A CONJECTURE OF CHINBURG-REID-STOVER FOR SURGERIES ON TWIST KNOTS

NICHOLAS ROUSE

Abstract. Associated to a hyperbolic knot complement in $S^3$ is a set of prime numbers corresponding to the residue characteristics of the ramified places of the quaternion algebras obtained by Dehn surgery on the knots. Previous work by Chinburg-Reid-Stover gives conditions on the Alexander polynomial of the knot for this set to be finite. We show that there are infinitely many examples of knots for which this set is infinite, providing evidence for a conjecture of Chinburg-Reid-Stover.

1. Introduction

When $\Gamma$ is a finitely generated group, one may form its $\text{SL}_2\mathbb{C}$-character variety, which is an algebraic set parametrizing representations $\Gamma \to \text{SL}_2\mathbb{C}$. Work of Thurston and Culler-Shalen \cite{4} introduced the character variety to the study of the geometry and topology of compact 3-manifolds. More recently, Chinburg-Reid-Stover in \cite{2} paid particular attention to the arithmetic aspects of the component of the character variety—called the canonical component—containing the character of the faithful discrete representation in the setting that $M$ is a hyperbolic knot complement. More specifically, if we write $C$ for the canonical component and $k(C)$ for its function field, there is a canonically defined quaternion algebra, $A_{k(C)}$, defined over $k(C)$. The geometric content encoded by this object is that it specializes at a character of a hyperbolic Dehn surgery to the quaternion algebra associated to that Kleinian group.

It is natural to ask how these quaternion algebras vary through different surgeries on the knot. Chinburg-Reid-Stover show in \cite{2} that a condition on the Alexander polynomial of the knot (called condition $(\star)$ in \cite{2}) guarantees that there are only finitely many rational primes lying under any finite prime ramifying the specializations of this quaternion algebra. Let us write $S$ for this set of rational primes. Let us define $S_D \subseteq S$ to be the set of rational primes $p$ such that there is a specialization to the character of a hyperbolic Dehn surgery such that the quaternion algebra is ramified at some prime lying above $p$ so that knots satisfying condition $(\star)$ have $S_D$ of finite cardinality. When condition $(\star)$ fails it is shown in \cite{2} Theorem 1.1(3)] (using work of Harari \cite{7}) that $S$ is infinite. They furthermore state as a conjecture \cite{2} Conjecture 6.7] that

Conjecture 1.1 ([2] Conjecture 6.7]). Let $K$ be a hyperbolic knot in $S^3$ that fails condition $(\star)$, then, in the notation above, $S = S_D$.

The first example of a knot with infinite $S_D$ was given in \cite{13}. Our main result is to give an infinite family of twist knots that fail condition $(\star)$ and that have infinite $S_D$.

Theorem 1.2. Let $t \geq 2$, $K_t$ be a hyperbolic twist knot with $t$ half-twists. Suppose further that there exist distinct, rational, odd primes $p$ and $q$ such that

(1) $pq | \frac{t+1}{2}$, and
(2) $t \equiv -1 \mod pq$.

Set $T$ to be the set of rational primes $l$ such that there exists a place $l$ lying above $l$ of the trace field of some hyperbolic Dehn surgery $(d,0)$ at which the canonical quaternion algebra associated to that surgery is ramified. Then $T$ is infinite.

Remark 1.3. Infinitely many twist knots are covered by the theorem. For example, one can fix any pair of distinct, rational, odd primes $p$ and $q$ and consider the arithmetic progression $\{2pq + 1 + 2jpq \mid j \in \mathbb{Z}_{\geq 0}\}$.

Date: November 2, 2021.
1.1. Outline. The paper is organized as follows. We introduce some background material on character varieties, cyclotomic fields, quaternion algebras, and the Brauer group of fields and varieties in Sections 2 and 3. We then give an outline of the proof of Theorem 1.2 in Section 4 without giving proofs of intermediate steps. The remaining sections contain the proofs of the needed lemmas and propositions.

1.2. Acknowledgments. The author wishes to thank his advisor, Alan Reid, for his help and support throughout this project. The author also wishes to thank Neil Hoffman for pointing out some errors in earlier versions of this paper.

2. Character varieties

In this section we give some background on $\text{SL}_2\mathbb{C}$-character varieties of Kleinian groups, trace fields, quaternion algebras. We defer more details about quaternion algebras over fields and quaternion Azumaya algebras to Section 4.

2.1. Generalities. We begin by recalling that, for a finitely generated group $\Gamma$, the $\text{SL}_2\mathbb{C}$-representation variety of $\Gamma$ is $R(\Gamma) = \text{Hom}(\Gamma, \text{SL}_2\mathbb{C})$. Given a generating set $\{\gamma_i\}$, we identify a representation $\rho : \Gamma \to \text{SL}_2\mathbb{C}$ with $\rho(\gamma_1), \ldots, \rho(\gamma_n) \subset \text{SL}_2\mathbb{C}^n \subset \mathbb{C}^{4n}$. Given a different choice of generators, there is a canonical isomorphism between the two algebraic sets obtained this way. Fixing an element $\gamma \in \Gamma$, we may define a map $I_\gamma$ on $R(\Gamma)$ that associates to a representation $\rho$ the trace of $\rho(\gamma)$. That is, $I_\gamma : R(\Gamma) \to \mathbb{C}$ is defined by $I_\gamma(\rho) = \text{tr} \rho(\gamma) = \chi_\rho(\gamma)$. This is a regular function on the algebraic set $R(\Gamma)$, and the ring $T$ generated by all such $I_\gamma$ turns out to be finitely generated (see [4, Proposition 1.4.1]). Fixing a generating set $I_{\gamma_1}, \ldots, I_{\gamma_n}$ for $T$, define a map $t : R(\Gamma) \to \mathbb{C}^m$ by $t(\rho) = (I_{\gamma_1}(\rho), \ldots, I_{\gamma_m}(\rho))$. Then the $\text{SL}_2\mathbb{C}$-character variety of $\Gamma$ is defined to be $t(R(\Gamma)) \subset \mathbb{C}^m$. This is a closed algebraic set, and different choices of generators for $T$ give isomorphic algebraic sets.

In the case of $\Gamma$ equal to the fundamental group of a complement of a hyperbolic knot $K$ in $S^3$, we define its canonical component to be the irreducible component of $X(\Gamma)$ containing the character of the discrete and faithful representation of $\pi_1(S^3 \setminus K)$. We refer the reader to [4] for more detail.

Let us now fix some notation that we will use for the remainder of the paper. Let $K \subset S^3$ be a two-bridge knot. The fundamental group of $S^3 \setminus K$ can be generated by two meridians, $a$ and $b$, which are conjugate in $\pi_1(S^3 \setminus K)$. Any nonabelian representation $\rho$ of the knot group then can be conjugated to be of the form

$$\rho(a) = \begin{pmatrix} x & 1 \\ 0 & 1/x \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} x & 0 \\ r & 1/x \end{pmatrix}. $$

When $r = 0$, the representation is reducible. We use the variables

$$Z = \chi_\rho(a) = \chi_\rho(b) = x + \frac{1}{x}, \qquad R = \chi_\rho(ab^{-1}) = 2 - r. $$

2.2. Computation of the character varieties. We now collect some facts about the $\text{SL}_2\mathbb{C}$-character variety of the knot $K_t$. Most of this follows from work in [9], but we prove some further specifics that will be needed for later proofs. For the knots covered by Theorem 1.2 (and others), results in [9] show that there is only one component containing the character of an irreducible representation. As a matter of notation our knots $K_t$ are their knots $J(-t, 2)$. We will use their work to prove the following characterization of the defining polynomial for the canonical component.

**Proposition 2.1.** Let $t \geq 3$ be an odd positive integer. Write $f_t(R, Z)$ for the defining polynomial of the $\text{SL}_2\mathbb{C}$-character variety for the knot $K_t$. Then,

$$f_t(R, Z) = \begin{cases} R^t + (1 - Z^2) + \sum_{i=1}^{t-1} (a_i - b_i Z^2) R^i & \text{if } t \equiv 1 \text{ mod } 4 \\ R^t - 1 + \sum_{i=1}^{t-1} (a_i - b_i Z^2) R^i & \text{if } t \equiv 3 \text{ mod } 4, \end{cases}$$

where $a_i, b_i \in \mathbb{Z}$ and $a_{t-1} = b_{t-1} = 1$. In particular, $\deg_Z f_t = 2$. 

The proof is straightforward using results in [9], but their work requires some setup. The following definition is from [9, Definitions 3.1 and 3.2] except their $f$ and $g$ are our $\sigma$ and $\tau$, respectively, and we use $i$ to index rather than their $j$ or $k$.

**Definition 2.2.** Set $\sigma_0 = 0$, $\sigma_1 = 1$. For all other $i \in \mathbb{Z}$, define $\sigma_i \in \mathbb{Z}[u]$ by the relation $\sigma_{i+1} - u\sigma_i + \sigma_{i-1} = 0$. For all integers $i$, define $\tau_i = \sigma_i - \sigma_{i-1}$, $\Phi_3 = \sigma_i$, $\Phi_{2i-1} = \tau_i$, and $\Psi_i = \Phi_{i+1} - \Phi_{i-1}$.

**Lemma 2.3 ([9, Lemma 3.5]).** For any integer $i$, we have $\Phi_{i+2} = u\Phi_i - \Phi_{i-2}$, $\Phi_i = (-1)^{i+1}\Phi_{-i}$, and $\deg\Phi_i = \left\lfloor (i| - 1)/2 \right\rfloor$.

Using these notations, we may write down polynomials defining the $\text{PSL}_2 \mathbb{C}$- and $\text{SL}_2 \mathbb{C}$-character varieties.

**Proposition 2.4 ([9, Proposition 3.8]).** Let $\mu, \nu$ be any integers with $\nu$ even. Let $Y = \chi_\rho(a^2)$ and $R, Z$ be as in Section 3. The $\text{PSL}_2 \mathbb{C}$-character variety of $J(\mu, \nu)$ is isomorphic to the subvariety of $\Lambda^2$ cut out by the polynomial $h_{\mu, \nu}(R, Y) = \sigma_\xi(\theta) \left( \Phi_{-\mu}(R)\Phi_{\mu-1}(R) (Y - R) - 1 \right) + \sigma_{-\xi}(1)$, where $\theta = \Phi_{-\mu}(R)\Phi_{\mu}(R)(Y - R) + 2$ and $\xi = \nu/2$. The $\text{SL}_2 \mathbb{C}$-character variety is isomorphic to the double cover of the above model of the $\text{PSL}_2 \mathbb{C}$-character variety given by $Y = Z^2 - 2$.

Fortunately for us, the above formula cleans up significantly when we restrict attention to the family of twist knots $K_t = J(-t, 2)$. In particular, $\xi = 1$ in which case $\sigma_1 = 1$ and $\sigma_{-1} = 0$. This also allows us to ignore the $\theta$ variable. We summarize this as

**Lemma 2.5.** Let $t$ be a nonzero integer. The $\text{PSL}_2 \mathbb{C}$-character variety of the knot $K_t$ is given by $h_t(R, Y) = \Phi_t(R)\Phi_{-t-1}(R)(Y - R) - 1$.

