

HECKE INVARIANTS OF KNOT GROUPS

by ROBERT RILEY

(Received 9 September, 1972)

For each characteristic p , let F_p be the prime field and let Ω_p be a fixed universal field which is algebraically closed and of infinite transcendence degree over F_p . When $p = 0$ we take $\Omega_p = \mathbb{C}$. Let F be a subfield of Ω_p and let R be an integral domain whose quotient field is F . We abbreviate $\text{SL}(2, R)$, $\text{PGL}(2, R)$, $\text{PSL}(2, R)$ to $\text{SL}(R)$, $\text{PGL}(R)$, $\text{PSL}(R)$ respectively, and we consider $\text{PSL}(R)$ as a group of projective transformations of the projective line $\mathcal{P}(\Omega_p)$ and of the "subline" $\mathcal{P}(F) \subset \mathcal{P}(\Omega_p)$. The elements of $\text{PSL}(R)$ are classified by the number of fixed points they have on $\mathcal{P}(F)$. If $x \in \text{PSL}(R)$ has one such fixed point P , then P is the unique fixed point of x on $\mathcal{P}(\Omega_p)$ and x is called *parabolic*. All other x (except the identity E) have two distinct fixed points on $\mathcal{P}(\Omega_p)$ and x is called *hyperbolic* if these are on $\mathcal{P}(F)$, and *elliptic* otherwise. We put symbols for operators on the right.

Let K be a knot type with group πK , and consider homomorphisms $\theta: \pi K \rightarrow \text{PSL}(\Omega_p)$. We shall call such a θ a *parabolic representation* if $\pi K\theta$ is nonabelian and $x\theta$ is parabolic for every meridian $x \in \pi K$. The abbreviation of "parabolic representation" will henceforth be "p-rep", instead of "rep" as used in [6], [7]. Note that, because πK is finitely generated, $\pi K\theta \subset \text{PSL}(R)$ for some integral domain R which is finitely generated over F_p . We call two p-reps $\theta_1, \theta_2: \pi K \rightarrow \text{PSL}(\Omega_p)$ *simply equivalent* when there exists $Y \in \text{PGL}(\Omega_p)$ such that $x\theta_2 = Y^{-1}x\theta_1Y$ for all $x \in \pi K$. Suppose that an over presentation of πK has been selected. Then, according to [7, §2], there is an algebraic set M_0 whose points are in one-one correspondence with the simple equivalence classes of p-reps in $\text{PSL}(\mathbb{C})$, and M_0 is defined by polynomial equations with rational integral coefficients. (There is an error in [7, §2], but it has no influence on the present paper.) If $\theta: \pi K \rightarrow \text{PSL}(\mathbb{C})$ is a p-rep we write $Z = Z(\theta)$ for the corresponding point of M_0 . Suppose that $Z(\theta)$ is a generic point of a subvariety N of M_0 which is also defined over \mathbb{Z} . Then, for each positive prime p we consider N_p , the reduction of N modulo p , which is an algebraic set in characteristic p defined by reducing the polynomial equations defining N modulo p . We shall say that the p-rep $\bar{\theta}: \pi K \rightarrow \text{PSL}(\Omega_p)$ is a *reduction of θ modulo p* if $\bar{\theta}$ corresponds to a generic point \bar{Z} of a component of N_p . The number of equivalence classes of reductions of θ modulo p is the number, l say, of components of N_p .

Suppose that $\bar{\theta}$ is a reduction of θ modulo p and $\pi K\bar{\theta}$ is a transitive group of projective transformations of the projective line $\mathcal{P}(F_q)$, where q is a power of p and F_q is the field with q elements. (According to Dickson's Theorem C of [7, §6], this implies that $\pi K\bar{\theta} = L_q := \text{PSL}(F_q)$ except possibly when $q = 9$ or $q = 2^r$ with $r > 1$.) Then $\bar{\theta}$ is a permutation representation of πK of degree $q + 1$, and there is a standard method of associating unbranched and branched $q + 1$ sheeted covering spaces of $S^3 - k$ with $\bar{\theta}$ (cf. [1, §8]). As in [6], we write $\mathcal{U}_{q+1} = \mathcal{U}_{q+1}(K, \bar{\theta})$ for the unbranched covering space, and \mathcal{M}_{q+1} for the completion of \mathcal{U}_{q+1} to a branched covering space. We call the groups $H_1\mathcal{U}_{q+1} := H_1(\mathcal{U}_{q+1}, \mathbb{Z})$, $H_1\mathcal{M}_{q+1} := H_1(\mathcal{M}_{q+1}, \mathbb{Z})$ respectively *unbranched* and *branched homology invariants of the pair (K, θ) at p* . There are l pairs of such invariants, and the collection of all the unbranched or branched homology invariants of (K, θ)

B

at p may be called respectively an *unbranched* or a *branched parabolic invariant of K at p* . This is in accord with a suggestion of Fox in the introduction to [2]. The importance of the parabolic invariants is due to the ease of computing them and their effectiveness in distinguishing isomorphism classes of knot groups.

