length isospectrality and complex length isospectrality is the appearance of roots of unity. While adjoining primitive third and fourth roots of unity to any trace field yields a degree 2 extension that contains a loxodromic eigenvalue, we still need to know if multiplication of a loxodromic eigenvalue by a root of unity yields another loxodromic eigenvalue. The following proposition answers that question.

Proposition 6.13 *Let λ be a generic loxodromic eigenvalue with conjugates λ, $1/\lambda$, $\bar{\lambda}$, $1/\bar{\lambda}$ and $e^{\pm i\phi_k}$ for $k = 1, \ldots, n$, and suppose $[k:\mathbb{Q}] > 2$. Then, for every root of unity $\mu \in \mathbb{Q}(\lambda)$, $\lambda\mu$ is a generic loxodromic eigenvalue with conjugates $\lambda\mu$, $1/\lambda\mu$, $\bar{\lambda}\bar{\mu}$, $1/\bar{\lambda}\bar{\mu}$ and $e^{\pm i\tau_j}$ for $j = 1, \ldots, n$*

Proof: Lemma 6.10 shows $\mu + 1/\mu \in k$ and $\mu \notin k$. Now, we need to ensure that the only conjugates of $\lambda\mu$ with norm not equal to 1 are $\lambda\mu$, $1/\lambda\mu$, $\bar{\lambda}\bar{\mu}$, and $1/\bar{\lambda}\bar{\mu}$. Let $\sigma \in G(N_\lambda/\mathbb{Q})$. If σ fixes λ, then σ also fixes μ. Also, if $\sigma(\lambda) = 1/\lambda$, then σ

restricted to $k(\lambda)$ is an element of $G(k(\lambda)/k)$. Since $\mu \notin k$, σ does not fix μ. The only other possibility is that σ sends μ to $1/\mu$. Also, since λ has a conjugate of norm 1 and all conjugates of μ have norm 1, it follows that $\lambda\mu$ has a conjugate of norm 1. Suppose $\lambda\mu$ has a conjugate with norm not equal to 1 that is different from the four possibilities above, i.e., a conjugate such as $\lambda\mu'$,$\bar{\lambda}\bar{\mu}'$, $1/\lambda\mu'$, or $1/\bar{\lambda}\bar{\mu}'$. We refer to this list as (1). Since λ has a conjugate with norm equal to 1, its minimal polynomial is palindromic by Lemma 7.7. If λ is conjugate to any of (1), then it is conjugate to all of them. So we may suppose that $\sigma(\lambda\mu) = \lambda\mu^{'}$ for some embedding σ.

Claim: $\sigma(\lambda) = \lambda$

Note that σ must send λ to a conjugate and that σ must send μ to another root of unity. Since $|\sigma(\lambda\mu)| = r$, by Theorem 4.16 part 3 i) the image of λ must be λ or $\bar{\lambda}$. If the image of λ is $\bar{\lambda}$, then

$$\lambda\mu' = \sigma(\lambda\mu) = \sigma(\lambda) \cdot \sigma(\mu) = \bar{\lambda} \cdot \sigma(\mu) = \lambda \cdot \frac{\bar{\lambda}}{\lambda} \cdot \sigma(\mu) = \lambda \cdot e^{2i\theta} \cdot \sigma(\mu)$$

Using the ends of the equalities above and dividing each side by λ implies $\mu/\sigma(\mu) = e^{2i\theta}$. Conjugates of roots of unity are roots of unity, and the roots of unity form a group under multiplication. So, this implies that $\mu/\sigma(\mu)$ is a root of unity, but this is a contradiction because λ is a generic loxodromic eigenvalue. Therefore, σ must send λ to λ.

Finally, notice $\lambda\mu \notin k$, since $\lambda\mu$ has at least four non-real conjugates which would exclude it from being contained in a field with exactly one complex place. So, $\lambda\mu$ is a loxodromic eigenvalue necessarily over the same quaternion algebras as λ. $\square$

Now, a natural question is which roots of unity may appear over a particular trace field, and, more generally, under what circumstances does a quadratic extension of a trace field contain a loxodromic eigenvalue? These question will be answered by Corollary 6.17 and Proposition 6.16, respectively. The following is a result from *Chapter 12* of [16] that we require to answer the aforementioned questions.

Theorem 6.14 *Let Γ be a Kleinian group derived from a quaternion algebra A/k. Then, L embeds in A if and only if Γ contains an element γ of infinite order such that $L = k(\lambda)$ where λ is an eigenvalue of γ.*

The following theorem is a restatement of Theorem 3.52 in language relevant to our setting. As a result, we restate it here.

Theorem 6.15 *Suppose that Γ is derived from a quaternion algebra A/k and γ is a loxodromic element of Γ with eigenvalue λ. Then, a quadratic extension, L, of k embeds in A/k if and only if no place of k which splits in L is ramified in A/k.*

Note that there are other equivalent conditions (see Theorem 3.52) to having a quadratic extension of k embed in a quaternion algebra over k, but we prefer the equivalent statement in terms of places of a number field.

Proposition 6.16 *If L is a quadratic extension of a number field, k with exactly one complex place, has no real embeddings, then L contains a loxodromic eigenvalue.*

Proof: By Theorem 6.15, L embeds into a quaternion algebra A/k if and only if no place of k which splits in L is ramified in A. Quaternion algebras that occur as the invariant quaternion algebra of some Kleinian group are ramified at all real places of k. If L has no real places, then no infinite place of k splits in L. Now, by the classification of quaternion algebras we may choose $Ram_f A = \varnothing$. By Theorem 4.18, we know that L embeds in A if and only if there exists a Kleinian group Γ and an element $\gamma \in \Gamma$ such that $L = k(\lambda_\gamma)$. $\square$

While we can choose $Ram_f A = \varnothing$, using the Chebotarev density Theorem, we could find an appropriate number of primes of k that do not split in L to put into $Ram_f A$ so that $Ram A$ is even.

Corollary 6.17 *Let k be a number field with exactly one complex place. Suppose that $\mu + 1/\mu \in k$ where μ is a nontrivial root of unity. Then, $k(\mu)$ contains a loxodromic eigenvalue of some Kleinian group Γ derived from some quaternion algebra over k.*

Proof: Since $\mu + 1/\mu \in k$ and k has exactly one complex place, $\mu \notin k$. Furthermore, $x^2 + (\mu + 1/\mu)\, x + 1$ is the minimal polynomial of μ over k. Therefore, $[k(\mu) : k] = 2$. Also, μ has no real embeddings. So, all embeddings of $k(\mu)$ are non-real. $\square$

Let μ be a primitive third, fourth, or sixth root of unity. Then, taking any number field, k, with exactly one complex place such that $k \neq \bar{k}$ and adjoining μ yields a number field that contains a generic loxodromic eigenvalue, by Corollary 6.17, and also a nontrivial root of unity. Furthermore, the product of that loxodromic eigenvalue with the nontrivial root of unity yields a loxodromic eigenvalue with equal norm but different angle by Proposition 6.13. One tangential question is "does the angle of a generic loxodromic eigenvalue completely determine the norm?" The answers to these questions can be found in Section 7.1.

We have investigated the problem of finding loxodromic elements with equal norms but unequal angles quite thoroughly. However, one question that remains is the following: for every root of unity, does there exist a trace field such that adjoining the root of unity results in a quadratic extension? This will be answered later after we are in need of a result from Chapter 12 of [16] that will help us with a completely separate result. But, now we return to the degree 3 case and more generally the degree p case where p is a prime number not equal to 2 in lieu of the results of this section.

6.4 Back to Degree 3 and Onward to Degree p

In this section, we prove the following theorems:

Theorem 1.7 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in an arithmetic Kleinian group derived from a quaternion algebra A/k over a number field k with $[k : \mathbb{Q}] = 3$. Suppose that the discriminant of the trace field is $-d$, where $d > 0$ is a square-free integer. Then, the only possibilities for the degree of r^2 are 3, 6, and 12.*

> *i) If $[\mathbb{Q}(r^2) : \mathbb{Q}] = 12$, then the angle of a loxodromic eigenvalue with norm r is unique.*
>
> *ii) Suppose $[\mathbb{Q}(r^2) : \mathbb{Q}] = 3$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $d \neq 1, 3$.*
>
> *iii) Suppose $[\mathbb{Q}(r^2) : \mathbb{Q}] = 6$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $\mathbb{Q}(r^2)$ does not contain $\sqrt{d}$ (if $d \neq 1$) or $\sqrt{3d}$.*

Theorem 1.8 *Let $r = |\lambda|$ be the norm of a loxodromic eigenvalue from an element γ in a Kleinian group derived from a quaternion algebra A/k with $[k : \mathbb{Q}] = p$ where p is a prime not equal to 2. Then, there is a unique quadratic extension contained in the Galois closure of the trace field. If the quadratic extension is $\mathbb{Q}(\sqrt{-d})$, where $d > 0$ is a square-free integer.*

> *i) If the Galois group of N_{r^2} is not isomorphic to S_p or $S_p \times \mathbb{Z}_2$, then the angle is unique.*
>
> *ii) If the Galois group of N_{r^2} is isomorphic to S_p. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if $d \neq 1, 3$.*

iii) If the Galois group of N_{r^2} is isomorphic to $S_p \times \mathbb{Z}_2$. Then, the angle of a loxodromic eigenvalue with norm r is unique if and only if the Galois closure of r^2 does not contain $\sqrt{d}$ (if $d \neq 1$) or $\sqrt{3d}$.