**Proof of Proposition 2.4.** The content of Proposition 2.1 is

1. the $(R, Z)$-bidegree of $f_t(R, Z)$ is $(t, 2)$,

2. there are no $Z$ to the first power terms,

3. the coefficients of $R^2$ and $R^{t-1}$ are 1 and $(1 - Z^2)$ respectively, and

4. the constant term with respect to $R$ is $(1 - Z^2)$ when $t \equiv 1 \mod 4$ and $-1$ when $t \equiv 3 \mod 4$.

We note that the $R$-degree part of item 1 follows from Lemma 2.3 and the $Z$-degree part from Lemma 2.5 as the $\Phi_i$ family are univariate polynomials in $R$. We also get item 2 from Lemma 2.5. To prove items 3 and 4 we first show that $\Phi_i$ is of the form

$$\Phi_i(u) = \begin{cases} 0 & \text{if } i = 0 \\ u - u^{|i-1|} & \text{if } i \equiv 1, 7 \mod 8 \\ u^{|i-1|} - u & \text{if } i \equiv 3, 5 \mod 8 \\ \text{sgn}(i)u^{-1} + \lambda_iu^{-3} + \cdots + \lambda_{i-1}u & \text{if } i \not\equiv 0, i \equiv 0, 4 \mod 8 \\ \text{sgn}(i)u^{-1} - \lambda_iu^{-3} + \cdots + 1 & \text{if } i \equiv 2 \mod 8 \\ \text{sgn}(i)u^{-1} + \lambda_iu^{-3} + \cdots - 1 & \text{if } i \equiv 6 \mod 8, \end{cases}$$

where $\lambda_i \in \mathbb{Z}$. That is, when $i$ is odd, $\Phi_i$ is monic, its second leading coefficient is $-1$, and its constant term is $\pm 1$ depending on the residue class modulo 8 of $i$, and when $i$ is even, the leading coefficient is equal to the sign of $i$, the second leading coefficient is 0, and the constant term is 0 when $i$ is divisible by 4, 1 when $i \equiv 2 \mod 8$ and $-1$ when $i \equiv 6 \mod 8$. The degrees follow from Lemma 2.3. Moreover, note that it suffices to handle the cases of $i$ positive since we have the relation $\Phi_i = (-1)^{i+1}\Phi_{-i}$, so we henceforth assume $i$ positive. We use the base cases $\Phi_1(u) = \Phi_2(u) = 1$, $\Phi_3(u) = u - 1$, $\Phi_4(u) = u$, and $\Phi_5(u) = u^2 - u - 1$. We use the relation $\Phi_{i+2} = u\Phi_i - \Phi_{i-2}$ to see immediately that, when $i$ is even, $\Phi_{i+2}$ must be monic. To see that the second leading coefficient is 0 when $i$ is odd, we use the equality $\Phi_{i+2} = u\Phi_i - \Phi_{i-2}$ to find that the second leading coefficient of $\Phi_{i+2}$ is the same as that of $u\Phi_i$ because the second leading coefficient is the coefficient of $u$ to the power $(i - 2)/2$, but $\Phi_{i-2}$ has degree $(i - 4)/2$, so using the base case of $\Phi_4$, we see that
the second leading coefficient of $\Phi_i$ is 0 when $i$ is even. For $i$ odd, note that the relation $\Phi_{i+2} = u\Phi_i - \Phi_{i-2}$ implies that the leading coefficient of $\Phi_{i+2}$ is the same as that of $\Phi_i$ (and so equal to 1 by induction). Further the degree of $\Phi_{i-2}$ is $(i - 3)/2$, so it makes no contribution to the coefficient of $u^{i-2}$, which is the second leading term of $\Phi_{i+2}$. Then by the inductive hypothesis, we see that the second leading coefficient must be $-1$. To treat the constant term, note that $\Phi_{i+2}(0) = -\Phi_{i-2}$, so the constant term depends only on the residue class modulo 8. The base cases listed above combined with this observation handle all the constant terms.

Now we may prove item (3). Recall that $t$ is odd and positive, so $\Phi_t(R)$ is monic and $\Phi_{-t-1}(R)$ has leading coefficient $-1$. Note that the second leading coefficient of $\Phi_{t-1}(R)$ is 0, so the second leading coefficient of $\Phi_t(R)\Phi_{-t-1}(R)$ is the coefficient of $-R^{t-2}$ times $-R^{i+2}$, namely 1. We summarize this as

$$h_i(R, Y) = \Phi_t(R)\Phi_{-t-1}(R)(Y - R) - 1$$

$$= \left(-R^{t-1} + R^{t-2} + \cdots\right)(Y - R) - 1$$

$$= R^t + (-1 - Y)R^{t-1} + \cdots$$

Then we see that $h_i(R, Y)$ is monic is $R$ and after substituting $Y = Z^2 - 2$, the second leading coefficient is $(1 - Z^2)$.

For item (4) we first suppose that $t \equiv 1 \bmod 4$, so $t$ is equivalent to either 1 or 5 modulo 8. If $t \equiv 1 \bmod 8$, then $\Phi_t(0) = 1$ and $\Phi_{-t-1}(0) = -1$ as $-t - 1 \equiv 6 \bmod 8$. If $t \equiv 5 \bmod 8$, then $\Phi_t(0) = -1$ and $\Phi_{-t-1}(0) = 1$ since $-t - 1 \equiv 2 \bmod 8$. In either case, then, $h_i(0, Y) = -Y - 1$, which becomes $1 - Z^2$. If $t \equiv 3 \bmod 4$, then $-t - 1$ is divisible by 4, so $\Phi_{t-1}(0) = 0$, so $h_i(0, Y) = -1$. □

Next, we prove a lemma relating the character variety to the Alexander polynomial.

**Lemma 2.6.** Let $f_i$ be as above and $\Delta_{K_i}(x) = \left(\frac{t+1}{2}\right)x^2 - tx + \left(\frac{t+1}{2}\right)$ be the Alexander polynomial of $K_i$. Then,

$$f_i(2, x + x^{-1}) = \frac{-\Delta_{K_i}(x^2)}{x^2} = -\left(\left(\frac{t + 1}{2}\right)x^2 - t + \left(\frac{t + 1}{2}\right)x^{-2}\right).$$

**Proof.** We first note that

$$\Phi_i(2) = \begin{cases} 1 & i \text{ odd} \\ i/2 & i \text{ even} \end{cases}$$

Indeed, note that $\Phi_1(2) = \Phi_3(2) = 1$, $\Phi_0(2) = 0$, and $\Phi_2(2) = 1$. The specialized relation $\Phi_{i+2}(2) = 2\Phi_i(2) - \Phi_{i-2}(2)$ immediately handles the $i$ odd case. For $i$ even, we may induct and note that

$$\Phi_{i+2}(2) = 2\Phi_i(2) - \Phi_{i-2}(2)$$

$$= 2\left(\frac{i}{2}\right) - \frac{i - 2}{2}$$

$$= \frac{i + 2}{2}.$$ 

Now we compute using Lemma 2.5. We have $h_i(2, Y) = \left(-\frac{t - 1}{2}\right)(Y - R) - 1$. Then we substitute $Y = Z^2 - 2$ and $Z = x + x^{-1}$. After cleaning up, we get the desired equality. □

**2.3. Number Fields and Quaternion Algebras Associated to Subgroups of SL$_2$C.** We next turn to some background information about subgroups of SL$_2$C. A subgroup $\Gamma$ of SL$_2$C is non-elementary if its image in PSL$_2$C has no finite orbit in its action on $\mathbb{H}^3 \cup \mathbb{C}$. Given a non-elementary subgroup $\Gamma$ of SL$_2$C, we define its trace field by $k_\Gamma = \mathbb{Q}(\text{tr}\, \gamma | \gamma \in \Gamma)$ and quaternion algebra by the $k_\Gamma$-span of elements of $\Gamma$. That is,

$$A_\Gamma = \left\{ \sum_{\text{finite}} \alpha_i \gamma_i | \alpha_i \in k_\Gamma, \gamma_i \in \Gamma \right\}.$$
As shown in [10] p.78, we may write a Hilbert symbol for this quaternion algebra as
\[
\left( \frac{\chi(g)^2 - 4, \chi(g, h) - 2}{k} \right),
\]
where \(g, h\) are noncommuting hyperbolic elements of \(\Gamma\). In fact, this pointwise construction extends to define a quaternion algebra over the function field of the canonical component.

**Proposition 2.7 ([2 Corollary 2.9]).** Let \(\Gamma\) be a finitely generated group, and \(C\) an irreducible component of the character variety of \(\Gamma\) defined over the number field \(k\). Assume that \(C\) contains the character of an irreducible representation, and let \(g, h \in \Gamma\) be two elements such that there exists a representation \(\rho\) with character \(\chi_\rho \in C\) for which the restriction of \(\rho\) to \(\langle g, h \rangle\) is irreducible. Then the canonical quaternion algebra \(A_{k(C)}\) is described by the Hilbert symbol
\[
\left( \frac{I_g^2 - 4, I_{[g, h]} - 2}{k(C)} \right).
\]

3. **Algebraic number theory and cyclotomic fields**

In this section we collect some basic facts about number fields, cyclotomic fields, and their maximal totally real subfields that we will use in later sections. For context, the trace field of a \((d, 0)\) surgery always contains the maximally totally real subfield of the \(d\)-th cyclotomic field as a subfield, and we often leverage properties of this subfield and its elements for information about the trace field.

### 3.1. Number fields

We first fix some language. A **number field** is a finite degree extension of the rational numbers. For a number field of degree \(n\), there are \(n\) distinct embeddings into \(\mathbb{C}\) that fix \(\mathbb{Q}\). If all of these embeddings have image inside \(\mathbb{R}\), then the field is said to be **totally real**, and if none of them do, the field is **totally imaginary**. For \(L/K\) an extension of number fields, we will use an important function \(N_{L/K} : K \to K\) called the **field norm**. It is defined by
\[
N_{L/K}(x) = \prod \sigma(x),
\]
where the product is taken over embeddings \(\sigma : L \to \overline{K}\) that fix \(L\) element-wise and \(\overline{K}\) is an algebraic closure of \(K\). The norm behaves well in towers.

**Proposition 3.1 ([11 Corollary I.2.7]).** Let \(K \subseteq L \subseteq M\) be a tower of finite field extensions. Then,
\[
N_{M/K} = N_{L/K} \circ N_{M/L}.
\]

For an element \(x \in K\), a rational prime \(l\) divides \(N_{K/\mathbb{Q}}(x)\) if and only if there is a prime ideal \(l\) of \(K\) lying above \(l\) such that \(x \in l\). See the next subsection for a primer on ideals in number fields. One may efficiently compute norms if the minimal polynomial for an element is known. In particular, if \(p(t) \in \mathbb{Q}[t]\) is a monic minimal polynomial for \(x\), then \(N_{K/\mathbb{Q}}(x) = (-1)^{\deg p(0)}\). This observation is actually how we produce candidate primes that might ramify the relevant quaternion algebras.