The image of a p -rep θ in characteristic zero is only rarely a Fuchsian group, because $\pi K\theta$ usually does not lie in $\text{PSL}(\mathbb{R})$, and when $\pi K\theta \subset \text{PSL}(\mathbb{R})$ we generally find that $\pi K\theta$ is indiscrete. In fact, the only Fuchsian groups G known to be the image of a parabolic representation are isomorphic to the free product $C_r * C_s$ of cyclic groups of relatively prime orders $r, s > 1$. The modular group $\text{PSL}(\mathbb{Z})$ is the simplest group of this sort and $\text{PSL}(\mathbb{Z}) \approx C_2 * C_3$. For each odd integer $s > 1$ there is a Hecke group $\Pi_s \approx C_2 * C_s$ (whose definition is recalled in §1) and the simplest Hecke group is $\Pi_3 = \text{PSL}(\mathbb{Z})$. The Hecke groups may be regarded as the immediate generalization of the modular group, and Π_s is of the form $\pi K\theta$ for infinitely many knot types K , including 2-bridge knot types. The collection of all (unbranched or branched) homology invariants of K at a prime p corresponding to p -reps $\theta: \pi K \rightarrow \Pi_s$ may be called the (*unbranched* or *branched*) *Hecke invariant of (K, s) at p* . In this paper we shall apply the highly developed theory of Fuchsian groups to establish properties of Hecke invariants which are apparently not shared by more general parabolic invariants. Our main result is Theorem 3 of §3, which gives a lower bound for the Betti numbers of the unbranched Hecke invariants of (K, s) at a prime p not dividing s . The results of this paper are a necessary preliminary to any assault on Conjecture B of [6], and our main purpose in writing this paper is to raise interest in that conjecture in the hope that someone will try to prove it.

This paper is arranged as follows. In §1 we define the Hecke groups in the precise form in which we need them, and establish their most important properties. This material is presumably well known, but, because this paper is intended for knotters rather than for experts on Fuchsian groups, we felt it wise to be explicit. In §2 we discuss certain subgroups Γ of Π_s . The material here is a generalization of classical theorems about the modular group (see page 304 of Fricke's textbook [3]) and it may also be well known, but I cannot find a reference for it. In §3 we prove the advertised main theorem about $H_1 \mathcal{U}_{q+1}$. Finally, in §4 we restate Conjecture B in an improved form and discuss the Hecke invariants at primes $p > 3$ for p -reps on $\text{PSL}(\mathbb{Z})$ when K is one of the three torus knots $3_1, 9_1, 8_{19}$.

This paper could not have been written without the assistance of David Singerman, who brought his paper [8] to my attention and explained how to use the results therein to prove our Theorem 2 of §2 in the case where Π_s is $\text{PSL}(\mathbb{Z})$. A part of the proof of Theorem 3 was developed in a discussion with Gareth Jones, who is a ready source of wisdom about group theory.

1. Hecke groups. Let $s > 1$ be a fixed odd integer. We define the Hecke group Π_s in terms of the Morgan-Voyce polynomials $f_j = f_j(y)$, $g_j = g_j(y)$ following [7, §5] as follows. The Morgan-Voyce polynomials are defined inductively by

$$\left. \begin{aligned} f_0 &= 1, & g_0 &= 1, \\ f_{j+1} &= f_j + yg_j, & g_{j+1} &= f_{j+1} + g_j. \end{aligned} \right\} \tag{1.1}$$

Let $s_1 > 1$ be a divisor of s and let $n_1 = \frac{1}{2}(s_1 - 1)$. In particular, let $n = \frac{1}{2}(s - 1)$. Then there is a factor $\chi_{n_1}(y)$ of $f_n(y)$ and

$$f_n(y) = \prod_{s_1 | s} \chi_{n_1}(y).$$

The degree of $\chi_{n_1}(y)$ is $\frac{1}{2}\phi(s_1)$, where ϕ is the Euler function. We are mainly interested in $\chi_n(-y)$ whose roots are

$$\xi_j = 2 + 2 \cos 2\pi j/s = (2 \cos \pi j/s)^2, \tag{1.2}$$

where

$$1 \leq j < s, \quad (j, s) = 1. \tag{1.3}$$

Note that $\xi_j = \xi_{s-j}$. The largest root of $\chi_n(-y) = 0$ (which is also the largest root of $f_n(-y) = 0$) is $\xi = \xi_1 = \xi_{s-1}$. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = B(\xi) = \begin{pmatrix} 1 & 0 \\ -\xi & 1 \end{pmatrix} \quad \text{in } \text{PSL}(\mathbb{R}). \tag{1.4}$$