Now, the question may arise as to why S_p plays such an important role in the Galois groups over trace fields of degree p. The answer is that the Galois group of a trace field of prime degree p is isomorphic to the symmetric group on p objects. But, first, we state Cauchy's Theorem, which may be found in [5].

Theorem 6.18 *(Cauchy's Theorem)If G is a finite group and p is a prime dividing the order of G, then G has an element of order p.*

Just as a reminder, N_k refers to the Galois closure (or Galois closure) of k.

Proposition 6.19 *Suppose that k is a number field with exactly one complex place with $[k : \mathbb{Q}] = p$ a prime number. Then, $G(N_k/\mathbb{Q}) \cong S_p$.*

Proof: Conjugation is a nontrivial automorphism of N_k. Since k has exactly one complex place, conjugation is a transposition that swaps k and $\bar{k}$ and fixes all other fields isomorphic to k. Since $[k : \mathbb{Q}]$ is a prime number, the order of $G(N_k/\mathbb{Q})$ is divisible by p. By Cauchy's theorem, there exists an element of $G(N_k/\mathbb{Q})$ that has order p. Furthermore, since the Galois group permutes the p roots of a minimal polynomial defining k, the Galois group injects into S_p. An element of order p in S_p is a p-cycle. A generating set for S_n is $(x_1\ x_2)$ and $(x_1\ x_2\ x_3\ \ldots\ x_n)$. Without loss of generality, we may assume that conjugation is represented by $(x_1\ x_2)$. Also, by taking an appropriate power of our p-cycle, we can find another p-cycle in which x_1 is sent to x_2. So, conjugation and the p-cycle generate a group isomorphic to S_p. $\square$

We will actually prove Theorem 1.8 first, then we prove Theorem 1.7 as a corollary. From Theorem 1.6, we know that when the angles of loxodromic eigenvalues of equal norm are not equal, their quotient is a root of unity. Furthermore, by Proposition 6.13, we know that λ has a unique angle precisely when $\mathbb{Q}(\lambda)$ does not contain nontrivial roots of unity. We will start by characterizing when the Galois closure of r^2 contains a nontrivial root of unity. Then we apply the following proposition (Proposition 6.20), which relates the Galois closure of r^2 to the Galois closure of $\lambda = re^{i\theta}$. The result that gives us these two field are equal is Proposition 4.4 from [4]. Proposition 6.20 follows from Proposition 4.4 of [4].

Proposition 6.20 *If λ is a generic loxodromic eigenvalue, then the Galois closure of r^2, N_{r^2}, is equal to the Galois closure of λ, N_λ.*

Corollary 6.21 *If $k \neq \bar{k}$, then the Galois closure of r^2, N_{r^2}, is equal to the Galois closure of λ, N_λ.*

Proof: Recall that Proposition 5.9 tells us that $k \neq \bar{k}$ if and only if $[k : k \cap \mathbb{R}] > 2$ and Proposition 5.8 tells us that if $[k : k \cap \mathbb{R}] > 2$, then the underlying Kleinian group cannot contain hyperbolic elements. Therefore, all loxodromic eigenvalues are generic. $\square$

So, the approach will be to first narrow down to the Galois closures of r^2, or rather the Galois closures of λ by the above proposition, that contain a nontrivial root of unity. The Galois closure of r^2 contains the trace field k. So, if it also contains a nontrivial root of unity, then $k(\mu)$ is contained in the Galois closure of r^2 and by Corollary 6.17 this field contains a loxodromic eigenvalue and by Proposition 6.13 the angle is not unique. Now, we need a result from [5].

Proposition 6.22 *The Galois group of a number field with degree n is contained in A_n if and only if the discriminant of the number field is a square in $\mathbb{Q}$. If the Galois group is isomorphic to the S_n, then $\mathbb{Q}(\sqrt{D})$ is the unique quadratic extension of $\mathbb{Q}$*

contained in the Galois closure of the number field, where D is the discriminant of the number field.

Note that the uniqueness of $\mathbb{Q}(\sqrt{D})$ follows from the correspondence from the fundamental theorem of Galois theory provided by the fact that S_n has only one group of index two, A_n.

Proposition 6.23 *Let K_1 and K_2 be Galois extensions of a field F. Then,*

i) The composite K_1K_2 is a Galois extension of $K_1 \cap K_2$.

ii) The Galois group of K_1K_2/F is isomorphic to

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

where σ and τ are elements of the Galois group of K_1 and K_2 respectively.

iii) Furthermore, if $K_1 \cap K_2 = F$, then $G(K_1K_2/F) \cong G(K_1/F) \times G(K_2/F)$ where the isomorphism is specified by $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$.

Proof of Theorem 1.8 Now, the question arises: "why do we only need to consider Galois groups isomorphic to S_p or $S_p \times \mathbb{Z}_2$?" The Galois closure of a loxodromic eigenvalue contains the Galois closure of the trace field. Furthermore, we know that nontrivial roots of unity create angles that are not unique and by Remark 6.11 we know that the only possible roots of unity that may appear are fourth and sixth roots of unity. The fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ contain the fourth and sixth roots of unity. Let n be a square-free integer. The composite of N_k and $\mathbb{Q}(\sqrt{n})$ is a Galois extension because the composite of two Galois extensions is a Galois extension of their intersection (see Proposition 6.23 below from [5]). Either the intersection of the two fields is $\mathbb{Q}(\sqrt{n})$ in which case the Galois group is the Galois group of N_k, which is isomorphic

S_p under our assumptions, or the intersection is $\mathbb{Q}$ in which case the Galois group is the direct product of Galois groups of each field, which is isomorphic to $S_p \times \mathbb{Z}_2$.

Along the way, we will prove the following claims that will aid us in the proof.

a) If $G(N_\lambda/\mathbb{Q}) \cong S_p$, then $G(N_\lambda/k) \cong S_{p-1}$.

b) If $G(N_\lambda/\mathbb{Q}) \cong S_p \times \mathbb{Z}_2$, then $G(N_\lambda/k) \cong S_{p-1} \times \mathbb{Z}_2$.

part *i*): For *a*), note that $N_k = N_\lambda$. Also, recall that $k = \mathbb{Q}(\lambda + 1\lambda)$. So, we may think of $G(N_\lambda/\mathbb{Q})$ as permuting the p conjugates of $\lambda + 1/\lambda$. Since $k \neq \bar{k}$ or any real isomorphic field for that matter, the elements of $G(N_\lambda/\mathbb{Q})$ that fix $\lambda + 1/\lambda$ generate a group isomorphic to S_{p-1}.

Assuming the Galois group of N_{r^2} is isomorphic to S_p implies that the Galois closure of r^2 is equal to the Galois closure of k. First of all, S_p has precisely one subgroup of index 2, which is A_p. Therefore, the Galois closure of k contains exactly one quadratic extension of $\mathbb{Q}$, say $\mathbb{Q}(\sqrt{-d})$. Also, the Galois group of N_k/k is isomorphic to S_{p-1}. Therefore, there is exactly one quadratic extension of k contained in N_k. Also, $k(\sqrt{-d})$ is a quadratic extension of k contained in the Galois closure of k, which means it must be the unique extension. Furthermore, this is the only possible subfield that can contain a loxodromic eigenvalue. Since the degree of k is an odd prime, by Remark 6.12 and Remark 6.11, $k(\sqrt{-d})$ contains a nontrivial root of unity if and only if $d = 1, 3$. From Proposition 6.13, we know that the angle is not unique precisely when the number field generated by a loxodromic eigenvalue contains a nontrivial root of unity.

part *ii*): Before we prove part *ii*), we need to characterize the index 2 subgroups of $S_n \times \mathbb{Z}_2$ because this will tell us information about degree 2 extensions via the fundamental theorem of Galois theory. Let H be a subgroup of index 2 of $S_n \times \mathbb{Z}_2$, and consider the following sequences:

$$H \hookrightarrow S_n \times \mathbb{Z}_2 \to S_n$$

$$H \hookrightarrow S_n \times \mathbb{Z}_2 \to \mathbb{Z}_2$$

where the first map is inclusion, i, and the second map is the projection, π, on the first and second factor respectively. Firstly, if $\pi \circ i$ is not surjective in the first sequence, then we know that the image must be A_n. Otherwise, H would not have index 2. Also, in this case, $\pi \circ i$ must be surjective because, otherwise, H would not have index 2. This implies that $H = A_n \times \mathbb{Z}_2$. Secondly, if $\pi \circ i$ is surjective in the first sequence, then we know that the image must be S_n. Also, if $\pi \circ i$ is not surjective in the second sequence, then $H = S_n \times \langle 0 \rangle$. Finally, if $\pi \circ i$ is surjective in the first sequence and surjective in the second sequence, then one possibility is that $H = \{((ij), 1) \mid 1 \leq i < j \leq n\}$. Note the group generated by this set has order $n!$. Are there any other possibilities? Since the image of the first sequence is isomorphic to S_n, H must contain an element of the form $((ij), x)$ for every transposition in S_n. Also, H cannot contain $((ij), 0)$ and $((ij), 1)$ because then $H = S_n \times \mathbb{Z}_2$. The last case to rule out is that H contains $((ij), 0)$ and $((k\ell), 1)$. We will show that in this case the subgroup contains $(e, 1)$, which would imply that the subgroup is the entire group. If this is the case:

$$((jk), x)\,((ij), 0)\,((jk), x)\,((k\ell), 1) = ((jk), x)\,((ijk\ell), x + 1)$$

$$((jk), x)\,((jk\ell i), x + 1) = ((k\ell i), 2x + 1) = ((k\ell i), 1)$$

where $x = 0, 1$. Now, taking the third power of the last element gives $(e, 1)$. Thus, there are only three possibilities.