### 3.2. Rings of integers and prime ideals

For a number field \(K\), the integral closure of \(\mathbb{Z}\) inside \(K\) is called the **ring of integers** of \(K\), and is often written \(\mathcal{O}_K\). This ring may be more concretely identified as the set of elements of \(K\) that satisfy a monic polynomial with coefficients in \(\mathbb{Z}\). The ring of integers is often not a unique factorization domain, but its ideals uniquely factor into prime ideals. By a “prime in a number field,” we will mean a prime ideal in the ring of integers of that number field. For an extension \(L/K\) of number fields and a prime \(l\) of \(\mathcal{O}_K\), the primes appearing in the factorization of \(l\mathcal{O}_L\) are said to **lie above** \(l\), and \(l\) **lies below** those primes of \(\mathcal{O}_L\).

For a prime \(l\) of \(\mathcal{O}_K\) with factorization
\[
l\mathcal{O}_L = \prod_i \mathfrak{p}_i^{e_i},
\]
the integer \(e_i\) is the **ramification index** of \(\mathfrak{p}_i\) over \(l\). There is an analogy between ramification of prime ideals in extensions and ramification of quaternion algebras, but they are distinct concepts. The degree of the field extension \(\mathcal{O}_L/\mathfrak{p}_i\) over \(\mathcal{O}_K/l\) is the **inertia degree** of \(\mathfrak{p}_i\) over \(l\). A fundamental fact is that if \(l\) splits
into \( r \) distinct primes in \( L \) with inertia degrees \( f_i \) and inertia degrees \( e_i \), then \( [L:K] = \sum_{i=1}^{r} e_i f_i \). When \( r = e_i = 1 \) for all \( i \), we say that \( I \) is totally inert or simply inert. When \( L/K \) is Galois, the ramification indices and inertia degrees for any given prime \( \mathfrak{p} \) above \( I \) are the same as any other prime \( \mathfrak{p}' \) above \( I \). In this setting, we simply write \( e \) and \( f \) for the ramification index and inertia degree of any prime above \( I \), and we have \( [L:K] = ref \), where \( r \) is the number of distinct primes that \( I \) splits into.

### 3.3. Cyclotomic fields

**A cyclotomic field** is a field extension obtained by adjoining roots of unity. All finite field extensions are cyclotomic. We shall write \( \zeta_d \) for a primitive \( d \)-th root of unity, and by the **cyclotomic field** \( \mathbb{Q}(\zeta_d) \), the field obtained by adjoining \( \zeta_d \) to \( \mathbb{Q} \). These fields and hence their subfields are abelian. For \( d \geq 3 \), \( \mathbb{Q}(\zeta_d) \) is totally imaginary, but it does have a totally real subfield generated by \( \zeta_d + \zeta_d^{-1} \). Moreover this subfield is maximal with respect to inclusion among totally real subfields, so it may be uniquely identified as the maximal totally real subfield of \( \mathbb{Q}(\zeta_d) \). We will often write \( 2 \cos(2\pi/d) \) for \( \zeta_d + \zeta_d^{-1} \) without a particular embedding of \( \zeta_d \) into \( \mathbb{C} \) in mind. We will also often write \( \mathbb{Q}(\zeta_d)^+ \) in place of \( \mathbb{Q}(2\cos(2\pi/d)) \). The rings of integers of \( \mathbb{Q}(\zeta_d) \) and \( \mathbb{Q}(\zeta_d)^+ \) are \( \mathbb{Z}[\zeta_d] \) and \( \mathbb{Z}[2\cos(2\pi/d)] \), respectively (see [16, Theorem 2.6, Proposition 2.16]).

We will use the following description of the splittings of primes in cyclotomic extensions.

**Theorem 3.2 (11, Proposition I.10.3).** Let \( l \) be a rational prime comprime to \( d \). Then \( l \) factors into distinct primes in \( \mathbb{Z}[\zeta_d] \) all with inertia degree equal to the multiplicative order of \( l \mod d \).

We emphasize some special cases of the above theorem. A rational prime \( l \) is totally split in \( \mathbb{Q}(\zeta_d) \) if and only if it is \( l \mod d \) and is totally inert if and only if it is a primitive root modulo \( d \). It follows that if \( l \in \mathbb{Z} \) is totally split in \( \mathbb{Q}(\zeta_d)^+ \) but is not equivalent to \( l \mod d \), then any prime \( I \) of \( \mathbb{Q}(\zeta_d)^+ \) above \( l \) is inert in \( \mathbb{Q}(\zeta_d) \).

### 4. Quaternion algebras, Azumaya algebras, and Brauer groups

#### 4.1. Quaternion algebras over fields

In this section we recall some facts about quaternion algebras and their generalization, Azumaya algebras. A **quaternion algebra** \( A \) over a field \( k \) is a 4-dimensional central simple algebra over \( k \). When \( k \) has characteristic different from 2, \( A \) can be described as an \( k \)-vector space with basis \( \{1, i, j, ij\} \) and algebra structure given by \( i^2 = a, j^2 = b, \) and \( ij = -ji \) where \( a, b \in k^* \). One may encode this information in a **Hilbert symbol** as \( (a,b/k) \). We will be primarily interested in the cases where \( k \) is either a number field arising as a trace field of Dehn surgeries on a knot or the function field of the canonical component of the \( \text{SL}_2 \mathbb{C} \)-character variety of a hyperbolic knot. The fundamental dichotomy for quaternion algebras is that they are either division algebras or matrix algebras. Let us collect some facts about quaternion algebras that we will use later.

**Proposition 4.1.** Let \( k \) be a field of characteristic not equal to 2 and \( a, b, x, y \in k^* \).

\[
\begin{align*}
(1) \quad & \left( \frac{a,b}{k} \right) \cong \left( \frac{b,a}{k} \right), \\
(2) \quad & \left( \frac{a,1}{k} \right) \cong M_2(k), \\
(3) \quad & \left( \frac{ax^2, by^2}{k} \right) \cong \left( \frac{a,b}{k} \right).
\end{align*}
\]

A quaternion algebra \( A \) over a number field \( k \) is determined up to isomorphism by the places \( I \) of \( Fk \) for which \( A_I = A \otimes_k k_I \) is a division algebra where \( k_I \) is the completion of \( k \) with respect to \( I \). The set of such \( I \) is finite and of even cardinality. We say \( A \) is ramified at these places and split at all the others. By abuse of notation, we occasionally write \( \left( \frac{a,b}{k_I} \right) = -1 \) when \( A \) is ramified at \( I \) and +1 when it is split. As a justification for this notation is that, we may break up the Hilbert symbols as follows.

\[
\left( \frac{a,bc}{k_I} \right) = \left( \frac{a,b}{k_I} \right) \left( \frac{a,c}{k_I} \right),
\]

which is essentially equivalent to quadratic reciprocity. This multiplicative notation can also be understood as equivalence in the Brauer group. In particular, \( \left( \frac{a,bc}{k} \right) \otimes_k M_2(k) \cong \left( \frac{a,b}{k} \right) \otimes_k \left( \frac{a,c}{k} \right) \), which is equivalence
in the Brauer group. We will also use this multiplicative notation for number fields where it should be interpreted as an equality of ramification sets. That is, \( \left( \frac{a, bc}{k} \right) = \left( \frac{a, b}{k} \right) \left( \frac{a, c}{k} \right) \) means that \( \left( \frac{a, bc}{k_1} \right) = \left( \frac{a, b}{k_1} \right) \left( \frac{a, c}{k_1} \right) \) for every prime \( l \) of \( k \). There is also an efficient way to compute ramification sets, which is another avatar of quadratic reciprocity.

**Theorem 4.2** ([10 Theorem 2.2.6(b)]). Let \( A \) be a quaternion algebra over a nondyadic \( l \)-adic field \( k_1 \) with ring of integers \( O \) and maximal ideal \( l \). Let \( A = \left( \frac{a, b}{k_1} \right) \) with \( a, b \in O \). If \( a \notin l \) and \( b \in l \setminus l^2 \), then \( A \) splits if and only if \( a \) is a square modulo \( l \).

Let us also point out that quaternion algebras generate the 2-torsion of the Brauer group of the field \( k \).

### 4.2. Azumaya algebras

For a Noetherian scheme \( X \), its **Brauer group** \( \text{Br} \ X \) is defined to be \( H^2_{\text{ét}}(X, G_m) \). We will have no need for the details of étale cohomology, and in this paper one may think of \( X \) as being the canonical component of a hyperbolic knot, or a smooth model thereof.

We now wish to define a generalization of quaternion algebras over fields. Let \( O_X \) be the structure sheaf of \( X \) so that \( O(U)_X \) is the ring of regular functions on \( U \). A coherent sheaf of \( O_X \) algebras is a sheaf \( F \) of abelian groups on \( X \) such that \( F(U) \) is a finitely generated \( O_X \) algebra and the restriction maps are compatible with the algebra structure. Moreover, \( F \) is locally free if it has an open covering by sets \( U \) such that \( F|_U \) is a free \( O_X|_U \)-module. An **quaternion Azumaya algebra** is a nonzero \( O_X \) algebra that is locally free of rank 4.

The connection to quaternion algebras over fields is that when \( X \) is a variety over a field \( k \) characteristic not equal to 2 and \( A \) is a quaternion Azumaya algebra, there is a finite open covering of \( X \) by sets \( U \) such that for each \( U \), there is an isomorphism of \( O_X|_U \)-modules

\[
A|_U \cong O_U \oplus iO_U \oplus jO_U \oplus ijO_U,
\]

where \( i^2 = f_U, j^2 = g_U \), and \( ij = -ji \) for \( f_U, g_U \in k[U]^* \). So quaternion Azumaya algebras locally look like quaternion algebras. Moreover, one can take the fiber at a point \( A(x) = A \otimes_{O_X} k(x) \) where \( k(x) \) is the residue field to obtain a quaternion algebra over the residue field.

Writing \( k(X) \) for the function field of \( X \), there is a canonical injection \( \text{Br} \ X \hookrightarrow \text{Br} k(X) \) and an exact sequence which determines its image.

**Theorem 4.3** ([12 Theorem 6.8.3.]). Let \( X \) be a regular integral Noetherian scheme. Let \( X^{(1)} \) be the set of codimension 1 points of \( X \). Then the sequence

\[
0 \longrightarrow \text{Br} \ X \longrightarrow \text{Br} k(X) \xrightarrow{\text{res}} \bigoplus_{x \in X^{(1)}} H^1(k(x), \mathbb{Q}/\mathbb{Z})
\]

is exact with the caveat that one must exclude the \( p \)-primary part of all the groups if \( X \) is of dimension \( \leq 1 \) and some \( k(x) \) is imperfect of characteristic \( p \), or if \( X \) is of dimension \( \geq 2 \) and some \( k(x) \) is of characteristic \( p \).