Then we define the Hecke group Π_s by

$$\Pi_s = \langle A, B \rangle. \tag{1.5}$$

THEOREM 1. *The Hecke group Π_s is a Fuchsian group with a presentation*

$$\Pi_s = | C, D : C^2 = D^s = E | \tag{1.6}$$

which is related to (1.5) by

$$C = (AB)^s A, \quad D = AB, \quad A = D^{-s} C, \quad B = A^{-1} D. \tag{1.7}$$

Proof. The only part of the proposition which is not contained in Theorem 6 of [7] is the assertion that Π_s is Fuchsian, i.e., that Π_s acts discontinuously on the upper half-plane. To verify this, we need the explicit formulae

$$D = \begin{pmatrix} 1-\xi & 1 \\ -\xi & 1 \end{pmatrix}, \tag{1.8}$$

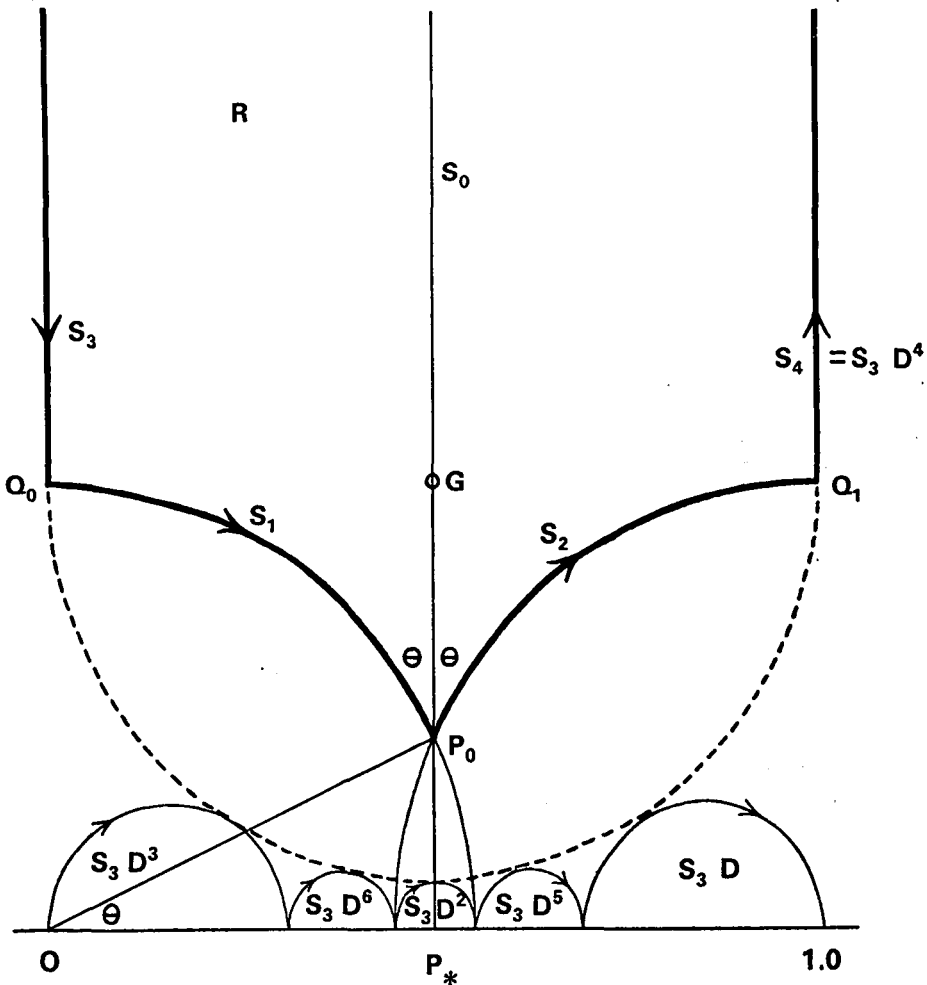
$$C = \begin{pmatrix} 0 & g_{n-1}(-\xi) \\ -\xi g_{n-1}(-\xi) & 0 \end{pmatrix}. \tag{1.9}$$