For b), recall that we want to prove that $G(N_\lambda/k) \cong S_{p-1} \times \mathbb{Z}_2$ when $G(N_\lambda/\mathbb{Q}) \cong S_p \times \mathbb{Z}_2$, we claim that N_λ equals the composite of N_k and a degree 2 extension. $N_k \subset N_\lambda$. All that we need is to show that N_λ contains a quadratic extension of $\mathbb{Q}$ that is not contained in N_k. By the previous discussion, we have characterized the index 2 subgroups of $S_p \times \mathbb{Z}_2$ of which there are 3. However, there is only one index 2 subgroup of S_p. Via the fundamental theorem of Galois theory, we know that these correspond to quadratic extensions of $\mathbb{Q}$. Therefore, $N_\lambda = N_k\mathbb{Q}(\lambda)$. By Theorem 6.23, we know that $G(N_\lambda/\mathbb{Q}) \cong \{(\sigma, \tau) \mid \sigma \in G(N_k/\mathbb{Q}), \tau \in G(\mathbb{Q}(\sqrt{e})/\mathbb{Q})\}$. Now, we will look at the image of $G(N_\lambda/k)$ under this isomorphism with the direct product $G(N_k/\mathbb{Q}) \times G(\mathbb{Q}(\sqrt{-e})/\mathbb{Q})$ composed with the projection on the first component. Let $\sigma \in G(N_\lambda/k)$. Then, its image is $\sigma|_{N_k}$, and this element fixes k. Since any isomorphism of N_k lifts to and isomorphism of N_λ, this map surjects onto $G(N_k/k)$. Thus, the image must be isomorphic to S_{p-1}, and in order for $G(N_\lambda/k)$ to have index p the only possibility is that $G(N_\lambda/k) \cong S_{p-1} \times \mathbb{Z}_2$. Now, the proof is similar to part i). Except now there are 3 quadratic extensions of $\mathbb{Q}$ contained in the Galois closure of r^2 because of the previous discussion. Let these be $\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{-e})$, and $\mathbb{Q}(\sqrt{de})$ where $e > 0$ is square-free and $e \neq d$. Also, the Galois group of N_{r^2}/k is isomorphic to $S_{p-1} \times \mathbb{Z}_2$. Similarly, there are exactly three quadratic extensions of k contained in N_{r^2}, which must necessarily be $k(\sqrt{-d})$, $k(\sqrt{-e})$, and $k(\sqrt{de})$. The loxodromic eigenvalue with Galois group $S_p \times \mathbb{Z}_2$ must be an element of $k(\sqrt{-e})$ because the Galois group of $k(\sqrt{-d})$ is S_p and $k(\sqrt{de})$ has real embeddings since k has a real embedding and $\sqrt{de}$ is the square root of a positive real number. The field $k(\sqrt{-e})$ contains a nontrivial root of unity precisely if $e = 1, 3$. Then, $e = 1$ precisely when $de = d$ and $e = 3$ precisely when $de = 3d$. $\square$

Proof of Theorem 1.7: From the discussion in Section 6.2, we know that the

Galois group of N_{r^2} is not isomorphic to $S_3 \times \mathbb{Z}_2$ or S_3 when the degree of r^2 is equal to 12. So, the angle must be unique. When the degree of r^2 is equal to 6, the Galois group is isomorphic to D_6 ($\cong S_3 \times \mathbb{Z}_2$) so Theorem 1.8 part *ii*) applies. In this case, the Galois closure of r^2 has degree 12. If $\sqrt{d}$ or $\sqrt{3d}$ is not an element of $\mathbb{Q}(r^2)$, then real field $\mathbb{Q}(r^2, \sqrt{d})$ or $\mathbb{Q}(r^2, \sqrt{3d})$ is equal to the non-real Galois closure of r^2, which is a contradiction. Hence, $\sqrt{d}$ or $\sqrt{3d}$ is an element of $\mathbb{Q}(r^2)$. When the degree of r^2 is 3 the Galois group is isomorphic to S_3 so Theorem 1.8 part i) applies. □

Now that we have characterized when the angle of a loxodromic eigenvalue is not unique, we will come up with characterizations as to when the Galois closure of the trace field contains a loxodromic eigenvalue that has a non-unique angle. This discussion mainly serves to produce many examples when the angle is not unique. The goal of the rest of this section is to show the following proposition.

Proposition 6.24 *Let k be a number field with exactly one complex place such that $[k : \mathbb{Q}] = 3$. Then, N_k contains a loxodromic eigenvalue with a non-unique angle if and only if either one of the following conditions hold:*

i) The absolute value of the discriminant of k is a square, in which case the fourth root of unity is the culprit.

ii) The number field k is a radical extension of $\mathbb{Q}$, in which case the third (or sixth) root of unity is the culprit.

Proposition 6.25 *For any trace field k such that $[k : \mathbb{Q}] = 3$, the Galois closure of k contains a loxodromic eigenvalue.*

Proof: Since k is a degree 3 field with exactly one complex place, the Galois closure of k must have Galois group isomorphic to S_3. Therefore, the Galois closure of k is a degree 2 extension of k and is not contained in the set of real numbers. Since the Galois closure is non-real, it has no real embeddings. By Proposition 6.16, the Galois closure contains a loxodromic eigenvalue □

The next proposition is an elementary result on the Galois groups of polynomials of degree 3 from [5]. An irreducible polynomial of degree 3 has Galois group isomorphic to $\mathbb{Z}_3$ or S_3 depending whether or not the discriminant of the field arising from the polynomial is a square in $\mathbb{Q}$. By Proposition 6.25, we know that the Galois group is isomorphic to S_3. Therefore, the discriminant is not a square in $\mathbb{Q}$. However, we know that adjoining the square root of the discriminant to the field k results in the Galois closure. Thus, we have the following result.

Proposition 6.26 *The closure of a trace field of degree* 3 *contains* $\mathbb{Q}(\sqrt{-d})$ *if and only if the square root of the discriminant of the trace field generates the quadratic extension* $\mathbb{Q}(\sqrt{-d})$.

Corollary 6.27 *The closure of the trace field of degree* 3 *contains the fourth roots of unity if and only if the absolute value of the discriminant of the trace field is a square.*

Such polynomials do exist! For example, $x^3 + 6x + 4$ is irreducible over $\mathbb{Q}$, has discriminant equal to -1296, and $1296 = 36^2$. Hence, the splitting field for this polynomial contains the fourth roots of unity. Thus, $x^3 + 6x + 4$ has only one real root. The discriminant is not a square in $\mathbb{Q}$, which means the Galois group must be S_3. Since the Galois closure must have only complex places (it contains a nontrivial root of unity!), having only real roots would be a contradiction. Putting this together with the proposition above, there do exist trace fields whose closures have a primitive fourth root of unity.

Corollary 6.28 *The Galois closure of a trace field of degree* 3 *contains the sixth roots of unity if and only if the square class of the discriminant of the trace field has the same square root class as* $\sqrt{-3}$.

In the degree 3 case, there is even more appealing characterization when the Galois closure of the trace field contains the sixth roots of unity. But first, we need a result characterizing when a cubic extension is radical from [10].

Theorem 6.29 *Let K be a field such that $char(K) \neq 3$. Suppose that $K(\alpha)$ is an extension field of K and the minimal polynomial of α over K is $x^3 + ax + b$ for some a, $b \in K$ with $b \neq 0$. Let $D = -4a^3 - 27b^2$. A necessary and sufficient condition that there exists $\beta \in K(\alpha)$ such that $K(\alpha) = K(\beta)$ and $\beta^3 \in K$ is that, for some $c \in K$, $-3D = c^2$ if $char(K) \neq 2$.*

Now, we may complete our discussion when the Galois closure of a trace field of degree 3 contains the sixth roots of unity.

Proposition 6.30 *Let k be an arbitrary number field such that $[k : \mathbb{Q}] = 3$, k is a radical extension if and only if the Galois closure of k contains a primitive third root of unity. Furthermore, k must have one complex place if one of the previous equivalent conditions hold, and, thus, k is the trace field of some Kleinian group.*

Proof: Let N_k denote the Galois closure of k. If $k = \mathbb{Q}(\sqrt[3]{a})$ where $a \in \mathbb{Q}$, then $\sqrt[3]{a}$ has minimal polynomial $x^3 - a$ and adjoining ${\mu_3}^2\sqrt[3]{a}$ or ${\mu_3}^2\sqrt[3]{a}$ yields N_k, which has degree 6. Thus, N_k contains the third roots of unity, and, furthermore, $x^3 - a$ has one real and two complex roots. If the Galois closure of a cubic field contains the third roots of unity then the unique quadratic extension must be $\mathbb{Q}(\sqrt{-3})$. Thus, the discriminant of a minimal polynomial defining the cubic extension is in the same square class as -3. Hence, $-3D = -3 \cdot -3 = 9$, which is a square in $\mathbb{Q}$. By Theorem 6.29, k must be a radical extension. $\square$

Therefore, the Galois closure of a trace field of degree 3 contains the sixth roots of unity precisely when the trace field arises from an irreducible polynomial of the form $x^3 + a$, where a is an integer.