This theorem is known as absolute cohomological purity. It was conjectured by Grothendieck and proved by Gabber, though the above formulation appears in [12]. The last arrow is the residue homomorphism to the Galois cohomology group \( H^1(k(x), \mathbb{Q}/\mathbb{Z}) = H^1(\text{Gal}(k(x)^{\text{sep}}/k(x), \mathbb{Q}/\mathbb{Z}) \). We say that a quaternion algebra \( A_{k(X)} \) defined over the function field \( k(X) \) “extends” over a point \( x \in X \) if its residue is trivial at \( x \). The exact sequence in Theorem 4.3 says that \( A_{k(X)} \) extends to a quaternion Azumaya algebra if and only if its residue is trivial everywhere. For quaternion algebras over function fields, the residues may be calculated using a tame symbol at least when the residue field has characteristic different from 2. Namely, let \( \alpha, \beta \in k(X) \) and \( x \) be a codimension 1 point, and write

\[
\{\alpha, \beta\} = (-1)^{\text{ord}_x(\alpha) \text{ord}_x(\beta) / \text{ord}(\alpha)} \frac{\alpha^\text{ord}(\beta)}{\beta^\text{ord}(\alpha)} \in k(x)^*/k(x)^{x^2},
\]

where \( \text{ord}_x(\alpha) \) is the order of vanishing of \( \alpha \) at \( x \). Then this class in \( k(x)^*/k(x)^{x^2} \) is equal to the residue of \( \left( \frac{\alpha, \beta}{k(X)} \right) \) at \( x \). In particular, if this class is the trivial square class, then the algebra extends over \( x \). See [3 §2] for details.
An important property of Azumaya algebras of varieties over number fields is that their fibers, which are quaternion algebras over number fields, can only ramify at a finite set of places. We give the statement that appears in [15] Theorem 2.4(2), though we point out that it holds for any Azumaya algebra, not just the quaternion ones.

**Theorem 4.4.** Let $X$ be a smooth projective irreducible variety over a number field $k$, and let $\mathcal{A}$ be a quaternion Azumaya algebra on $X$. Then, for almost all places $\frak{P}$, we have $\mathcal{A}(\frak{P}) \cong M_2(k_{\frak{P}})$ for all $\frak{P} \in X(k_l)$.

However, work of Harari ([7]) shows that if $A_k(X)$ has a residue, then there are infinitely many places $\frak{P}$ for which there is a nontrivial fiber at some local point.

### 4.3. Connection to Kleinian groups

We now explain the connection between the Azumaya algebra machinery and Kleinian groups. We refer the reader to [2] for more details. Let $C$ denote the canonical component of a hyperbolic knot $K$. As mentioned in the introduction, there is always a quaternion algebra defined over the function field of the canonical component that specializes at a character of a hyperbolic Dehn surgery to the usual quaternion algebra of a Kleinian group. A natural question to ask is whether this quaternion algebra extends to an Azumaya algebra. The answer for hyperbolic knot complements is that it extends if and only if the Alexander polynomial satisfies condition $\star$ of [2].

**Theorem 4.5** ([2] Theorems 1.2., 1.4.). Let $K$ be a hyperbolic knot with $\Gamma = \pi_1(S^3 \setminus K)$, and suppose that $\Delta_K$ satisfies condition $\star$. Then

1. $A_{k(C)}$ comes from an Azumaya algebra in $Br \hat{C}$ where $\hat{C}$ denotes the normalization of the projective closure of $C$.

2. Furthermore, if the canonical component is defined over $\mathbb{Q}$, there exists a finite set $S_K$ of rational primes such that, for any hyperbolic Dehn surgery $N$ on $K$ with trace field $k_N$, the $k_N$-quaternion algebra $A_N$ can only ramify at real places of $k_N$ and finite places lying over primes in $S_K$.

For example, the authors calculate in [2] that the figure-eight knot can have only real and dyadic ramification. There is also a partial converse in [2] (Theorems 1.2, 1.4), namely that $A_{k(C)}$ does not extend when the knot fails condition $\star$. With the results of [7], this implies that one can obtain ramification above infinitely many rational primes by specializing $A_{k(C)}$. However, these points a priori need not be interesting from the point of view of geometric structures. Experimental evidence led them to conjecture (Conjecture 1.1) that when the knot fails condition $\star$, there should be ramification above infinitely many rational primes, even when one restricts attention to Dehn surgery points.

### 4.4. Ramification for Dehn surgery points

We now prove that the ramification of the specializations to $(d,0)$ surgery can be expressed in terms of the following Hilbert symbol. Throughout, we write $r_d$ for the algebraic number that $r$ specializes to at $(d,0)$ surgeries to avoid confusion with the coordinate $r = 2 - R$.

**Proposition 4.6.** Let $d$ be an odd positive integer that is not a power of a prime and suppose that $K$ is a 2-bridge knot whose Alexander polynomial has only simple roots and is Azumaya negative. Let $k_d$ be the trace field of the $(d,0)$ surgery and $r_d$ as above. Then, there is a finite set $S$ of rational primes such that for a prime $\mathfrak{L}$ of $k_d$ lying above a prime not in $S$, the ramification of the (invariant) quaternion algebra for the $(d,0)$ surgery on $K$ agrees at $\mathfrak{L}$ with Hilbert symbol

\[
\left( \frac{2 \cos(2\pi/d) - 2, -r_d}{k_d} \right).
\]

**Remark 4.7.** Proposition 4.6 implies that if there are infinitely many primes $\frak{P}$ as $d$ varies of different residue characteristics at which

\[
\left( \frac{2 \cos(2\pi/d) - 2, -r_d}{k_d} \right),
\]

is ramified, then the (invariant) quaternion algebras for the $(d,0)$ surgeries have infinitely many different ramified residue characteristics as $d$ varies.

**Proof of Proposition 4.6.** In general the Hilbert symbol at a representation $\rho$ is given (see Proposition 2.7) by

\[
\left( \frac{\chi_\rho(a)^2 - 4, \chi_\rho([a,b]) - 2}{k_\rho} \right).
\]
Using the coordinates $Z$ and $R$ defined above, this looks like

$$
\left( \frac{Z^2 - 4,2Z^2 + R^2 - Z^2 R - 4}{k(C)} \right) = \left( \frac{Z^2 - 4, R - 2}{k(C)} \right) \left( \frac{Z^2 - 4, R + 2 - Z^2}{k(C)} \right).
$$

For notational convenience, call the leftmost symbol in Equation 8 $A$, the first symbol to the right of the equals sign $B$, and the rightmost symbol $C$. We claim that $C$ extends to an Azumaya algebra. Indeed, its two entries vanish only at the points determined by $R = 2$, $Z = \pm 2$, and $Z^2 = R + 2$. For $R = 2$, note that $C$ has trivial residue there. In fact specializing to $R = 2$ makes the second entry $4 - Z^2$, so that the algebra is split (see [10, Corollary 2.3.3]) at all specializations outside of $Z = \pm 2$, which we treat later. Then, we find that the $B$ retains the nontrivial residue at $R = 2$. Moreover, $C$ a priori might have a nontrivial residue at $Z^2 = R + 2$, but neither $A$ nor $B$ does, so neither does the rightmost symbol. Finally, $B$ and $C$ have nontrivial residue at $Z = \pm 2$. However, when $Z = \pm 2$, $R = 2$ is a global square in the residue field. Indeed, since $a$ and $b$ are conjugate in the fundamental group, there is a conjugation

$$
\left( \begin{array}{cc}
\alpha & \beta \\
\gamma & \delta
\end{array} \right) \left( \begin{array}{cc}
1 & 1 \\
0 & 1
\end{array} \right) \left( \begin{array}{cc}
\delta & -\beta \\
-\gamma & \alpha
\end{array} \right) = \left( \begin{array}{cc}
1 & 0 \\
r & 1
\end{array} \right).
$$

Multiplying everything out on the left-hand side yields an $\alpha^2$ in the upper right entry, so $\alpha = 0$, which allows us to obtain

$$
\left( \begin{array}{cc}
0 & \beta \\
\gamma & \delta
\end{array} \right) \left( \begin{array}{cc}
1 & 1 \\
0 & 1
\end{array} \right) \left( \begin{array}{cc}
\delta & -\beta \\
-\gamma & \alpha
\end{array} \right) = \left( \begin{array}{cc}
-\beta \gamma & 0 \\
-\gamma^2 & -\beta \gamma
\end{array} \right) = \left( \begin{array}{cc}
1 & 0 \\
-r^2 & 1
\end{array} \right).
$$

Note further than $\gamma$ is in the trace field of any representation with $Z = 2$. Indeed, writing $\rho(c)$ for the element effecting the above conjugation (so $\rho(cac^{-1}) = \rho(b)$), $\gamma + \delta$ and $\delta - \gamma$ are the traces of $\rho(ca)$ and $\rho(ac^{-1})$, respectively. So $r = -\gamma^2$ implying $R = 2 = \gamma^2$, which is a global square in the trace field of the representation.

This implies that the tame symbol (see Subsection 1.2) and hence the residue is trivial. A similar argument handles $Z = -2$. Since $A$ has trivial residue at $Z = \pm 2$ and $B$ does too, then $C$ must have trivial residue there as well. Then $C$ extends to an Azumaya algebra, so by Theorem 4.4 there is a finite set $S$ of rational primes such that if $l \notin S$, then no specialization of the second symbol is ramified at a prime above $l$. That is for $l \notin S$ and $l$ above $l$, the ramification of $A$ and $B$ agree.

Specializing to $(d, 0)$ surgery sends $Z$ in as $2 \cos(2\pi/d)$, so $B$ specializes to

$$
\left( \frac{4 \cos^2(\pi/d) - 4, R_d - 2}{k_d} \right) = \left( \frac{2 \cos(2\pi/d) - 2, R_d - 2}{k_d} \right),
$$

where $R_d = 2 - r_d$. The above equality follows from the fact that when $d$ is odd, $2 \cos(2\pi/d) + 2$ is a global square in $\mathbb{Q}(\zeta_d)^+$, which is a subfield of $k_d$. One of its square roots is $\zeta_d^{d+1} + \zeta_d^{-d+1}$. Changing $R_d - 2$ to $-r_d$ completes the proof.

\[ \square \]

5. Proof of Theorem 1.2

The basic strategy for proving Theorem 1.2 is as follows. Proposition 4.6 gives an explicit description for the Hilbert symbol of $(d, 0)$ surgeries on the knots. In Lemma 5.1 we use that Hilbert symbol to determine places that the associated quaternion algebra is ramified at in terms of splitting conditions on the primes diving $r_d$. Then, in Lemmas 5.2 and 5.3 we give conditions for a prime to divide $r_d$ and for it to satisfy the appropriate splitting conditions coming from Lemma 5.1, respectively. Finally Lemmas 5.4 and 5.5 show how to find infinitely many such primes. The remainder of the section states these intermediate steps and explains how they add up to a proof of Theorem 1.2.

Theorem 1.2 then will follow once we can prove that there are infinitely many rational primes that are residue characteristics of ramified primes of the quaternion algebra determined $\left( \frac{2 \cos(2\pi/d) - 2, -r_d}{k_d} \right)$ for some $d$. The next lemma describes the ramification of this quaternion algebra in terms of the splitting of primes between $\mathbb{Q}(\zeta_d)^+ = \mathbb{Q}(\zeta_d + \zeta_d^{-1})$ and $k_d$. 
Lemma 5.1. Let \( r \) be an algebraic integer inside some fixed finite extension \( k_d/Q(\zeta_d)^+ \) for \( n \) odd. Suppose that \( \Sigma \) is a prime of \( k_d \) that does not lie above 2 or \( d \), divides \( -r_d \) an odd number of times, and has odd inertia degree over \( Q(\zeta_d)^+ \). Suppose further that \( l = \Sigma \cap Q(\zeta_d)^+ \) does not split in \( Q(\zeta_d) \). Then

\[
\left( \frac{2 \cos(2\pi/d) - 2, -r_d}{k_d} \right)
\]

is ramified at \( \Sigma \).