The elements $C, D \in \text{PSL}(\mathbb{R})$ are elliptic linear fractional transformations of the upper half-plane $\mathcal{U} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. Hence each transformation has a unique fixed point in \mathcal{U} , say $P_0 D = P_0$ and $Q_0 C = Q_0$. We calculate readily that

$$P_0 = \frac{1}{2} + \frac{1}{2}\sqrt{(1-4/\xi)}, \quad Q_0 = \frac{1}{\sqrt{(-\xi)}}. \tag{1.10}$$

Another calculation shows that P_0 and Q_0 have the same euclidean distance from the point $O = (0, 0)$ on the euclidean boundary V of \mathcal{U} . In terms of the standard non-euclidean (NE) metric on \mathcal{U} in which the geodesics are euclidean semicircles with centres on V or euclidean straight lines perpendicular to V , let s_1 be the NE line segment $P_0 Q_0$. Let s_0 be the NE segment $P_0 \infty = \{\frac{1}{2} + it \mid t \geq \frac{1}{2}\sqrt{(4/\xi - 1)}\}$, and let $s_2 = P_0 Q_1$ be the reflection of s_1 in s_0 . Let $s_3 = \{it \mid t \geq 1/\sqrt{\xi}\}$ be the NE segment $Q_0 \infty$, and let s_4 be the reflection of s_3 in s_0 . Then $s_4 = \{1 + it \mid t \geq 1/\sqrt{\xi}\}$ has finite endpoint $Q_1, Q_1 = Q_0 A$ and $s_4 = s_3 A$. If we close the

segments s_3, s_4 by the point ∞ , the path $s_1 s_2 s_4 s_3$ is the boundary of an open NE polygonal region R of \mathcal{U} . It is easy to see that s_1 meets s_3 in a right angle at Q_0 , and likewise s_2 meets s_4 in a right angle at Q_1 . The angle at P_0 between s_1 and s_2 is bisected by s_0 ; let $\theta = \text{angle } s_1 s_0 = \text{angle } s_0 s_2$. Let $P_* = (\frac{1}{2}, 0) \in V$ and consider the euclidean right triangle $P_0 O P_*$. The angle $P_0 O P_* = \theta$ and $\cos \theta = O P_* / O P_0 = \frac{1}{2} / (2 \cos \pi / s)^{-1} = \cos \pi / s$. But $0 < \theta < \pi / 2$; so $\theta = \pi / s$. The transformation D is a NE rotation of exact period s about the fixed point P_0 ; so the angle of rotation necessarily has the form $2\pi j / s$ for some integer j such that $(j, s) = 1$.



The situation when $s = 7, \xi = 3.2470$.

G is the centre of the dashed circle. The transforms of s_3 by powers of D are indicated by $s_3, s_3 D, \dots, s_3 D^6$.

(The value of j is irrelevant but it turns out that $j = -2$.) Consequently, for some exponent r , $s_2 = s_1 D^r$. Finally note that $\langle A, D \rangle = \Pi_s$, from (1.7).

We now appeal to the theorem of Poincaré stated in Note 6, page 64 of Chapter 1 of [4] and proved in [5]. The conclusion is that Π_s acts discontinuously on \mathcal{U} and that R is a fundamental open region for the action. Poincaré’s theorem also verifies the completeness of the relations in (1.6), and this method should be taken as the standard proof of Theorem 1. ■

The final reference, [9], appeared several months after the present paper was submitted for publication. It is closely related to the contents of this section, and it contains a reference to E. Hecke’s own work on Hecke groups.

2. Subgroups of Hecke groups. This section is devoted to the application of the material summarized in the first two sections of Singerman’s paper [8] to the determination of the genus of a certain subgroup Γ of a Hecke group Π_s . It is convenient to define the *class* of the element g of a group G to be the set of all conjugates of powers g^v of g such that $g^v \neq E$ if $g \neq E$. By $\mathfrak{U}G$ we mean $G/[G, G]$.

A Fuchsian group G which has no hyperbolic boundary elements has a canonical presentation as follows:

$$\text{Generators: } \left\{ \begin{array}{l} a_1, b_1, \dots, a_g, b_g \text{ hyperbolic, } g = \text{genus}(G), \\ u_1, u_2, \dots, u_h \text{ elliptic,} \\ v_1, v_2, \dots, v_t \text{ parabolic.} \end{array} \right\} \quad (2.1a)$$

$$\text{Relations: } u_1^{m_1} = u_2^{m_2} = \dots = u_h^{m_h} = \prod_{i=1}^g [a_i, b_i] \cdot \prod_{j=1}^h u_j \cdot \prod_{k=1}^t v_k = E. \quad (2.1b)$$

Every nontrivial element of G is in the class of exactly one of the generators (2.1a). When G is presented by (2.1), define $M(G)$ by

$$M(G) = 2g - 2 + t + \sum_{i=1}^h \left\{ 1 - \frac{1}{m_i} \right\}. \quad (2.2)$$