6.5 Isospectrality

In this section, we prove the following two theorems and a corollary:

Theorem 1.9 *There exist infinitely many commensurability classes of arithmetic Kleinian groups such that if Γ_1 and Γ_2 are derived and iso-length-spectral, then Γ_1 and Γ_2 complex iso-length-spectral.*

Theorem 1.10 *Consider a commensurability class of arithmetic Kleinian groups with invariant quaternion algebra A/k where $[k : \mathbb{Q}] = 3$, $k(\sqrt{-1}) \not\hookrightarrow A$, and $k(\sqrt{-3}) \not\hookrightarrow A$. Then, if Γ_1 and Γ_2 are derived and iso-length-spectral, then Γ_1 and Γ_2 are complex iso-length-spectral.*

Theorem 1.11 *For every $n \geq 2$, there exists a loxodromic norm, r, such that exactly n numbers on the unit circle make $re^{i\theta}$ a loxodromic eigenvalue. That is, the angle of a loxodromic angle can be highly non-unique.*

A possible obstruction to the equivalence of real-length isospectrality and complex length isospectrality is the angle of a loxodromic eigenvalue. If the two conditions are equivalent, the trace field is not restrictive enough to prove equivalence. However, we can find a certain restrictive case where the two conditions are equivalent. In this section, we will find infinitely many commensurability classes of derived arithmetic hyperbolic 3-manifolds where they are equivalent. The general idea is the following argument. Suppose Γ is an arithmetic Kleinian group derived from A/k such that $k \neq \bar{k}$. Suppose Γ does not contain a loxodromic element whose eigenvalue λ is such that $k(\lambda) = k(\mu)$ where $k(\lambda)$ is a quadratic extension of k and μ is a root of unity. If Γ' is any arithmetic Kleinian group derived from A/k that is iso-length-spectral to Γ, then Γ' is complex iso-length-spectral to Γ. In order to prove Theorem 1.9, we will need a result from Chapter 12 of [16]. This characterizes when group of elements of (reduced) norm 1 in a quaternion algebra contain an elements with finite order.

Theorem 6.31 *Let A be a quaternion division algebra over a number field k such that $C(A)$ is a class of arithmetic Kleinian or Fuchsian groups. Then, the following are equivalent:*

i) $P(A^1)$ contains an element of order n

ii) $\mu_{2n} + 1/\mu_{2n} \in k$, $\mu_{2n} \notin k$, and $L = k(\mu_{2n}) \hookrightarrow A$

iii) $\mu_{2n} + 1/\mu_{2n} \in k$, $\mu_{2n} \notin k$, and if $\wp \in Ram_f(A)$, then $\wp$ does not split in L/k.

Proof of Theorem 1.9: For any trace field $k \neq \bar{k}$, there are only finitely many "problematic" quadratic extensions of k because there are only finitely many roots of unity of bounded degree by Theorem 6.7. Furthermore, we have established that the problematic loxodromic eigenvalues come from quadratic extensions that contain nontrivial roots of unity by Theorem 1.6. Producing such manifolds relies on placing restrictions on the quaternion algebra A/k, which will prohibit embeddings of $k(\lambda)$ into A where $k(\lambda) = k(\mu)$ and μ is a root of unity. Recall that a commensurability class of arithmetic Kleinian groups is fully specified by an invariant quaternion algebra A/k and an invariant trace field k by Theorem 4.11. The flow of the proof is given a trace field, $k \neq \bar{k}$, with exactly one complex place, we specify a quaternion algebra A/k such that for every $\mu + 1/\mu \in k$, $k(\mu)$ does not embed in A. As a result, if Γ_1 and Γ_2 are derived arithmetic Kleinian groups with invariant quaternion algebra A/k and invariant trace field k such that Γ_1 is iso-length-spectral to Γ_2, then Γ_1 is complex iso-length-spectral to Γ_2. In order to prove this theorem, we will have to use a result in [16]. For clarification, $P(A^1)$ are the elements of reduced norm 1 in $P(A)$ where $P(A)$ is the quotient of A and $\{\pm I\}$. Also, note that taking the quotient of A

by $\{\pm I\}$ makes elements of order $2n$ have order n in $P(A^1)$. This makes no difference. We have noted before that λ and $-\lambda$ give rise to the same geodesic length, and this is what is happening here. Also, it is worth stating explicitly that any $\mathcal{O}^1 \subset A^1$.

Let k be a number field with exactly one complex place such that $k \neq \bar{k}$. By the classification theorem of quaternion algebras, choosing the places for $Ram(A)$ will determine a quaternion algebra over k. We require that all real places of k be in $Ram_\infty(A)$, since we do want this quaternion algebra to arise as one in the construction of arithmetic hyperbolic 3-manifolds. For every field $k \neq \bar{k}$, we will specify $Ram_f(A)$. There are only finitely many $\mu + 1/\mu \in k$ where μ is a root of unity. We need to ensure that for every $\mu + 1/\mu \in k$, there exists some $\wp \in Ram_f(A)$ such that $\wp$ splits in $k(\mu)/k$. Then, by Theorem 6.31, $P(A^1)$ will have no torsion. And, thus, every eigenvalue norm of elements in $P(A^1)$ has a unique angle paired with it.

This condition on $Ram_f(A)$ can be accomplished by using the Cheboratev Density Theorem. Infinitely many primes split in $k(\mu)/k$. Simply choose a prime in k that splits in $k(\mu)$ for each $\mu + 1/\mu \in k$. It may be necessary to add an extra prime to ensure that the cardinality of $Ram(A)$ is even. Though, a different construction is to choose a single prime $\wp$ of k such that $\wp$ splits in every $k(\mu)$, which may be done by Corollary 3.44. Then, the rest of $Ram_f(A)$ may be populated with any primes so long as the cardinality of $Ram(A)$ is even. $\square$

Proof of Theorem 1.10: The assumptions in this proof are that k has prime degree $p \neq 2$ and that $k(\sqrt{-1}) \not\hookrightarrow A$, and $k(\sqrt{-3}) \not\hookrightarrow A$. By Theorem 6.14, the loxodromic eigenvalues in these number fields cannot occur as a loxodromic eigenvalue in such a derived Kleinian group. By Theorem **??** and Proposition 6.13, the angles of loxodromic eigenvalues in these fields might not be unique. By Remark 6.12, these are the only μ, such that $k(\mu)$ is a quadratic extension of k are the primitive fourth and primitive sixth roots of unity. Therefore, these are the only quadratic extensions of k with loxodromic eigenvalues with possibly non-unique angles. $\square$

Now that we have proved Theorem 1.9 and Corollary 1.10, we shift gears to Theorem 1.11. In the proof of a corollary to Theorem 6.31 in [16], number fields with exactly one complex place are constructed with arbitrarily large degree such that $k = \bar{k}$. One may wonder, do there exist number fields k with exactly one complex place such that $k \neq \bar{k}$ and contains $\mu + 1/\mu$ of arbitrarily large degree, where μ is a root of unity. Theorem 1.11 shows that this is indeed the case. Although, the fields produced have $[k : k \cap \mathbb{R}] = 3$. A more general resolution to the problem would allow us to find number fields $k \neq \bar{k}$ with exactly one complex place containing $\mu + 1/\mu$ of arbitrarily large degree and with $[k : k \cap \mathbb{R}] = n$ for any integer n.

Proposition 6.32 *Let $e^{i\theta}$ be an algebraic integer on the unit circle such that all conjugates of $e^{i\theta} + e^{-i\theta}$ are real numbers (excluding ± 1). Then, there exists a number field k with exactly one complex place such that $k_0 = \mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subset k$. (Due to the restrictions of the construction, all the fields k have $[k : k_0] = 3$.)*

Proof: Given any finite set of real algebraic integers, we can multiply each number in the set by an integer q and then add an integer r to each number so that exactly one of the numbers in the set is positive and all others are negative. To see that this is possible, notice that the map from the real line to itself given by $f(x) = q \cdot x$ fixes 0 and stretches the real line to ∞ and $-\infty$. We need to choose q large enough so that there exists an integer strictly between the largest element of the set and the second largest element of the set. Then, we can choose r to be the negative of the integer that is strictly between the two values. Then, our derived set will consist of real algebraic integers with exactly one positive value and the rest will be negative. This may seem a little odd at the moment, but the motivation is to start with a maximal set of real algebraic integers that are conjugates and all of which are real numbers.

Let $\alpha \in k_0$ be an algebraic integer such that $\mathbb{Q}(\alpha) = k_0$. Next, we multiply α by a rational integer q and add a rational integer r such that $q\alpha + r$ has one positive conjugate and $n-1$ negative conjugates. We may rename $q\alpha + r$ as α and assume it is the positive conjugate. Note that the algebraic integers of a number field form a ring, so we have not changed the fact that α is an algebraic integer. Choose a rational prime, p, that does not ramify in k_0. This is possible by Theorem 3.39 which states only finitely many primes ramify in a given number field.