To prove that the quaternion algebra at the \((d,0)\) surgery is ramified at a prime \( \Sigma \) of the trace field that lies above neither 2 nor \( d \), it suffices to show:

1. \( \Sigma \) divides \(-r_d\) and odd number of times,
2. \( \Sigma \) has odd inertia degree over \( Q(\zeta_d)^+ \), and
3. \( l = \Sigma \cap Q(\zeta_d)^+ \) does not split in \( Q(\zeta_d) \).

Theorem 1.2 will follow if we can arrange these conditions for primes above infinitely many distinct rational primes as we vary \( d \).

To handle conditions (1) and (2), we exploit a connection to the Alexander polynomial of the knot. To find primes dividing \( r_d \), we compute its field norm, \( N_{k_d/Q}(r_d) \). The (absolute) field norm will be a rational integer whose prime divisors correspond to prime ideals dividing \( r_d \). To compute this norm, we first find the relative field norm, \( N_{k_d/Q(\zeta_d)^+}(r_d) \), which can be expressed in terms of the Alexander polynomial of the knot.

Recall from Section 4 that \( N_{k_d/Q(\zeta_d)^+}(r_d) = N_{Q(\zeta_d)^+}/Q(N_{k_d/Q(\zeta_d)^+}(r_d)) \) and that the Alexander polynomial of the knot \( K_t \) is \( \Delta_{K_t}(x) = \left( \frac{t+1}{2} \right) x^2 - tx + \left( \frac{t+1}{2} \right) \).

Lemma 5.2. Let \( d \) be odd, \( k_d \) the trace field of the \((d,0)\) surgery of a hyperbolic twist knot \( K_t \). Then the norm of \( r_d \) in the relative extension \( k_d/Q(\zeta_d)^+ \) is \( \Delta_{K_t}(\zeta_d^2) = \left( \frac{t+1}{2} \right) \zeta_d^4 - t\zeta_d^2 + \left( \frac{t+1}{2} \right) \) for all but finitely many \( d \).

The proof of the above lemma involves being able to prove that specializing the character variety at \( Z = 2 \cos(2\pi/d) \) produces an irreducible polynomial over the field \( Q(\zeta_d)^+ \). Calculation of the character variety can be found above in Section 2, and irreducibility of the relevant specializations is treated in Section 7. This irreducibility also somewhat justifies the notation \( r_d \) as it represents an algebraic number that is well defined up to Galois conjugation. We are still left to find rational primes dividing the absolute norm, \( N_{k_d/Q}(r_d) \). This will be done in Lemma 5.3 once we may state precisely which rational primes ensure the desired ramification.

To handle condition (2) about the inertia degree, we use the following lemma.

Let \( d \) be odd and that \( l \) is an odd rational prime coprime to \( d \) dividing \( N_{Q(\zeta_d)^+}/Q(\Delta_{K_t}(\zeta_d^2)) \) an odd number of times. Then there is a prime \( \Sigma \) of \( k_d \) above \( l \) such that \( \Sigma \) divides \(-r_d\) and odd number of times and \( \Sigma \) has odd inertia degree over \( Q(\zeta_d)^+ \).

The next lemma applies Lemma 5.3 to cast condition (3) also in terms of the Alexander polynomial.

Lemma 5.4. Suppose that \( d \) is odd and that \( l \) is a rational prime below a prime dividing \( \Delta_{K_t}(\zeta_d^2) \). Suppose further that \( l \) and \( d \) are coprime to \( t \) and \( \frac{t+1}{2} \). Then \( l \) is totally split in \( Q(\zeta_d)^+ \). Hence, if \( l \not\equiv 1 \mod d \), then all primes of \( Q(\zeta_d)^+ \) above \( l \) are inert in \( Q(\zeta_d) \).

We work with \( d \) of the form \( d = p^u q^v \) for \( p, q \) as in the statement of Theorem 1.2 and \( u, v \) integers. Our work so far says that if a rational prime \( l \) divides \( N_{Q(\zeta_d)^+}/Q(\Delta_{K_t}(\zeta_d^2)) \) an odd number of times and is not equivalent to 1 mod \( pq \), then there is some prime \( \Sigma \) of \( k_d \) above \( l \) at which the quaternion algebra for the \((d,0)\) surgery is ramified. We have not yet proved that any such \( l \) exist. The next lemma shows that we may find infinitely many. Its proof combines an analysis of the resultant of the Alexander polynomial with the cyclotomic polynomials and a dynamical result of Furstenberg appearing in [6].

Lemma 5.5. Let \( t \in Z_{\geq 0} \) be odd, \( \Delta(x) = \left( \frac{t+1}{2} \right) x^2 - tx + \left( \frac{t+1}{2} \right) \in Z[x] \). Let \( p, q \) be distinct, rational, odd primes and suppose that \( \Delta(x) \equiv 1 \mod pq \). Then there are infinitely many positive integers \( d \) for which \( N_{Q(\zeta_d)^+}/Q(\Delta(\zeta_d^2)) \) is divisible by a rational prime \( l \) an odd number of times and \( l \not\equiv 1 \mod pq \).

Fixing an integer \( t \geq 2 \), we apply Lemma 5.5 using the polynomial \( \Delta_{K_t}(x) = \left( \frac{t+1}{2} \right) x^2 - tx + \left( \frac{t+1}{2} \right) \), which is the Alexander polynomial of \( K_t \). Then for each of the \( d \) produced by Lemma 5.5, the quaternion algebra
for the \((d, 0)\) surgery is ramified at some prime with residue characteristic \(l\) as in the statement of Lemma 5.5. The proof of Theorem 1.2 will be complete one we show (see Lemma 6.2 for details) that each such \(l\) can only occur for finitely many \(d\).

6. Ramification

In this section, we prove Lemmas 5.1, 5.3, 5.4, and 5.5.

**Lemma 6.1.** If \(n\) is an odd positive integer and \(l\) is a prime ideal of \(\mathbb{Q}(\zeta_d)^+\), then \(2\cos(2\pi/d) - 2\) is a nonsquare modulo \(l\) if and only if \(l\) is inert in \(\mathbb{Q}(\zeta_d)^+\).

**Proof.** Note that \(2\cos(2\pi/d) - 2\) is not a global square in \(\mathbb{Q}(\zeta_d)^+\) as it is negative at the real embeddings. It is, however, a global square in \(\mathbb{Q}(\zeta_d)\). To see this, note that when \(d\) is odd, \(\zeta_d^{(d+1)/2} \in \mathbb{Q}(\zeta_d)\), and

\[
\left(\zeta_d^{(d-1)/2} (\zeta_d - 1)\right)^2 = \zeta_d^{d+1} - 2\zeta_d^{(d+1)/2 + (d-1)/2} + \zeta_d^{d-1}
= 2\cos(2\pi/d) - 2.
\]

So if \(l\) splits (or ramified) in \(\mathbb{Q}(\zeta_d)\), then \(\mathbb{Z}[2\cos(2\pi/d)]/l\) coincides with a quotient of \(\mathbb{Z}[\zeta_d]\) wherein \(2\cos(2\pi/d) - 2\) is a square. On the other hand if \(l\) is inert, then the finite field containing the square root of the reduction of \(2\cos(2\pi/d) - 2\) modulo \(l\) is a proper extension of \(\mathbb{Z}[2\cos(2\pi/d)]/l\). That is, if \(2\cos(2\pi/d) - 2\) is a nonsquare modulo \(l\).

**Proof of Lemma 5.1.** This ramification is equivalent to \(2\cos(2\pi/d) - 2\) being a nonsquare modulo \(l\) by Theorem 1.2. By hypothesis, the inertia degree is odd, so the residue field has odd degree over the finite field \(\mathbb{Z}[2\cos(2\pi/d)]/l\). Moreover, since \(l\) is inert in \(\mathbb{Q}(\zeta_d)\), \(2\cos(2\pi/d) - 2\) is a nonsquare modulo \(l\) by Lemma 6.1. Then no odd degree extension of \(\mathbb{Z}[2\cos(2\pi/d)]/l\) can contain a square root of \(2\cos(2\pi/d) - 2\), so it is a nonsquare modulo \(l\).

**Proof of Lemma 5.3.** Consider the norm absolute norm \(N_{l}/\mathbb{Q}(-r)\). By Lemma 5.2,

\[
N_{l}/\mathbb{Q}(-r) = N_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q} \left(N_{l}/\mathbb{Q}(\zeta_d)^+(-r)\right)
= N_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(\Delta_K(\zeta_d^2)).
\]

Now suppose that \(l\) divides \(N_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(\Delta_K(\zeta_d^2))\) an odd number of times. Then there is a prime \(l\) of \(l\) of odd inertia degree over \(\mathbb{Q}\) and hence over \(\mathbb{Q}(\zeta_d)^+\).

**Lemma 6.2.** Let \(d\) be odd and \(l\) be a rational prime lying below a prime of \(\mathbb{Q}(\zeta_d)\) dividing \(\Delta_K(\zeta_d^2)\). Then \(l\) has multiplicative order either 1 or 2 modulo \(d\).

**Proof.** Write \(l\) for a prime of \(\mathbb{Q}(\zeta_d)\) above \(l\). Note that \(\Delta_K(\zeta_d^2)\) is conjugate to \(\Delta_K(\zeta_d)\) over \(\mathbb{Q}(\zeta_d)\) as long as \(d\) is odd. After multiplying by roots of unity, we may assume that \(l\) divides the ideal generated by \(t \Delta_K(\zeta_d, \zeta_d^{-1}) - t\). Observe that \(l\) cannot divide \(t \Delta_K(\zeta_d, \zeta_d^{-1}) - t\) because this implies \(t \Delta_K = 0 \mod l\), but then \(l\) divides \(t\) and \(t + 1\). Similarly, \(l\) cannot divide \(t\) as this implies \((t+1)^2 \zeta_d + \zeta_d^{-1} \equiv 0 \mod l\), but \(\zeta_d + \zeta_d^{-1}\) is a unit for \(d\) odd, so this implies \(t + 1 \equiv 0 \mod l\).

Recall that the multiplicative order of \(l\) modulo \(d\) is equal to the inertia degree of \(l\) in \(\mathbb{Q}(\zeta_d)\) by Theorem 3.2, so the result will follow once we show that the degree of \(\mathbb{Z}[\zeta_d]/l\) over \(\mathbb{F}_l\) is 1 or 2. Now, \(\Delta_K(\zeta_d^2)\) has 3 nonzero terms, so \(\Delta_K(\zeta_d^2)\) dying modulo \(l\) forces a linear dependence modulo \(l\) of \(\{1, \zeta_d, \zeta_d^2\}\), so the finite field obtained by reducing modulo \(l\) must have degree only 1 or 2 above its prime subfield.