The Riemann-Hurwitz formula asserts that, if $G_1 \subset G$ is a subgroup of finite index $N = [G : G_1]$, then

$$N = M(G_1)/M(G). \quad (2.3)$$

The presentation (1.6) for Π_s is not quite in the form (2.1), but this is no problem because it is readily apparent from (1.6) that the genus of Π_s is zero, that the number of parabolic classes $t = 1$ (certainly $t \geq 1$, and $t > 1$ would give $\mathfrak{U}\Pi_s$ a torsion-free direct summand), that $h = 2$ and $m_1 = 2, m_2 = s$, say. Consequently

$$M(\Pi_s) = \frac{s-2}{2s}. \quad (2.4)$$

Let p be an odd prime which does not divide s . Then the factorization of $\chi_n(y)$ modulo p has the form

$$\chi_n(y) \equiv \chi^{(1)}(y) \dots \chi^{(l)}(y) \pmod{p}, \quad (2.5)$$

where

$$\deg \chi^{(1)} = \deg \chi^{(2)} = \dots = \deg \chi^{(l)} = \frac{\phi(n)}{2l} = r, \quad \text{say.} \tag{2.6}$$

For each j with $1 \leq j \leq l$, let $\xi_j \in \Omega_p$ be a root of $\chi^{(j)}$. Then there is a surjective homomorphism $\phi_p^j: \Pi_s \rightarrow L_{p^r}$ defined by

$$A\phi_p^j = \begin{pmatrix} & 1 \\ 0 & \end{pmatrix}, \quad B\phi_p^j = \begin{pmatrix} 1 & 0 \\ -\xi_j & 1 \end{pmatrix} \tag{2.7}$$

in $\text{PSL}(\Omega_p)$. Then ϕ_p^j is called a *reduction of Π_s modulo p* . Up to equivalence there are exactly l such reductions, where two homomorphisms $\theta_1, \theta_2: G_1 \rightarrow G_2$ are *equivalent* if G_2 has an automorphism ψ such that $\theta_2 = \theta_1 \psi$. Let $\Pi_{s,f}(p)$ denote the subgroup of Π_s consisting of all γ such that the projective transformation $\gamma\phi_p^j$ acting on the projective line $\mathcal{P}(F_{p^r})$ leaves ∞ fixed. To simplify the notation we fix one reduction ϕ_p^j and write

$$\phi = \phi_p^j, \quad \Gamma = \Pi_{s,j}(p), \quad \xi = \xi_j. \tag{2.8}$$

We also set $q = p^r$, where r is defined in (2.6).

The main result of this section is a presentation for the abelianized group $\mathfrak{A}\Gamma = \Gamma/[\Gamma, \Gamma]$. We will get this by computing the various quantities h, m_1, \dots, m_n, t, g of a canonical presentation (2.1) for Γ . The parabolic class number t is, according to the summary in [8], the number of cycles in $A\phi$, considered as a permutation of the points of $\mathcal{P}(F_q)$. But $A\phi$ has one fixed point and order p , whence $A\phi$ must be the product of q/p p -cycles and one 1-cycle. This implies that

$$t = p^{r-1} + 1. \tag{2.9}$$

We next consider h and the m_i . The u_i of (2.1) for Γ are induced (in Singerman’s language) by the elliptic elements C, D of (1.7). The involution C induces ν elliptic elements u of Γ , where ν is the number of cycles of the permutation $C\phi$ of length less than 2. Such cycles must be fixed points; so either C induces no elliptic elements, or else C induces two elliptic elements and these are involutions. From (1.9) and (1.10) we see that the number of classes of involutions induced by C is the number of solutions of

$$z^2 + \bar{a}^2 = 0, \quad \bar{a} = g_{n-1}(-\xi), \tag{2.10}$$

in F_q . Clearly (2.10) has solutions in F_q if and only if -1 is a square in F_q , or, equivalently, if and only if $q \equiv +1 \pmod{4}$.