Now, consider $D = -4(\alpha p)^3 - 27p^2 \in k_0$. We desire that D has one negative and $n-1$ positive conjugates. If this is not the case, then multiply α by a large enough positive, rational integer and rename as α. To see that this always accomplishes what we want, recall that α is positive. Multiplying by p and taking the third power does not make the new product negative. In fact, it makes the number even larger in absolute value. Multiplying it by -1 makes the new product negative, then if we have been careful, subtracting $27p^2$ will still keep the value negative. Furthermore, all conjugates of $-4(\alpha p)^3 - 27p^2$ are equal to $-4(\sigma(\alpha)p)^3 - 27p^2$ for some σ. Running through the same argument makes all of these values positive.

Now, we claim that $k_0 = \mathbb{Q}(D)$. There are n conjugates of D, due to the fact that the function $g(x) = -4x^3 - 27p^2$ is one-to-one when restricted to the real numbers. This guarantees the claim is true. Now consider the polynomial $f(x) = x^3 + \alpha p x + p$ with coefficients in k_0. This polynomial is irreducible over k_0 by Eisenstein's criterion: αp, $p \in \wp$, and $p \notin \wp^2$ where $\wp$ lies over p. Next, we claim that the Galois group of $f(x)$ over k_0 is S_3. This must be the case because the square root of the discriminant, $\sqrt{D}$, is non-real. Thus, there are three degree 3 extensions contained in the splitting field of f. Since the coefficients of f are totally real and the splitting field of f is non-real, two of the three degree 3 extensions must be complex, call these k and $\bar{k}$, and the third must be real. Every other field isomorphic to k, $\bar{k}$, and the unnamed real field must be realized as the splitting field of $x^3 + p\sigma(\alpha)x + p$, where σ is any embedding of k_0 not equal to the identity embedding. We know by construction that all of those discriminants must be positive. Hence the splitting fields of those polynomials over $\sigma(k_0)$ must be real, which makes the three roots of those polynomials real. Therefore, there is only one pair of degree 3 extensions of k_0 that are non-real. Thus, k has exactly one complex place and contains $e^{i\theta}+e^{-i\theta}$. $\square$

Proof of Theorem 1.11: Recall that any conjugate of a root of unity is a root of unity. (They are solutions to the same minimal polynomial.) Any nontrivial root of unity fulfills the requirements of the above theorem because $\mu + 1/\mu = \mu + \bar{\mu} \in \mathbb{R}$ and the image of $\mu + 1/\mu$ under an isomorphism of $\mathbb{Q}(\mu + 1/\mu)$, say τ, is

$$\tau(\mu + 1/\mu) = \tau(\mu) + 1/\tau(\mu) = \tau(\mu) + \overline{\tau(\mu)} \in \mathbb{R}$$

Hence, for every n, there exists a norm of a loxodromic eigenvalue such that there are n loxodromic eigenvalues with the prescribed norm. Or in algebraic terms, for every nontrivial root of unity μ, there exists a field k with exactly one complex place such that $[k(\mu) : k] = 2$, and we know this field contains a loxodromic eigenvalue by Corollary 6.17.

Some fortunate investigation has produced a trace field of degree 6 that has a degree 2 extension which contains a loxodromic eigenvalue and a primitive twelfth root of unity: $p(x) = x^{12} - 2x^{11} - 2x^{10} + 4x^9 + 2x^8 - 2x^7 - x^6 - 2x^5 + 2x^4 + 4x^3 - 2x^2 - 2x + 1$

6.6 Salem Numbers and the Short Geodesic Conjecture

In this section, we prove the following theorem:

Theorem 6.33 *The Salem conjecture is equivalent to the Short Geodesic conjecture for arithmetic hyperbolic 3-orbifolds with invariant trace field $k = \bar{k}$.*

The conjectures are now listed.

Conjecture 6.34 *(Salem conjecture) There exists $m_s > 1$ such that if u is a Salem number, then $u \geq m_s$.*

Conjecture 6.35 *(Short Geodesic conjecture for dimension 3 with $k = \bar{k}$. There is a positive lower bound for the lengths of closed geodesics in arithmetic hyperbolic 3-orbifolds with $k = \bar{k}$.*

This conjecture, as a geometric statement, is fairly surprisingly. Why should the set of all (real) lengths of closed geodesics in some subclass of arithmetic hyperbolic 3-orbifolds be equal to the set of all lengths of closed geodesics in arithmetic hyperbolic 2-orbifolds? However, as an algebraic statement, the proof of this equivalence is quite straightforward. Note that normally the Short Geodesic conjecture in dimension 3 is not restricted to orbifolds with $k = \bar{k}$. The motivation for Conjecture 6.35 is that there is a connection between a conjecture of a universal lower bound on the lengths of closed geodesics in arithmetic hyperbolic 2-orbifolds and the Salem conjecture. This discussion can be found in Chapter 12.3 in [16], which is summarized in the following theorem:

Theorem 6.36 *The Salem conjecture is equivalent to the Short Geodesic conjecture in the two dimensional case.*

Conjecture 6.37 *(Short Geodesic conjecture for dimension 2) There is a positive lower bound for the lengths of geodesics in arithmetic hyperbolic 2-orbifolds.*

Definition 6.38 *A* **Salem number** *is a real algebraic integer $\alpha > 1$ whose other conjugates have norm at most equal to 1, with at least one conjugate that has norm equal to 1.*

Note that if $e^{i\theta}$ is an algebraic integer, then $\overline{e^{i\theta}} = 1/e^{i\theta}$ is a conjugate. Therefore, by Lemma 7.7, the minimal polynomial is palindromic.

Proposition 6.39 *Let $\alpha > 1$ be a Salem number. Then the set of conjugates of α is* $\{\alpha, 1/\alpha, e^{i\phi_1}, \ldots, e^{i\phi_k}\}$

Proof: Since α has a conjugate, $e^{i\theta}$, of norm equal to 1, the minimal polynomial, $p(x)$, of α is palindromic. Thus, if α is a root of $p(x)$, then $1/\alpha$ is also a root of $p(x)$. Since $p(x)$ has only one root with norm greater than 1, the set of conjugates is precisely as described above. $\square$

Now what we will show is that the square of the norm of a loxodromic eigenvalue is a Salem number when $k = \bar{k}$ with the exception of one case when $[k : \mathbb{Q}] = 2$. The one exceptional case is not a problem, which will be explained in the following paragraph. Proposition 4.17 shows that for any Salem number, we can find an arithmetic Kleinian group containing a hyperbolic element with eigenvalue equal to the Salem number. Therefore, the entire real length set from all arithmetic Kleinian groups with $k = \bar{k}$ only contains lengths of the form $2ln|\lambda| = ln|\lambda^2|$ where either λ^2 is a Salem number or $|\lambda^2|$ is a Salem number. Then, the Short Geodesic conjecture in the 3-dimensional case with $k = \bar{k}$ is equivalent to the Short Geodesic conjecture in the 2-dimensional case.

There are norms of loxodromic eigenvalues that are not Salem numbers when $[k : \mathbb{Q}] = 2$. However, in that case the norms are Pisot numbers, and it is known that these have a universal lower bound greater than 1.

Definition 6.40 *A* **Pisot number** *is a real algebraic integer $\alpha > 1$ whose other conjugates have norm less than 1.*

Now, we directly handle the case when $[k : \mathbb{Q}] = 2$.

Proposition 6.41 *Let $\lambda = re^{i\theta}$ be a loxodromic eigenvalue from a Kleinian group derived from A/k. Suppose $[k : \mathbb{Q}] = 2$. Then, r^2 is a Salem number if and only if*

$e^{i\theta}$ is not a root of unity. If $e^{i\theta}$ is a root of unity, then r^2 has two conjugates, r^2 and $1/r^2$, and r^2 is a Pisot number.

Proof: If $[k:\mathbb{Q}] = 2$, then $k = \bar{k}$. By Proposition 5.3, this falls into two cases:

Case 1: $\mathbb{Q}(\lambda) = \mathbb{Q}(\bar{\lambda})$

Note that $k(\lambda) = \mathbb{Q}(\lambda) = \mathbb{Q}(\bar{\lambda}) = k(\bar{\lambda})$. Therefore, by Proposition 5.3, $e^{i\theta}$ is a root of unity. Since $\mathbb{Q}(\lambda)$ contains all conjugates of λ, this is a Galois extension. Since $\mathbb{Q}(\lambda) = \mathbb{Q}(\bar{\lambda})$, determining the image of λ, determines the element of the Galois group. Once we determine the Galois group, then we need to compute the image of $r^2 = \lambda\bar{\lambda}$ under all elements. Finally, we can then determine the conjugates of r^2 by listing the elements of the Galois group of the Galois closure of λ in permutation notation.

$$\begin{aligned}
\lambda \mapsto \lambda \quad &: \quad (\lambda)(\bar{\lambda})(\lambda^{-1})(\bar{\lambda}^{-1}) \\
\lambda \mapsto \bar{\lambda} \quad &: \quad (\lambda\bar{\lambda})(\lambda^{-1}\bar{\lambda}^{-1}) \\
\lambda \mapsto \lambda^{-1} \quad &: \quad (\lambda\lambda^{-1})(\bar{\lambda}\bar{\lambda}^{-1}) \\
\lambda \mapsto \bar{\lambda}^{-1} \quad &: \quad (\lambda\bar{\lambda})(\lambda^{-1}\bar{\lambda}^{-1})
\end{aligned}$$

The conjugates of r^2 are r^2 and $1/r^2$.