**Remark 6.3.** It follows from Lemma 6.2 that if we fix \(f\) as in the lemma, a given prime \(l\) can only have a prime above it in \(\mathbb{Q}(\zeta_d)\) dividing \(\Delta_K(\zeta_d^2)\) for finitely many values of \(d\) unless \(l\) divides \(d\) itself infinitely often as \(d\) varies. In applying Lemma 5.5, we will take \(d\) equal to \(p^u q^v\) for \(p, q\) fixed distinct, odd rational primes and vary the powers \(u\) and \(v\). The primes \(l\) produced will be \(-1 \mod pq\), so in particular they do not divide \(d\).

**Proof of Lemma 5.4.** By Lemma 6.2, we know that \(l\) has multiplicative order either 1 or 2. Write \(l\) for a prime of \(\mathbb{Q}(\zeta_d)^+\) above \(l\) that divides \((t+1)\zeta_d + \zeta_d^{-1} - t\). Note that since \(d\) is odd, \((t+1)\zeta_d + \zeta_d^{-1} - t\) is Galois conjugate to \((t+1)\zeta_d + \zeta_d^{-1} - t\). Recall that \(\mathbb{Z}[\zeta_d + \zeta_d^{-1}]\) is the ring of integers of \(\mathbb{Q}(\zeta_d)^+\), and consider the reduction map \(\mathbb{Z}[\zeta_d + \zeta_d^{-1}] \rightarrow \mathbb{Z}[\zeta_d + \zeta_d^{-1}]/l\). Then \((t+1)\zeta_d + \zeta_d^{-1} - t\) is in the kernel of this
Lemma 6.4. Let \( f \) and \( i \) be distinct odd primes, \( t \) as in the statement of Theorem 1.2, \( n \) an odd positive integer, and \( f(x) = (\frac{t+1}{2})x^2 - tx + (\frac{t+1}{2}) \). Further, let
\[
\begin{align*}
    w &= \frac{1}{\sqrt{2(t+1)}} \left( \sqrt{2t+1} + i \right) \\
    y &= \sqrt{\frac{t+1}{2}} w.
\end{align*}
\]
Then
1. \( w \) is a square root of a root of \( f \).
2. \( i (\sqrt{y^n} - y^n) \in \mathbb{Z} \), and
\[
i (\sqrt{y^n} - y^n) = \begin{cases} 
1 \mod pq & n \equiv 1 \mod 4 \\
-1 \mod pq & n \equiv 3 \mod 4.
\end{cases}
\]

Proof: The assertion that \( w \) is a square root of a root of \( f \) may be checked by direct calculation or with software. We note as well here that \( |w| = 1 \) as \( t \) was assumed real and positive in the statement of Theorem 1.2. For the second claim, we first show that \( i (\sqrt{y^n} - y^n) \) is an integer. Consider the resultant
\[
\begin{align*}
\text{res}_x \left( x^n - 1, f(x^2) \right) &= \text{res}_x \left( x^n - 1, \frac{t+1}{2} (x-w)(x+w)(x-w) \right) \\
&= \text{res}_x \left( x^n - 1, \sqrt{\frac{t+1}{2}} (x-w)(x+w) \right) \text{res}_x \left( x^n - 1, \sqrt{\frac{t+1}{2}} (x+w)(x-w) \right).
\end{align*}
\]
We first observe that the two factors above are equal in absolute value. Indeed, recalling that \( n \) is assumed odd, we compute
\[
\text{res}_x \left( x^n - 1, \sqrt{\frac{t+1}{2}} (x-w)(x+w) \right) = \left( \sqrt{\frac{t+1}{2}} \right)^n (w^n - 1) (\mp w^n - 1) = \left( \sqrt{\frac{t+1}{2}} \right)^n (-w^2)^n - w^n + 1 = (\sqrt{y^n} - y^n).
\]
Similarly the other factor of \( \text{res}_x \left( x^n - 1, f(x^2) \right) \) is the complex conjugate of the one just considered, so the two factors are equal in absolute value. They also lie on the imaginary axis, so multiplying by \( i \) moves them to the real axis. Then, that \( i (\sqrt{y^n} - y^n) \) is an integer will follow once we show that \( \text{res}_x \left( x^n - 1, f(x^2) \right) \) is a square integer. Indeed, writing \( \Phi_d \) for the \( d \)th cyclotomic polynomial, we have
\[
\text{res}_x \left( x^n - 1, f(x^2) \right) = \prod_{d\mid n} \text{res}_x (\Phi_d(x), f(x^2)) = \prod_{d\mid n} N_{Q(\zeta_d)/Q(f(\zeta_d^2))}.
\]
Since \( f \) is an integer polynomial, \( f(\zeta_d^2) \) is an algebraic integer, so its norm is in \( \mathbb{Z} \). Furthermore, \( f(\zeta_d^2) \) is in \( Q(\zeta_d)^+ \), which has \( Q(\zeta_d) \) as a quadratic extension, so that its norm in \( Q(\zeta_d)/Q \) must be a square. So then, \( i (\sqrt{y^n} - y^n) \) is a real square root of a square integer. That is, \( i (\sqrt{y^n} - y^n) \in \mathbb{Z} \).

To show the claim about the residue modulo \( pq \), the strategy is to first show that \( i (\sqrt{y} - y) \equiv 1 \mod pq \) and \( i (\sqrt{y} - y) \equiv -1 \mod pq \), then show that \( y^5 \equiv y \mod pq \) and \( y^5 \equiv y \mod pq \). We compute \( i (\sqrt{y} - y) = 1 \)
and \( i(\sqrt[3]{y} - y^3) = (3m + 1)/2 \). However, since \( pq \mid t + 1 \) and \( t \equiv -1 \mod pq \), we have that \( (3t + 1)/2 = t + 1/2 + 1 \equiv -1 \mod pq \). Now we turn to showing that \( y^5 \equiv y \mod pq \). We remark that this reduction is slightly more delicate since \( y \) is not a rational (or in fact an algebraic) integer, so the reduction map is really \( \mathcal{O}[1/2] \to \mathcal{O}[1/2]/(pq) \), where \( \mathcal{O} \) is the ring of integers of the extension \( \mathbb{Q}(\sqrt[5]{t+1}, i) \). However, we may still compute

\[
y^5 = \frac{1}{5} \left( (t^2 - 4t - 1) \sqrt{2t + 1} + i \left( 5t^2 - 1 \right) \right),
\]

and observe that \( t^2 - 4t - 1 \equiv 5t^2 - 1 \equiv 4 \mod pq \), so since

\[
y = \frac{1}{2} \left( \sqrt{2t + 1} + i \right),
\]

we deduce that \( y^5 \equiv y \mod pq \). The analogous computation shows that \( \sqrt[5]{y} \equiv \sqrt[5]{y} \mod pq \). □

Lemma 6.5. Let \( t, f, w, \) and \( y \) be as in Lemma 6.4. If \( n \equiv 1 \mod 4 \), then

\[
\prod_{d \mid n} \mathbb{N}_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(f(\zeta_d^2)) = i(\sqrt[n]{y} - y^n) = 2 \Im(y^n) = 2 \left( \frac{t + 1}{2} \right)^n \Im(y^n).
\]

Proof. As in the proof of Lemma 6.4, \( (i(\sqrt[n]{y} - y^n))^2 \) is equal in absolute value to \( \text{res}_x(x^n - 1, f(x)) \). On the other hand, \( \text{res}_x(x^n - 1, f(x)) \) is also equal to \( \prod_{d \mid n} \mathbb{N}_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(f(\zeta_d^2)) \). Note, however, that each term in this product is in \( \mathbb{Q}(\zeta_d)^+ \) since \( f(x) \) is a reciprocal polynomial. So

\[
\text{res}_x(x^n - 1, f(x)) = \prod_{d \mid n} \mathbb{N}_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(f(\zeta_d^2))
\]

\[
= \left( \prod_{d \mid n} \mathbb{N}_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(f(\zeta_d^2)) \right)^2.
\]

Note that, after possibly multiplying by a root of unity, \( f(\zeta_d^2) = \left( \frac{t + 1}{2} \right)^2 (\zeta_d^2 + \zeta_d^{-2}) - t \). Let \( p, q \) be as in Lemma 6.4. The hypotheses that \( pq \mid t + 1 \) and \( t \equiv -1 \mod pq \) imply \( f(\zeta_d^2) \equiv 1 \mod pq \), so its norm is as well. Hence \( \prod_{d \mid n} \mathbb{N}_{\mathbb{Q}(\zeta_d)^+}/\mathbb{Q}(f(\zeta_d^2)) \) and \( i(\sqrt[n]{y} - y^n) \) are equal in absolute value and agree modulo \( pq \) by Lemma 6.4, so they are the same integer. The other equalities are direct calculations. □

We now want to show that we can change the sign of \( \Im(w^n) \) infinitely often as we vary \( n \) through powers of \( p \) and \( q \). To do this, we use a result of Furstenberg. Before stating it, we recall that a multiplicative semigroup of the integers is called lacunary if it consists of powers of a single integer and non-lacunary otherwise.

Theorem 6.6 (6 Theorem IV.1). If \( \Sigma \) is a non-lacunary semigroup of integers and \( \eta \) is irrational, then \( \Sigma \eta \) is dense modulo 1.

Lemma 6.7. Let \( f(x) = ax^2 + bx + a \in \mathbb{Z}[x] \) be a reciprocal polynomial of degree 2 with \( b/a < 2 \) and \( p \) and \( q \) distinct positive integers. Let \( w \) be a square root of a root of \( f \). Then for infinitely many pairs of positive integers \((u, v)\), we have \( \Im(w^n) < 0 \) where \( n = p^u q^v \). Moreover, each \( u \) and \( v \) may be taken to be even.

Proof. Since \( w \) is on the unit circle, we may write it as \( w = \exp(2\pi i \eta) \) so that \( w^n = \exp(2\pi i n \eta) \). If we let \( \Sigma = \{ p^u q^v \} \), then Furstenberg’s Theorem 6.6 implies that \( \Sigma \eta \) is dense modulo 1 so that for infinitely many \( n \in \Sigma \), \( w^n \) is in the lower-half plane. If we desire each \( u \) (resp. \( v \)) produced to be even, we may replace \( p \) (resp. \( q \)) with \( p^2 \) (resp. \( q^2 \)) in the definition of \( \Sigma \). □

The above lemma holds if the less than sign is replaced with a greater than sign.
Proof of Lemma 5.5. Let $n = p^u q^v$ for $p, q$ distinct odd primes and $u, v$ positive integers. If $p$ (resp. $q$) is equivalent to 3 mod 4, then suppose that $u$ (resp. $v$) is even. Note that \( \prod_{d \mid n} N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(f(\zeta_4^d)) = 2 \Im(y^n) \) is always 1 mod $pq$ when $n \equiv 1$ mod 4 by Lemma 6.4. Moreover, by Lemma 6.5, it is equal to $2 \left( \sqrt{\frac{n+1}{2}} \right)^n \Im(w^n)$, so when $\Im(w^n)$ is negative, the absolute value of $\prod_{d \mid n} N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(f(\zeta_4^d))$ must be equivalent to $-1$ mod $pq$.