Now consider the elliptic elements u of Γ induced by D . Since D has order s , $D\phi$ has order s_1 , where $s_1 | s$. To see that $s_1 = s$, consider the multiplier κ of D and the multiplier $\bar{\kappa}$ of $D\phi$. Then κ is a root of the cyclotomic polynomial $\Phi_s(x)$, and we recall that

$$x^s - 1 = \prod_{m | s} \Phi_m(x).$$

It is well known that $x^s - 1$ has no multiple factors modulo p , so that, in $\Omega_p[x]$,

$$x^s - 1 = \prod_{m | s} \bar{\Phi}_m(x),$$

where $\bar{\Phi}_m$ is the reduction of $\Phi_m(\text{mod } p)$. Also, $\bar{\kappa}$ is a root of $\bar{\Phi}_s(x)$. Hence a comparison of degrees shows that, if $\bar{\kappa}^v = 1$, then $s \mid v$, which implies that $s_1 = s$. The permutation $D\phi$ may contain only s -cycles and 1-cycles, and furthermore there are either two or zero 1-cycles. Hence $q + 1 \equiv$ the number of fixed points of $D\phi \pmod{s}$, so that, if $q \equiv +1 \pmod{s}$, then D induces two elliptic elements of order s , and, if $q \equiv -1 \pmod{s}$, then D induces no elliptic elements of Γ .

We finally determine the genus of Γ indirectly using (2.3) and the information about $M(\Gamma)$ deduced from the above results. The index N of (2.3) $= q + 1 =$ the number of points of $\mathcal{P}(F_q)$. Hence

$$q + 1 = \frac{2g - 2 + 1 + p^{r-1} + \Sigma}{[(s-2)/2s]}, \quad \Sigma := \sum_{i=1}^h \left\{ 1 - \frac{1}{m_i} \right\}. \tag{2.11}$$

The calculation splits into four cases and the results are summarized in the following theorem.

THEOREM 2. *The abelianized group $\mathfrak{A}\Gamma$ depends only on s and p , and not on the specific reduction ϕ_p^1 of Π_s . Write $\mathfrak{A}\Gamma = F \oplus T$ where T is the torsion subgroup and F is a free abelian summand of rank $f_s(p)$. Then the genus $g = g_s(p)$ of Γ , $f = f_s(p)$ and the torsion numbers of T are determined by the value of $q \pmod{4}$ and $q \pmod{s}$, by*

$$f_s(p) = 2g_s(p) + p^{r-1} \tag{2.12}$$

and the following table.

- (I) $q \equiv +1 \pmod{4}$ and $q \equiv +1 \pmod{s}$.
 $g = (s-2) \frac{p^r - 1}{4s} - \frac{p^{r-1} + 1}{2}$; torsion numbers $2, 2, s, s$.
- (II) $q \equiv +1 \pmod{4}$ and $q \equiv -1 \pmod{s}$.
 $g = \frac{p^r - 2p^{r-1} + 1}{4} - \frac{p^r + 1}{2s}$; torsion numbers $2, 2$.
- (III) $q \equiv -1 \pmod{4}$ and $q \equiv +1 \pmod{s}$.
 $g = \frac{p^r - 2p^{r-1} - 1}{4} - \frac{p^r - 1}{2s}$; torsion numbers s, s .
- (IV) $q \equiv -1 \pmod{4}$ and $q \equiv -1 \pmod{s}$.
 $g = (s-2) \frac{p^r + 1}{4s} - \frac{p^{r-1} - 1}{2}$; no torsion.

3. The homology of the unbranched covering spaces. Let πK be a knot group which has a surjective parabolic representation $\theta: \pi K \rightarrow \Pi_s$ for some odd $s > 1$.

LEMMA. *There is a presentation*

$$\pi K = \langle x_1, \dots, x_v; r_2, \dots, r_v \rangle \tag{3.1}$$

in which the generators x_i are conjugate meridians of πK and such that θ can be normalized with respect to (3.1) so that

$$x_1\theta = A, \quad x_2\theta = B \tag{3.2}$$

where A, B are defined in (1.4).

Proof. We start with an arbitrary over-presentation

$$\pi K = \langle \tilde{x}_1, \dots, \tilde{x}_{v-1}; \tilde{r}_2, \dots, \tilde{r}_{v-1} \rangle. \tag{3.3}$$

The representation θ can be normalized with respect to (3.3) so that $\tilde{x}_1\theta = A$. Since B is conjugate to A in Π_s , there is a $W \in \Pi_s$ such that $B = W^{-1}AW$. Because θ is surjective there is a $w \in \pi K$ such that $W = w\theta$. Let $x = w^{-1}\tilde{x}_1 w$; then x is a meridian of πK which is conjugate to x_1 and satisfies $x\theta = B$. It is now obvious that, by adjoining the new generator x and the relation $x = w^{-1}\tilde{x}_1 w$ to (3.3) (with w written out as a word in $\tilde{x}_1, \dots, \tilde{x}_{v-1}$), and suitably re-naming the generators and relations, we produce the required presentation. ■

Let p be an odd prime not dividing s and let $\phi = \phi_p^j$ be one of the l reductions of Π_s modulo p . Then $\phi: \Pi_s \rightarrow L_q$, where $q = p^r$ and r is determined by (2.6). Again write $\Gamma = \Pi_{s,j}^\infty(p)$ and let $M = \theta^{-1}(\Gamma)$ be the pre-image of Γ in πK . Then the unbranched $(q+1)$ -sheeted covering space \mathcal{U}_{q+1} of the introduction has fundamental group $\pi_1\mathcal{U}_{q+1} \approx M$. Consequently $H_1\mathcal{U}_{q+1} \approx \mathfrak{A}M$ and we are ready to apply Theorem 2.