Case 2: $\mathbb{Q}(\lambda) \neq \mathbb{Q}(\bar{\lambda})$

Again, we have that $k(\lambda) = \mathbb{Q}(\lambda) = \mathbb{Q}(\bar{\lambda}) = k(\bar{\lambda})$. So, by Proposition 5.3, $e^{i\theta}$ is not a root of unity. Similarly, we compute the elements of the Galois group. In this case, for every image of λ, there are exactly two such elements of the Galois group.

$$\begin{array}{llll} \lambda \mapsto \lambda & : & (\lambda)(\bar{\lambda})(\lambda^{-1})(\bar{\lambda}^{-1}) & (\lambda)(\lambda^{-1})(\bar{\lambda}\bar{\lambda}^{-1}) \\ \lambda \mapsto \bar{\lambda} & : & (\lambda\bar{\lambda})(\lambda^{-1}\bar{\lambda}^{-1}) & (\lambda\bar{\lambda}\lambda^{-1}\bar{\lambda}^{-1}) \\ \lambda \mapsto \lambda^{-1} & : & (\lambda\lambda^{-1})(\bar{\lambda}\bar{\lambda}^{-1}) & (\lambda\lambda^{-1})(\bar{\lambda})(\bar{\lambda}^{-1}) \\ \lambda \mapsto \bar{\lambda}^{-1} & : & (\lambda\bar{\lambda})(\lambda^{-1}\bar{\lambda}^{-1}) & (\lambda\bar{\lambda}^{-1}\lambda^{-1}\bar{\lambda}) \end{array}$$

Then, the conjugates of r^2 are $r^2, 1/r^2, e^{2i\theta}$, and $e^{-2i\theta}$. $\square$

Now, we need a lemma and a remark before we prove that given a loxodromic eigenvalue, $\lambda = re^{i\theta}$, from a derived Kleinian group such that $[k : \mathbb{Q}] > 2$, then r^2 is a Salem number if and only if $k = \bar{k}$.

Lemma 6.42 *Let $\lambda = re^{i\theta}$ be a loxodromic eigenvalue derived from a quaternion algebra A/k. Then, if a $\mathbb{Q}$-embedding $\sigma : \mathbb{Q}(r^2) \hookrightarrow \mathbb{C}$ maps r^2 to $e^{2i\theta}$ then $\lambda \mapsto \lambda$ and $\bar{\lambda} \mapsto 1/\bar{\lambda}$, or $\lambda \mapsto 1/\bar{\lambda}$ and $\bar{\lambda} \mapsto \lambda$.*

Proof: There exist conjugates of λ, say x, y, such that $x \mapsto \lambda$ and $y \mapsto \bar{\lambda}$. Since x/y is sent to $e^{i\theta}$ as well and the embedding is a permutation, $x/y = r^2$. However, from Lemma 6.1, the only possibility is that $\{x, y\} = \{\lambda, \bar{\lambda}\}$. $\square$

Remark 6.43 *Now suppose that r^2 is not a conjugate of $e^{2i\theta}$. Then, no such embedding can do any of the following four possibilities: $\lambda \mapsto \lambda$ and $\bar{\lambda} \mapsto 1/\bar{\lambda}$, $\lambda \mapsto 1/\bar{\lambda}$ and $\bar{\lambda} \mapsto \lambda$, $\lambda \mapsto \lambda$ and $\bar{\lambda} \mapsto 1/\bar{\lambda}$, or $\lambda \mapsto 1/\bar{\lambda}$ and $\bar{\lambda} \mapsto \lambda$.*

Proposition 6.44 *Let $\lambda = re^{i\theta}$ be a loxodromic eigenvalue from a Kleinian group derived from A/k. Suppose $[k : \mathbb{Q}] \neq 2$. Then, r^2 is a Salem number if and only if $k = \bar{k}$.*

Proof: Suppose r^2 is a Salem number.

Case 1: $e^{2i\theta}$ is not a conjugate of r^2.

Then, r^2 has conjugates r^2, $1/r^2$, and $e^{i\phi_k}$. Any $\mathbb{Q}$-embedding $\sigma : \mathbb{Q}(e^{2i\theta}) \hookrightarrow$

$\mathbb{C}$ lifts to an embedding $\hat{\sigma} : N_\lambda \hookrightarrow \mathbb{C}$ where N_λ is the Galois closure of λ and $\hat{\sigma} \in G(N_\lambda/\mathbb{Q})$. Notice $|\hat{\sigma}(\lambda)|$ is in the set $\{r, 1/r, 1\}$, $|\hat{\sigma}(r^2)|$ is in the set $\{r^2, 1/r^2, 1\}$ because r^2 is a Salem number, and $\hat{\sigma}(\lambda)\hat{\sigma}(\bar{\lambda}) = \hat{\sigma}(r^2)$. Along with Remark 6.43, we may deduce $|\hat{\sigma}(\lambda)| = |\hat{\sigma}(\bar{\lambda})|$ for all $\hat{\sigma} \in G(N_\lambda/\mathbb{Q})$. Therefore, $|\hat{\sigma}(e^{2i\theta})| = |\hat{\sigma}(\lambda)|/|\hat{\sigma}(\bar{\lambda})| = 1$. By Theorem 6.6, all conjugates of $e^{2i\theta}$ have norm 1, which implies $e^{i\theta}$ is a root of unity. Hence, λ is the eigenvalue of a non-generic isometry. By Proposition 5.8 and Proposition 5.9, $k = \bar{k}$.

Case 2: $e^{2i\theta}$ is a conjugate of r^2.

By Lemma 6.42, any field isomorphism that sends r^2 to $e^{\pm 2i\theta}$ lifts to a field isomorphism that either fixes λ and inverts $\bar{\lambda}$ or inverts λ and fixes $\bar{\lambda}$ up to complex conjugation. Since r^2 has no conjugates of norm r or $1/r$, the only other possible images of λ and $\bar{\lambda}$ under an embedding are elements of norm 1. Then, $\lambda + 1/\lambda$ and $\bar{\lambda} + 1/\bar{\lambda}$ are not fixed because $e^{i\phi} + 1/e^{i\phi}$ is a real number. This implies that any map fixing $\mathbb{Q}(\lambda + 1/\lambda)$ also fixes $\mathbb{Q}(\bar{\lambda} + 1/\bar{\lambda})$ and vice versa. Therefore, $k = \bar{k}$.

For the converse, suppose $k = \bar{k}$. By Proposition 5.3, either $e^{2i\theta}$ is a root of unity or $e^{2i\theta}$ is a conjugate of r^2.

Case 1: $e^{2i\theta}$ is a root of unity.

Any $\hat{\sigma} : N_\lambda \hookrightarrow \mathbb{C}$ must have $|\hat{\sigma}(\lambda)| = |\hat{\sigma}(\bar{\lambda})|$. Otherwise, there exists $\hat{\sigma} \in G(N_\lambda/\mathbb{Q})$ such that $|\hat{\sigma}(e^{2i\theta})| = |\hat{\sigma}(\lambda)|/|\hat{\sigma}(\bar{\lambda})| \neq 1$, which contradicts Theorem 6.6. Thus, the possible conjugates of r^2 are r^2, $1/r^2$, and $e^{i\phi_k}$. By Proposition 6.39, we need to show that r^2 has a conjugate of norm 1. Since $[k : \mathbb{Q}] > 2$, we know $[k(\lambda) : \mathbb{Q}] > 4$. Thus, there exists $\hat{\sigma} \in G(N_\lambda/\mathbb{Q})$ such that $\hat{\sigma}(\lambda) = e^{i\tau}$. Since $|\hat{\sigma}(\lambda)| = |\hat{\sigma}(\bar{\lambda})|$, it must be the case that $|\hat{\sigma}(r^2)| = 1$. Hence, r^2 is a Salem number.

Case 2: $e^{2i\theta}$ is a conjugate of r^2.

By Proposition 4.16, $k = \mathbb{Q}(\lambda + 1/\lambda)$ and $\bar{k} = \mathbb{Q}(\bar{\lambda} + 1/\bar{\lambda})$. By Remark 6.42 and $\mathbb{Q}(\lambda + 1/\lambda) = \mathbb{Q}(\bar{\lambda} + 1/\bar{\lambda})$, $\lambda \mapsto \lambda^{\pm 1}$ if and only if k is fixed if and only if $\bar{k}$ is fixed if and only if $\lambda \mapsto \lambda^{\pm 1}$. Otherwise, an embedding sends λ and $\bar{\lambda}$ to elements of norm 1. Furthermore, $\mathbb{Q}(\lambda + 1/\lambda) \neq \mathbb{Q}(e^{i\phi} + e^{-i\phi})$, since $e^{i\phi} + e^{-i\phi}$ is a real number. Therefore, we may conclude $|\sigma(\lambda)| = 1$ if and only if $|\sigma(\bar{\lambda})| = 1$. Hence, the only conjugates of r^2 of norm not equal to 1 are precisely r^2 and $1/r^2$. From degree argument in the case above, we know that λ has a conjugate of norm 1. By Lemma 7.7, we know that $1/r^2$ is a conjugate of r^2 because r^2 has a conjugate with norm equal to 1. By Lemma 6.39, r^2 is a Salem number.