Then one of the $N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(f(\zeta_4^d))$ must be not equivalent to 1 mod $pq$, so it must have a rational prime divisor to an odd power (note that all prime divisors must have multiplicative order either 1 or 2 modulo $d = p^u q^v$ by Lemma 6.2, so if all the powers were even, $\prod_{d \mid n} N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(f(\zeta_4^d))$ would be equivalent to 1 mod $p^u q^v$) that is not 1 mod $pq$, so by Lemma 5.4, it lies below a prime $l$ of $\mathbb{Q}(\zeta_4)$ that is inert in $\mathbb{Q}(\zeta_4)$. One may repeatedly apply Lemma 6.7 to change the sign of $\Im(w^n)$ back and forth to produce infinitely many $d$ with $N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(f(\zeta_4^d))$ not equivalent to 1 mod $pq$. \( \square \)

Remark 6.8. The infinitely many $d$ produced by Lemma 5.5 will provide $(d, 0)$ surgeries for which quaternion algebra has infinitely many distinct residue characteristics.

7. IRREDUCIBILITY

The goal of this section is to prove Lemma 5.2. The main ingredient will be the following proposition.

Proposition 7.1. Let $l$ be odd and $f_l(R, Z)$ the polynomial defining the canonical component of the character variety for the knot $T_l$. Then $f_l(R, 2 \cos(2\pi/n))$ is irreducible as an element of $\mathbb{Q}^{ab}[R]$ for all but finitely many $n$.

We will ultimately apply the following theorem of Dvornicich and Zannier.

Theorem 7.2 ([13] Corollary 1(a))). Let $k$ be a number field and $k^c$ the field obtained by adjoining all roots of unity to $k$. If $g \in k^c[R, Z]$ and $g(R, Z^m)$ is irreducible in $k^c[R, Z]$ for all positive integers $m \leq \deg_R g$, then $g(R, \zeta)$ is irreducible in $k^c[R]$ for all but finitely many roots of unity $\zeta$.

To apply this theorem, we actually consider the polynomials $g_t(R, Z) = Z^{\deg g} f_t(R, Z + Z^{-1})$, so that specializing $g_t$ at $Z = \zeta_n$ yields $\zeta_n^{\deg g} f_t(R, 2 \cos(2\pi/n))$. In particular, $g_t(R, \zeta_n)$ is irreducible over $\mathbb{Q}(\zeta_n)$ if and only if $f_t(R, 2 \cos(2\pi/n))$ is. We record the analogous formula for $g_t(R, Z) = Z^2 f_t(R, Z + Z^{-1})$ here.

Lemma 7.3. Let $t$ be an odd positive integer.

$$g_t(R, Z) = \begin{cases} Z^2 R^t - (Z^4 + Z^2 + 1) + \sum_{i=1}^{t-1} (a_i Z^2 - b_i (Z^4 + 2Z^2 + 1)) R^i & t \equiv 1 \text{ mod 4} \\ Z^2 R^t - Z^2 + \sum_{i=1}^{t-1} (a_i Z^2 - b_i (Z^4 + 2Z^2 + 1)) R^i & t \equiv 3 \text{ mod 4}, \end{cases}$$

where $a_i, b_i \in \mathbb{Z}$ and $a_{i-1} = b_{i-1} = 1$.

Our strategy will be first to show that $f_t(R, Z^m)$ is irreducible for all positive integers $m$ and then to show that the irreducibility of $f_t(R, Z^m)$ implies that of $g_t(R, Z^m)$. We begin by proving that—over $\mathbb{Q}$—changing $Z$ to $Z + Z^{-1}$ and clearing denominators does not affect irreducibility.

Lemma 7.4. Let $f_t(R, Z)$ be as above. Then for all positive integers $m$, $f_t(R, Z^m)$ is absolutely irreducible.

We need a version of Capelli’s theorem due to Kneser. This formulation appears in [14].

Theorem 7.5 ([14] Theorem 19)). Let $k$ be a field and $n$ an integer $\geq 2$. Let $a \in k$. The binomial $Z^n - a$ is reducible over $k$ if and only if either $a = b^p$ for some prime divisor $p$ of $n$ or $4 \mid n$ and $a = -4b^4$. 

Proof of Lemma 7.4. Let \( f_t(R, Z) \) be an element of \( C(R)[Z] \). Since polynomials in \( R \) are units in this ring, we may clear the denominators to obtain the monic polynomial

\[
F_t(R, Z^m) = \begin{cases} 
Z^{2m} - \frac{R^t + 1 + \sum_{i=1}^{l-1} a_i R^i}{1 + \sum_{i=1}^{l-1} b_i R^i} & \text{if } l \equiv 1 \mod 4, \\
Z^{2m} - \frac{R^t - 1 + \sum_{i=1}^{l-1} a_i R^i}{\sum_{i=1}^{l-1} b_i R^i} & \text{if } l \equiv 3 \mod 4,
\end{cases}
\]

which is irreducible if and only if \( f_t(R, Z) \) is. Let \( a \) denote the constant term and write \( a = \frac{\alpha(R)}{\beta(R)} \) where \( \alpha \) and \( \beta \) are coprime in \( C[R] \). Suppose that \( a = p^k \) for some prime divisor \( p \) of \( 2m \). Then, there are polynomials \( A_1, B_1 \in C[R] \) such that \( A_1^p = \alpha_1 \) and \( B_1^p = \beta_1 \). So then for some nonnegative integers \( l_1, l_2 \), we have \( \deg(\alpha_1) = p l_1 \) and \( \deg(\beta_1) = p l_2 \). However, \( \alpha_1 \) is of degree \( l - j \) and \( \beta_1 \) is of degree \( l - j - 1 \) where \( j \) is the degree of the original common factors between the numerator and denominator of \( a \). In particular, \( \deg(\alpha_1) \) and \( \deg(\beta_1) \) are coprime integers unless \( j = l - 1 \). In this case, however, \( \deg(\alpha_1) = 1 \), so it can't be a \( p \)th power. Finally to apply Theorem 7.3 we must check that \( a \neq -4b^4 \) when \( 4 \mid 2m \). However, the analogous degree considerations show that \( -a/4 \) cannot be a fourth power. Then we apply Gauss's lemma to conclude that \( f_t(R, Z^m) \) is irreducible as an element of \( C[R, Z] \).

Lemma 7.6. Let \( g_t(R, Z) \) be as above. Then for all positive integers \( m \), \( g(R, Z^m) \) is irreducible in \( \mathbb{Q}[R, Z] \).

Proof of Lemma 7.6. Fix a positive integer \( m \) and suppose that \( g_t(R, Z^m) = G_1(R, Z)G_2(R, Z) \) where \( G_i(R, Z) \in \mathbb{Q}[R, Z] \) of positive \( R \)-degree. Note that there cannot be a factorization involving a term of \( R \)-degree 0 since—in the case that \( l \equiv 1 \mod 4 \)—the \( R \)-leading coefficient, \( Z^{2m} \) is coprime with \( R \)-degree zero term, \( -Z^{4m} - Z^{2m} \). When \( l \equiv 3 \mod 4 \), the gcd of the leading and constant terms is \( Z^{2m} \), but reducing modulo \( Z \) produces \( -\sum_{i=1}^{l-1} b_i R^i \), which is nonzero by Lemma 7.3. Since the \( R \)-leading coefficient of \( g_t(R, Z^m) \) is \( Z^{2m} \), specializing \( Z = 1 \) produces a nontrivial factorization in \( \mathbb{Q}[R] \). However, \( g_t(R, 1^m) = f_t(R, 1^m + 1^{-m}) = f_t(R, 2) \), which is irreducible by [8].

Now we prove

Lemma 7.7. Let \( g_t \) be as above. Then \( g_t(R, Z^m) \) is absolutely irreducible for all positive integers \( m \).

We apply the following result of Bertone, Chèze, and Galligo.

Theorem 7.8 ([1 Proposition 3]). Let \( k \) be a field and \( g_t(R, Z) \in k[R, Z] \) be an irreducible polynomial. Let \( \{(i_1, j_1), \ldots, (i_t, j_t)\} \subset Z^2 \) be the vertex set of its Newton polygon. If \( \gcd(i_1, j_1, \ldots, i_t, j_t) = 1 \), then \( g_t(R, Z) \) is irreducible over \( k \).

Proof of Lemma 7.7. Note that the coefficients of \( R^{t-1}, Z^2 R^t \), and \( Z^4 R^{t-1} \) in \( g_t(R, Z) \) are all nonzero. Moreover, the coefficient of \( R^t \) and \( Z^4 R^t \) is zero, and there are no terms with \( Z \) to an odd power or a power greater than 4. All this implies that the top of the Newton polygon (with \( Z \) and \( R \) the horizontal and vertical directions respectively) looks like \((0, t - 1), (2, t), (4, t - 1)\). See Figure 1 for the Newton polygon of \( g_{13}(R, Z) \). These lattice points alone are sufficient to apply Theorem 7.8 together with the rational irreducibility furnished by Lemma 7.6 to conclude that \( g_t(R, Z) \) is absolutely irreducible. To apply theorem 7.2 we must further show that \( g_t(R, Z^m) \) is irreducible for all \( m \leq \deg_R(g_t) = t \). Indeed, \( g_t(R, Z^m) \) is irreducible over \( \mathbb{Q} \) for all positive integers \( m \). Increasing the power on \( Z \) has the effect of horizontally stretching the Newton polygon so that its top consists of the lattice points \((0, t - 1), (2m, t), (4m, t - 1)\). The coordinates of these points still have \( t \) and \( t - 1 \), which are coprime, so Theorem 7.8 still applies, so we find that \( g_t(R, Z^m) \) is absolutely irreducible for all positive integers \( m \). Then Theorem 7.2 applies so that \( g_t(R, \zeta_n) \) is irreducible in \( \mathbb{Q}(\zeta_n)[R] \), and hence \( f_t(R, 2 \cos(2\pi/n)) \) is as well.

Proof of Lemma 7.2. We may find a monic polynomial that \( r_d \) satisfies by specializing the character variety defining polynomial \( f_t(R, Z) \) to \( f_t(2 - r, 2 \cos(2\pi/d)) \). The resulting polynomial in \( \mathbb{Q}(\zeta^+_d)[r] \) is irreducible.
Let us first consider the theoretical results in the paper to prove ramification. We will not dwell on the exact nature of the computational complexities involved, but instead use some of which exceeds the record for the largest factored integer not of a special form by over 100 decimal digits. For example, the discriminant of a minimal polynomial for the invariants of this minimal polynomial, but computing reduction modulo primes (i.e. trying to apply Theorem 4.2) involves computing a maximal order in the field, which usually involves factoring a large discriminant. For example, the discriminant of a minimal polynomial for the (11,0) surgery on $T_{29}$ has 359 decimal digits, which exceeds the record for the largest factored integer not of a special form by over 100 decimal digits. We will not dwell on the exact nature of the computational complexities involved, but instead use some of the theoretical results in the paper to prove ramification.