THEOREM 3. *The Betti number $b = b(K, \theta, j, p)$ of $H_1\mathcal{U}_{q+1}$ satisfies*

$$b \geq 1 + f_s(p), \tag{3.4}$$

where $f_s(p)$ is defined in Theorem 2.

Proof. Write $H = \ker \theta$. The system of groups and homomorphisms under consideration is summarized by the commutative diagram (3.5) in which the rows are exact, the vertical arrows represent canonical inclusion homomorphisms, and θ', θ'' denote restrictions of θ to the appropriate subgroups.

$$\begin{array}{ccccccc} \langle E \rangle & \rightarrow & H & \rightarrow & \pi K & \xrightarrow{\theta} & \Pi_s & \rightarrow & \langle E \rangle \\ & & & & \uparrow & & \uparrow & & \\ & & & & M & \xrightarrow{\theta'} & \Gamma & \rightarrow & \langle E \rangle \\ & & & & \uparrow & & \uparrow & & \\ & & & & [M, M] & \xrightarrow{\theta''} & [\Gamma, \Gamma] & \rightarrow & \langle E \rangle \end{array} \tag{3.5}$$

It is easy to see that θ induces a surjective homomorphism $\theta_*: \mathfrak{A}M \rightarrow \mathfrak{A}\Gamma$. This shows that $b \geq f$. To show that equality does not hold it is sufficient to exhibit $h \in H$ such that no nonzero power of h lies in $[M, M]$, because h would then generate a free summand of $\ker \theta_*$. Suppose that θ has been normalized as in the lemma. Let $w_1 = (x_1 x_2)^n x_1 \in \pi K$, where $n = \frac{1}{2}(s-1)$ as usual. Then $w_1\theta$ is the element C of (1.7); so $h_1 = w_1^2$ must lie in $\ker \theta = H$. But h_1 represents $s+1 \neq 0$ in $\mathfrak{A}\pi K \approx \mathbb{Z}$, whence $h_1^m \notin [\pi K, \pi K]$ for any nonzero m .

4. Conjecture B. In this section we consider the relation between the two homology invariants $H_1\mathcal{U}_{p+1}, H_1\mathcal{M}_{p+1}$ at a prime $p > 3$ of a p -rep $\theta: \pi K \rightarrow \Pi_3 = \text{PSL}(\mathbb{Z})$. In this case

the polynomial $\chi_n(y)$ is $1 + y$ and the numbers r, l of (2.6) are both 1. The formulae of Theorem 2 simplify to $f_3(p) = 1 + 2g(p)$, where

$$g(p) = \frac{p + j(p)}{12}, \tag{4.1}$$

in which $j(p)$ is determined by the value of $p \pmod{12}$ as follows.

$$\left. \begin{aligned} p &\equiv 1 & 5 & 7 & 11 & \pmod{12} \\ j(p) &= -13 & -5 & -7 & +1 \\ r(p) &= 1 & 3 & 2 & 6 \end{aligned} \right\} \tag{4.2}$$

The lower bound $1 + f$ of Theorem 3 becomes $2 + 2g(p)$. We shall also need

$$d(p) = \frac{p + 1}{r(p)}, \tag{4.3}$$

where $r(p)$ is defined by the bottom line of (4.2). As further notation, let bX denote the Betti number of $H_1 X := H_1(X; \mathbb{Z})$ and let $T_1 X$ denote the torsion subgroup of $H_1 X$. Then the desired relation is the

SHARPENED CONJECTURE B. *Given $\theta: \pi K \rightarrow \text{PSL}(\mathbb{Z})$ and a prime $p > 3$, the relation between the homology invariants $H_1 \mathcal{U}_{p+1}, H_1 \mathcal{M}_{p+1}$ is as follows.*

$$b\mathcal{U}_{p+1} = 2 + b\mathcal{M}_{p+1}. \tag{4.4}$$

According to Theorem 3 the assertion 4.4 implies that

$$b\mathcal{M}_{p+1} \geq 2g(p). \tag{4.5}$$

Write m_p for the order of $T_1 \mathcal{M}_{p+1}$ and u_p for the order of $T_1 \mathcal{U}_{p+1}$. Then

$$b\mathcal{M}_{p+1} = 2g(p) \Rightarrow m_p = d(p)u_p; \tag{4.6}$$

$$b\mathcal{M}_{p+1} > 2g(p) \Rightarrow m_p/u_p \text{ is an integer which divides } d(p). \tag{4.7}$$

No general assertion is made about the comparison of the torsion coefficients of $T_1 \mathcal{U}_{p+1}, T_1 \mathcal{M}_{p+1}$.