□

That finishes the proof that the Short Geodesic conjecture for arithmetic Kleinian groups with $k = \bar{k}$ is equivalent to the Salem conjecture. What follows in Section 7 are some results that followed from the theorem above and also Corollary 6.3. The main motivation is to find which roots of unity may appear as the angle of a non-generic loxodromic eigenvalue. By Proposition 5.8 and Proposition 5.9, these necessarily occur in derived arithmetic Kleinian groups with $k = \bar{k}$. Then, we also show that some Salem numbers cannot appear as the norm of a generic loxodromic eigenvalue through one case where a simple degree consideration argument works but also another more interesting example when degree considerations are not enough. This material is contained in Section 7.2.

7 Appendix

7.1 More on loxodromic eigenvalues

Remark 7.1 *The norm of a loxodromic eigenvalue does not completely determine the angle of the eigenvalue as seen above. But, the angle of a generic loxodromic eigenvalue completely determines the norm of the eigenvalue. Since we know the conjugates of a loxodromic eigenvalue, we can determine the possible conjugates of* $\lambda/\bar{\lambda} = e^{2i\theta}$*. The possible conjugates have one of the following forms:* r^2, $\lambda \cdot e^{i\phi}$, $\bar{\lambda} \cdot e^{i\phi}$, *and* $e^{i\phi_1} \cdot e^{i\phi_2}$*. (Of course, there are more possibilities. We could take reciprocals and complex-conjugate if we wanted.) Either* $e^{2i\theta}$ *only has conjugates of norm* 1*, in which case it is a root of unity, or it has at least one conjugate of norm* r^2 *or* r*. The latter case means that* $e^{i\theta}$ *has a real conjugate of norm* r *or a non-real conjugate of norm* $\sqrt{r}$*, and, thus, the angle completely determines the norm of the eigenvalue because any other norm that occurs will be* 1*.*

We have pretty much pinned down what loxodromic elements may occur in a quadratic extension of a trace field $k \neq \bar{k}$. That is, the only loxodromic eigenvalues that do occur are the ones we have mentioned thus far. This is summed up in Proposition 7.3 with the help of Lemma 7.2, which we state and prove now.

Lemma 7.2 *Let* $\lambda_1 = r_1 e^{i\theta_1}$ *and* $\lambda_2 = r_2 e^{i\theta_2}$ *be loxodromic eigenvalues arising from trace field* k*. Suppose* $e^{i\theta_1}$ *and* $e^{i\theta_2}$ *are not roots of unity and* $k(\lambda_1) = k(\lambda_2)$*.*

i) If $\lambda_1 \neq \pm\bar{\lambda}_1$*, then* $\lambda_1 \cdot \lambda_2$ *is a loxodromic eigenvalue over* k*.*

ii) If $r_1 \neq r_2$ *and* $e^{i\theta_1} \neq e^{i\theta_2}$*, then* λ_1/λ_2 *is a loxodromic eigenvalue over* k*.*

Proof: From the proof of Proposition 1.6 and the fact that $\lambda_1\lambda_2 + 1/\lambda_1\lambda_2 \notin \mathbb{R}$, we may deduce $\mathbb{Q}(\lambda_1\lambda_2 + 1/\lambda_1\lambda_2) = k = \mathbb{Q}(\lambda_1 + 1/\lambda_1)$ and $\mathbb{Q}(\lambda_1\lambda_2) = \mathbb{Q}(\lambda_1)$. A similar argument shows *ii)* is true as well. $\square$

Proposition 7.3 *For a given generic loxodromic eigenvalue, λ, the only other loxodromic eigenvalues that $\mathbb{Q}(\lambda)$ contains are of the form $\lambda^n \cdot \mu$, where μ is a root of unity.*

Proof: From the discussion in the paragraph after Lemma 6.1, there must be finitely many algebraic integers whose conjugates are uniformly bounded away from 0 and ∞. So, if a number field contains a loxodromic eigenvalue, then there must be a loxodromic eigenvalue whose norm is greater than 1 but no other loxodromic eigenvalue in the number field has norm closer to 1. By Lemma 7.2, we are able to multiply and divide under certain circumstances, and what results will also be a loxodromic eigenvalue.

Suppose that there exists λ_1 such that $|\lambda|^k < |\lambda_1| < |\lambda|^{k+1}$. By Remark 7.1, we know that $e^{i\theta} \neq e^{i\theta_1}$. Thus, by Lemma 7.2, λ_1/λ^k is a loxodromic eigenvalue (λ^k is also a loxodromic eigenvalue), but the previous inequality implies that $1 < |\lambda_1/\lambda^k| < |\lambda|$. This contradicts the fact that λ has norm closest to but larger than 1. $\square$

7.2 Salem numbers and possible angles

The natural predecessor of what follows here is Theorem 1.5. Corollary 6.3 is a corollary to Theorem 1.5, which we will after some discussion on palindromic polynomials. After Corollary 6.3, we will look at some fun applications of some facts we have learned.

Definition 7.4 *A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_i \in \mathbb{R}$ is called* **palindromic** *if $a_i = a_{n-i}$ for $i = 1, \ldots, n$.*

Definition 7.5 *A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_i \in \mathbb{R}$ is called* **anti-palindromic** *if $a_i = -a_{n-i}$ for $i = 1, \ldots, n$*

Lemma 7.6 *A polynomial, $q(x)$, is anti-palindromic if and only if $q(x) = (x-1) \cdot p(x)$ where $p(x)$ is palindromic.*

Proof: Suppose $p(x)$ is palindromic, that is, $a_{n-i} = a_i$ for $i = 1, \ldots, n$. Then,

$$(x-1) \cdot (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) =$$

$$a_n x^{n+1} + a_{n-1} x^n + \ldots + a_1 x^2 + a_0 x - a_n x^n - \ldots - a_2 x^2 - a_1 x - a_0 =$$

$$a_n x^{n+1} + (a_{n-1} - a_n) x^n + \ldots + (a_1 - a_2) x^2 + (a_0 - a_1) x - a_0$$

By the assumption that $p(x)$ is palindromic, $a_n = -(-a_0)$ and $a_{n-(i+1)} - a_{n-i} = a_{i+1} - a_i = -(a_i - a_{i+1})$. Therefore, $(x-1) \cdot p(x)$ is anti-palindromic. Now, suppose that $q(x)$ is anti-palindromic. Then, $q(1) = \sum a_i = 0$. Therefore, we may divide by $x - 1$ to get a polynomial $p(x)$. The n coefficients of $p(x)$ yielded by the division algorithm for polynomials are

$$a_n, a_n + a_{n-1}, \ldots, a_n + a_{n-1} + \ldots + a_2, a_n + a_{n-1} + \ldots + a_2 + a_1$$

However, $q(x)$ is anti-palindromic. So, the i^{th} coefficient from the right with $i \leq n/2$ is

$$a_n + a_{n-1} + \ldots + a_{n-i} + \ldots + a_i$$

and this equals

$$a_n + a_{n-1} + \ldots + a_{n-i+1}$$

which is equal to the i^{th} coefficient from the left. Therefore $p(x)$ is palindromic. $\square$

Therefore, anti-palindromic polynomials are reducible. In the proof below, we show that for every root, α, of a palindromic polynomial, $1/\alpha$ is a root as well. Next we show that if a minimal polynomial has α and $1/\alpha$ as roots, then the polynomial is palindromic.

Lemma 7.7 *A minimal polynomial, $f(x)$, is palindromic if and only if there exists a non-zero $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0 = f(1/\alpha)$.*

Proof: Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ is palindromic. By the fundamental theorem of algebra, there exists $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Consider $f(1/\alpha) = a_n(1/\alpha)^n + a_{n-1}(1/\alpha)^{n-1} + \ldots + a_1(1/\alpha) + a_0$. Multiplying each side by α^n yields:

$$\alpha^n f(1/\alpha) = a_n + a_{n-1}\alpha + \ldots + a_1\alpha^{n-1} + a_0\alpha^n$$

However, we are assuming f is palindromic so,

$$\alpha^n f(1/\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + a_n\alpha^n$$

Furthermore, the value of the above expression is 0. Hence, $f(1/\alpha)$ is 0. On the other hand, suppose there exists a non-zero $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0 = f(1/\alpha)$ for a minimal polynomial f. Thus, $a_n = 1$. First, we have that

$$0 = f(\alpha) = (\alpha)^n + a_{n-1}(\alpha)^{n-1} + \ldots + a_1(\alpha) + a_0$$

And, by starting with the fact that $f(1/\alpha) = 0$ and multiplying both sides by α^n we have that

$$0 = \alpha^n f(1/\alpha) = 1 + a_{n-1}\alpha + \ldots + a_1\alpha^{n-1} + a_0\alpha^n$$

However, this implies that α satisfies another polynomial. If $a_0 = 1$, then the polynomials have the same coefficients, since minimal polynomials are unique. Hence, $a_i = a_{n-i}$ for $i = 1, \ldots, n$. Otherwise, $a_0 \neq 1$. In this case, divide the polynomial by a_0. (If $a_0 \neq 0$, then $p(x)$ is not irreducible.) Then, by the uniqueness of the minimal polynomial the constant terms are equal. So, $a_0 = 1/a_0$, which implies $a_0 = -1$. However, this implies $a_{n-i} = -a_i$, but, by the previous lemma, anti-palindromic polynomials are reducible. Therefore $p(x)$ is palindromic. $\square$

Note that by Proposition 4.16 eigenvalues of loxodromic and hyperbolic elements have minimal polynomials that are palindromic because they have conjugates that have norm 1. This fact will be used in Corollary 6.3 and later when we want to get our hands dirty by looking at some examples of minimal polynomials of loxodromic eigenvalues using PARI. To further explain the latter comment, we are going to ask PARI to look through some integral polynomials and find those that are irreducible with the appropriate types of roots (all but 4 are on the unit circle). By the discussion above, we can further restrict the those integral polynomials to those that are palindromic.