Let us first mention that the canonical component is of the following form.

$$f_{29}(R, Z) = -R^{28}Z^2 + R^{29} + R^{27}Z^2 + R^{28} + 26R^{26}Z^2 - 28R^{27} - 25R^{25}Z^2 - 27R^{26} - 301R^{24}Z^2 + 351R^{25} + 277R^{23}Z^2 + 325R^{24} + 2046R^{22}Z^2 - 2600R^{23} - 1792R^{21}Z^2 - 2300R^{22} - 9066R^{20}Z^2 + 12650R^{21} + 7506R^{19}Z^2 + 10626R^{20} + 27492R^{18}Z^2 - 42504R^{19} - 21335R^{17}Z^2 - 33649R^{18} - 58277R^{16}Z^2 + 109947R^{17} + 41941R^{15}Z^2 + 74613R^{16} + 86662R^{14}Z^2 - 170544R^{15} - 57044R^{13}Z^2 - 116280R^{14} - 89402R^{12}Z^2 + 203490R^{13} + 52834R^{11}Z^2 + 125970R^{12} + 62292R^{10}Z^2 - 167960R^{11} - 32206R^9Z^2 - 92378R^{10} - 27966R^8Z^2 + 92378R^9 + 12174R^7Z^2 + 43758R^8 + 7476R^6Z^2 - 31824R^7 - 2576R^5Z^2 - 12376R^6 - 1036R^4Z^2 + 6188R^5 + 252R^3Z^2 + 1820R^4 + 56R^2Z^2 - 560R^3 - 7RZ^2 - 105R^2 - Z^2 + 15R + 1. $$

Let us first consider the (11,0) surgery on $T_{29}$, so our quaternion algebra is of the form $$(2 \cos(2\pi/11) - 2, -r_{11})^k_{11}.$$ Note that this is not actually the quaternion algebra associated to the (11,0) surgery, but instead the specialization of the Azumaya negative part (see Proposition 4.6 for details). However, all ramification shown in this example will actually be associated to the quaternion algebra for the Kleinian group. This.
A CONJECTURE OF CHINBURG-REID-STOVER FOR SURGERIES ON TWIST KNOTS

Table 1. Ramified residue characteristics for \((d,0)\) surgery on \(T_{29}\).

| \(d\) | primes | \(d\) | primes |
|-------|--------|-------|--------|
| 5     | \(\emptyset\) | 53    | \(\emptyset\) |
| 7     | 13     | 55    | \(\emptyset\) |
| 9     | 431    | 57    | 12539, \(56706539232099509\) |
| 11    | 43,131,1033 | 59  | \(122878684647\) |
| 13    | 1117, 1481 | 61  | 35711295669068681, \(41553136798440921281\) |
| 15    | 149, 179 | 63    | \(\emptyset\) |
| 17    | 67, 101, 509, 4657 | 65  | 4679, \(656305837760821827656999\) |
| 19    | 37     | 67    | \(401\) |
| 21    | \(\emptyset\) | 69    | \(\emptyset\) |
| 23    | 10938592571969 | 71  | \(283\) |
| 25    | 90636599549 | 73    | \(5503792674161\) |
| 27    | \(\emptyset\) | 75    | \(2699, 15299\) |
| 29    | 292319 | 77    | \(5196259971209\) |
| 31    | \(\emptyset\) | 79    | \(157, 80263\) |
| 33    | 659, 24800291 | 81  | \(314974363685075649\) |
| 35    | 25409 | 83    | \(74201, 4093091532209, 16729850810909\) |
| 37    | 73, 294149, 531516948137827 | 85  | \(7386583213044449, 6505561202472999\) |
| 39    | 35883041 | 87    | \(1601\) |
| 41    | 4271162617 | 89    | \(42223, 12282879708481\) |
| 43    | 3697, 107069 | 91    | \(569, 145349, 15382678739\) |
| 45    | \(\emptyset\) | 93    | \(929, 461977630174887794607639300779\) |
| 47    | \(\emptyset\) | 95    | \(569, 145349, 15382678739\) |
| 49    | 97     | 97    | \(79151, 149328007, 38993908476080668241718399966621\) |
| 51    | 1055801, 823976217011 | 99   | \(2970791, 36832658481, 9934540457447231\) |

Basically amounts to checking that the Azumaya positive part doesn’t have any of the same ramification. We also remark that \(k_{11}\) is a degree 145 extension of the \(\mathbb{Q}\). Without knowing something about the ring of integers (e.g. the conductor of \(\mathbb{Z}[\eta]\) in it), it is difficult to explicitly establish the splitting of primes in this extension. However, applying Lemma 5.1, one may deduce the existence of a ramified prime. In particular, we first need to prove that some prime \(L\) of \(k_{11}\) divides \(-\eta_{11}\) an odd number of times. This is a problem amenable to software. Indeed, \(N_{k_{11}/\mathbb{Q}}(-\eta_{11}) = 43 \cdot 131 \cdot 1033\). Since these all appear to the first power, there is no worry of a prime dividing \(-\eta_{11}\) multiple times. Now, we check the other criterion for these rational primes, namely that any prime of \(\mathbb{Q}(\zeta_{11})\) above them does not split in \(\mathbb{Q}(\zeta_{11})\). Since the tower of extensions \(\mathbb{Q}(\zeta_{d})/\mathbb{Q}(\zeta_{d})\) is Galois, each prime above a particular rational prime has the same splitting behavior. We may check that each of 43, 131, and 1033 satisfy the conditions of Lemma 5.1, so there is a prime in \(k_{11}\) above each of these rational primes such that the quaternion algebra for \(T_{29}(11,0)\) is ramified at that prime. This procedure can be implemented on a computer; after doing so, we find the residue characteristics listed in Table 1 of ramified primes for the \((d,0)\) surgery.

The detected surgery coefficients for this example are of the form \(3^{u}5^{v}\). To simplify the explanation for this example, let us define a function

\[
\omega(n) = \prod_{d|n} N_{\mathbb{Q}(\zeta_{d})/\mathbb{Q}}(\Delta_{T_{29}}(\zeta_{d}^{2})).
\]

The above discussion is meant to illustrate that results in the paper allow relatively easy computation of the residue characteristics of ramified primes for \((d,0)\) surgeries. Of course, Theorem 1.2 indicates that there are in fact infinitely many distinct such residue characteristics. We now show how one can unpack the methods of the proof to find a subsequence of surgery coefficients that provides the infinitely many distinct residue characteristics. We can summarize previous work in the paper by saying that we ultimately want to find \(d\) such that

\[
\left| N_{\mathbb{Q}(\zeta_{d})/\mathbb{Q}}(\Delta_{T_{29}}(\zeta_{d}^{2})) \right| \not\equiv 1 \text{ mod } 15.
\]
Lemma 6.4 implies that $\omega(n) \equiv 1 \mod 15$. The idea is then that if $n_0 \mid n_1$ and $\sigma(n_0)$ and $\sigma(n_1)$ have different signs, then $\left| \sigma(n_1)/\sigma(n_0) \right| \not\equiv 1 \mod pq$, so there is a divisor $d_1$ of $n_1$ that does not divide $n_0$ such that

$$\left| N_{\mathbb{Q}(\zeta_{d_1})}^{\mathbb{Q}}(\Delta_{T_{29}}(\zeta_{d_1})) \right| \not\equiv 1 \mod 15.$$

Then the problem is just reduced to showing that for any $n_0$, we can find a $n_1$ as above. For the knot $T_{29}$, this amounts to asking whether—given powers $u$ and $v$—one can find powers $u' > u$ and $v' > v$ such that $\omega(3^u5^v)$ has a different sign from that of $\omega(3^{u'}5^{v'})$. We prove that one can always do this by using Furstenberg’s theorem on nonlacunary semigroups (see Theorem 6.6). However, for the present example, we just compute a few cases to show how one might go about constructing infinitely many distinct residue characteristics.

For technical reasons, we actually need even powers of 3. So our first $n_0$ to try is $3^25 = 45$. $\omega(45)$ is negative, so $[\omega(45)]$ has a divisor that works. In fact, consulting the table above, there are three divisors $d$ of 45 so that the $(d,0)$ surgery has finite ramification, namely 9, 15, and 45. Call one of them $d_0$. The smallest $n_1$ such that $\omega(n_1) > 0$ is $n_1 = 3^25^5 = 28125$. So there must be some divisor $d_1$ of 28125 that doesn’t divide 45 (and hence $d_0$) such that the $(d_1,0)$ surgery has finite ramification, for example 75. Next, if we set $n_2 = 3^25^6$, then $\omega(n_2) < 0$, so we may find $d_2$ in the same way. The numbers involved quickly become intractably large even for software, but results in the paper guarantee that proceeding in this manner produces an infinite sequence of $(d_i,0)$ surgeries with finite ramification. Moreover, because of Lemma 6.2 we can’t find the same residue characteristic infinitely often, so this process will in fact produce infinitely many distinct rational primes such that for each one, there is an integer $d$ and a prime of the trace field of the $(d,0)$ surgery above that prime that ramifies the quaternion algebra associated to the $(d,0)$ surgery.

**References**

1. C. Bertone, G. Chèze, and A. Galligo. “Modular Las Vegas algorithms for polynomial absolute factorization”. J. Symbolic Comput. 45.12 (2010), pp. 1280–1295.
2. T. Chinburg, A. W. Reid, and M. Stover. “Azumaya Algebras and Canonical Components”. International Mathematics Research Notices (Sept. 2020).
3. J.-L. Colliot-Thélène, M. Ojanguren, and R. Parimala. “Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes”. Algebra, arithmetic and geometry, Part I, II (Mumbai, 2000). Vol. 16. Tata Inst. Fund. Res. Stud. Math. Tata Inst. Fund. Res., Bombay, 2002, pp. 185–217.
4. M. Culler and P. B. Shalen. “Varieties of group representations and splittings of 3-manifolds”. Ann. of Math. (2) 117.1 (1983), pp. 109–146.
5. R. Dvornicich and U. Zannier. “Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps)”. Duke Math. J. 139.3 (2007), pp. 527–554.
6. H. Furstenberg, “Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation”. Math. Systems Theory 1 (1967), pp. 1–49.
7. D. Harari. “Méthode des fibrations et obstruction de Manin”. Duke Math. J. 75.1 (1994), pp. 221–260.
8. J. Hoste and P. D. Shanahan. “Trace fields of twist knots”. J. Knot Theory Ramifications 10.4 (2001), pp. 625–639.
9. M. L. Macasieb, K. L. Petersen, and R. M. van Luijk. “On character varieties of two-bridge knot groups”. Proc. Lond. Math. Soc. (3) 103.3 (2011), pp. 473–507.
10. C. Maclachlan and A. W. Reid. The arithmetic of hyperbolic 3-manifolds. Vol. 219. Graduate Texts in Mathematics. Springer-Verlag, New York, 2003.
11. J. Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999.
12. B. Poonen. *Rational points on varieties*. Vol. 186. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2017.
13. N. Rouse. “Arithmetic of the canonical component of the knot $7_4$” (June 2020). arXiv: 2006.15251.
14. A. Schinzel. *Polynomials with special regard to reducibility*. Vol. 77. Encyclopedia of Mathematics and its Applications. With an appendix by Umberto Zannier. Cambridge University Press, Cambridge, 2000, pp. x+558.
REFERENCES

[15] A. Skorobogatov. “Arithmetic geometry: rational points”. Online notes (2013).

[16] L. C. Washington. Introduction to cyclotomic fields. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1982, pp. xi+389.

Department of Mathematics,
Rice University,
Houston, TX 77005, USA

Email address: nicholas.rouse@rice.edu