The final topic is the question whether the homology invariants for a p -rep $\theta: \pi K \rightarrow \text{PSL}(\mathbb{Z})$ can be computed as functions of p by simple formulae. It seems that they can be, at least when K is a torus knot. A general answer to this question would be both important and interesting, and might be a step towards a substitute for the Alexander matrix which solves the corresponding problem for cyclic representations. To encourage further investigations along these lines we present conjectured formulae for the cases $K = 3_1, 9_1$ and 8_{19} . Our tables suggest that formulae probably exist for non-torus knots such as $8_5, 8_{18}$ which are similar to, but more complicated than, those given below. Unfortunately, much more data would be required to guess them, and the machine time required to calculate the invariants at p is a rapidly increasing function of p .

We use the notation of [6, §6] to describe groups $T_1 X$; i.e., if $T_1 X$ is the direct sum of

cyclic groups of orders a_1, \dots, a_m , we write $T_1 X = a_1, \dots, a_m$. These will always be ordered so that $a_j | a_{j+1}$ for $j < m$. When the torsion number a is repeated e times we abbreviate a, \dots, a to $a^{(e)}$.

The knot groups πK for $K = 3_1, 9_1, 8_{19}$, each have a unique p -rep on $\text{PSL}(\mathbb{Z})$ listed in [6, §3], using the table of group presentations in the microfiche section of the issue of Mathematics of Computation containing [6]. It is conjectured that the relations $b\mathcal{M}_{p+1} = 2g(p)$, $b\mathcal{U}_{p+1} = 2 + b\mathcal{M}_{p+1}$ hold for all primes $p > 3$ for these three knots. The torsion invariants are:

$$\begin{aligned}
 K = 3_1 & \left\{ \begin{array}{l} T_1 \mathcal{U}_{p+1} = \frac{6}{r(p)}. \\ T_1 \mathcal{M}_{p+1} = \frac{6d(p)}{r(p)}. \end{array} \right. \\
 K = 9_1 & \left\{ \begin{array}{l} T_1 \mathcal{U}_{p+1} = 3^{(e_p)}, \frac{18}{r(p)} \\ T_1 \mathcal{M}_{p+1} = 3^{(e_p)}, \frac{18d(p)}{r(p)} \end{array} \right\} \quad \text{where } e_p = \begin{cases} \frac{p-1}{3} & (p \equiv 1 \pmod{3}), \\ \frac{p-5}{3} & (p \equiv 2 \pmod{3}). \end{cases} \\
 K = 8_{19} & \left\{ \begin{array}{l} T_1 \mathcal{U}_{p+1} = 2^{(h_p)}, \frac{12}{r(p)} \\ T_1 \mathcal{M}_{p+1} = 2^{(h_p)}, \frac{12d(p)}{r(p)} \end{array} \right\} \quad \text{where } h_p = \begin{cases} \frac{p-1}{2} & (p \equiv 1 \pmod{4}), \\ \frac{p-3}{2} & (p \equiv 3 \pmod{4}). \end{cases}
 \end{aligned}$$

REFERENCES

1. R. H. Fox, A quick trip through knot theory, *Topology of 3-manifolds and related topics* (Englewood Cliffs, N.J., 1962), 120–167.
2. R. H. Fox, Metacyclic invariants of knots and links, *Canad. J. Math.* **22** (1970), 193–201.
3. R. Fricke, *Lehrbuch der Algebra*, Dritter Band (Braunschweig, 1928).
4. J. Lehner, *A short course in automorphic functions* (New York, 1966).
5. B. Maskit, On Poincaré’s theorem for fundamental polygons, *Advances in Mathematics* **7** (1971), 219–230.
6. R. Riley, Homomorphisms of knot groups on finite groups, *Math. Comp.* **25** (1971), 603–619.
7. R. Riley, Parabolic representations of knot groups, I, *Proc. London Math. Soc.* (3) **24** (1972), 217–242.
8. D. Singerman, Subgroups of Fuchsian groups and finite permutation groups, *Bull. London Math. Soc.* **2** (1970), 319–323.
9. R. Evans, A fundamental region for Hecke’s modular group, *J. Number Theory* **5** (1973), 108–115.

UNIVERSITY OF SOUTHAMPTON