Proposition 7.8 *If r is a Salem number and $e^{i\theta}$ is a non-trivial root of unity, then $re^{i\theta}$ is a loxodromic eigenvalue if and only if $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r + 1/r)$.*

Proof: By Corollary 6.3, if $re^{i\theta}$ is a loxodromic eigenvalue, then $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r + 1/r)$. Now assume, $\mathbb{Q}(e^{i\theta} + e^{-i\theta}) \subseteq \mathbb{Q}(r + 1/r)$. By Remark 6.2, $r \mapsto r^{\pm 1}$ implies $\mathbb{Q}(r + 1/r)$ is fixed. By the containment of fields, if $\mathbb{Q}(r + 1/r)$ is fixed, then $\mathbb{Q}(e^{i\theta} + 1/e^{i\theta})$ is fixed. Again, by Remark 6.2, $\mathbb{Q}(e^{i\theta} + 1/e^{i\theta})$ being fixed implies $e^{i\theta} \mapsto e^{\pm i\theta}$. Then, four conjugates of $re^{i\theta}$ do not lie on the unit circle. The remaining conjugates of r have norm equal to 1 and, since $e^{i\theta}$ is a root of unity, any conjugate of $e^{i\theta}$ has norm equal to 1. Thus, if r is not sent to $r^{\pm 1}$, then $|\sigma(re^{i\theta})| = |\sigma(r)||\sigma(e^{i\theta})| =$

$1 \cdot 1 = 1$. This proves that all other conjugates of $re^{i\theta}$ lie on the unit circle. Hence, $re^{i\theta}$ is a loxodromic eigenvalue. $\square$

Corollary 7.9 *There exist roots of unity (primitive third and fourth roots of unity) such that the product of the root of unity and any Salem number results in a loxodromic eigenvalue.*

Proof: For the roots of unity mentioned in the statement above, $\mathbb{Q}(e^{i\theta}+e^{-i\theta}) = \mathbb{Q}$. Hence, the field is always contained in $\mathbb{Q}(r + 1/r)$. $\square$

Definition 7.10 *A permutation group G acting on a set X is* **primitive** *if G acts transitively on X and any nontrivial partition of X is not preserved by G. Otherwise, G is imprimitive.*

Note that the symmetric group on n objects is a primitive group because the symmetric group is the set of *all* permutations. Thus, for any partition, there is some element of the symmetric group that does not preserve the given partition.

Proposition 7.11 *Let r^2 be a Salem number. Then, if the Galois group of the minimal polynomial of $r^2 + 1/r^2$ is primitive, then r^2 is not the norm of a generic loxodromic eigenvalue.*

Proof: Let $e^{i\phi}$ be any conjugate of r^2 that lies on the unit circle. Then, $[\mathbb{Q}(r^2 + 1/r^2) : \mathbb{Q}] = [\mathbb{Q}(e^{i\phi}+1/e^{i\phi}) : \mathbb{Q}]$, since they are roots of the same minimal polynomial. If the Galois group is primitive, then $\mathbb{Q}(r^2 + 1/r^2) \neq \mathbb{Q}(e^{i\phi} + 1/e^{i\phi})$. Otherwise, we could find a nontrivial partition of the conjugates of $r^2 + 1/r^2$ that is preserved by the Galois group. Therefore, $\mathbb{Q}(e^{i\phi} + 1/e^{i\phi}) \not\subseteq \mathbb{Q}(r^2 + 1/r^2)$. Now suppose that $r^2e^{i\theta}$ is a loxodromic eigenvalue. Then, by Proposition 5.3, $e^{i\theta}$ is a conjugate of r^2. The fact that $\mathbb{Q}(e^{i\phi} + 1/e^{i\phi}) \not\subseteq \mathbb{Q}(r^2 + 1/r^2)$ violates Corollary 6.3. Hence, r^2 is not the norm of a generic loxodromic eigenvalue. $\square$

Recall that Salem numbers can only occur as eigenvalues of Kleinian groups derived from A/k where $k = \bar{k}$. Every Salem number is a hyperbolic eigenvalue, and every Salem number is the norm of a periodically loxodromic eigenvalue. However, every Salem number cannot be realized as the norm of a generic loxodromic element. For example, Lehmer's number is a Salem number that is a root of the irreducible polynomial $x^{10} - x^9 + x^7 - x^6 + x^5 - x^4 + x^3 - x + 1$. By Proposition 5.3, we know that the degree of the of $\mathbb{Q}(r^2)$ must be equal to $2m$, where m is the degree of the trace field. In our case, r^2 is a Salem number. By Proposition 5.9, the degree of the trace field must be divisible by 2. Clearly, 5 is not divisible by 2. Hence, Lehmer's number cannot occur as the norm of a generic loxodromic eigenvalue. Moreover, even if the degree of the Salem number is divisible by 4, this does not guarantee that it may occur. By Proposition 7.11, the Salem number with minimal polynomial $x^{20} - x^{18} - x^{15} - x^5 - x^2 + 1$ has a trace polynomial (the trace polynomial is the minimal polynomial of $r^2 + 1/r^2$) with Galois group isomorphic to S_{10}.

References

[1] R. C. Alperin, *An elementary account of Selberg's lemma*, Enseign. Math. (2) 33 (1987), no. 3-4, 269-273.

[2] L. Bérard-Bergery, "Laplacien et géodésiques fermées sur les formes d'espace hyperbolique compactes" in *Seminaire Bourbaki*, 1971/72, Lecture Notes in Math. **317**, Springer, Berlin, 1973, 107-122.

[3] G. Butler and J. McKay, *The transitive groups of degree up to eleven.* Comm. in Algebra **11** (7): 863-911, (1983).

[4] T. Chinburg, E. Hamilton, D. D. Long, and A.W. Reid, *Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds*, Duke Math. J. **145** (2008), pp. 25-44.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley and Sons (2003).

[6] R. Gangolli, *The length spectra of some compact manifolds of negative curvature*, J. Differential Geom. **12** (1977), 403-424.

[7] C. Gordon, D. Webb, and S. Wolpert, *Isospectral plane domains and surfaces via Riemannian orbifolds*, Invent. Math., **110** (1992), 1-22.

[8] G. J. Janusz, *Algebraic Number Fields*, Graduate Studies in Math. Vol. **7** American Mathematical Society (2005).

[9] M. Kac, *Can one hear the shape of a drum?*, American Mathematical Monthly 73 (4, part 2): 1-23

[10] M. Kang, *Cubic Fields and Radical Extensions*, American Mathematical Monthly 107 (3): 254-256

[11] D. G. Kendall and R. Osborn *Two Simple Lower Bounds for Euler's Function*, Texas J. Sci. **17** 1965.

[12] L. Kronecker *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 173-175.

[13] C. Leininger, D. B. McReynolds, W. D. Neumann, and A.W. Reid, *Length and eigenvalue equivalence*, International Math. Research Notices, volume 2007, article ID rnm135, 24 pages, doi:10.1093/imrn/rnm135.

[14] H.P. McKean, *The Selberg trace formula as applied to a compact Riemann surface*, Comm. Pure Appl. Math. **25** (1972), 225-246.

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

[16] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Math. **219** Springer, (2002).

[17] PARI/GP, version `2.3.5`, Bordeaux, 2008, http://pari.math.u-bordeaux.fr

[18] R. Perlis, *On the Equation* $\zeta_K(s) = \zeta_{K'}(s)$. Journal of Number Theory **9** (1977), 342-360.

[19] A.W. Reid, *A note on trace-fields of Kleinian groups*. Bull. London Math. Soc. **22** (1990), 349-352.

[20] A.W. Reid, *Commensurability and isospectrality of arithmetic hyperbolic 2 and 3-manifolds*. Duke Math J. **65** (1992), 215-228.

[21] P. Samuel, *Algebraic Theory of Numbers*, Dover Publications (2008).

[22] C. Smyth, *Number Theory and Polynomials*, Cambridge University Press (2008).

[23] R.J. Spatzier, *On isospectral locally symmetric spaces and a theorem of von Neumann*, Duke Math J. **59** (1989); *Correction*, Duke Math. J. **60** (1990), 561.

[24] T. Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. **121** (1985), 169-186.

[25] M.-F. Vignéras, *Variétés Riemmannienes isopectrales et non isométriques*, Ann. of Math. **112** (1980), 21-32.

[26] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Math. **800**, Springer, Berlin, 1980.