

**GENERALISED KNOT GROUPS DISTINGUISH THE SQUARE
AND GRANNY KNOTS
(WITH AN APPENDIX BY DAVID SAVITT)**

CHRISTOPHER TUFFLEY

ABSTRACT. Given a knot K we may construct a group $G_n(K)$ from the fundamental group of K by adjoining an n th root of the meridian that commutes with the corresponding longitude. These “generalised knot groups” were introduced independently by Wada and Kelly, and contain the fundamental group as a subgroup. The square knot SK and the granny knot GK are a well known example of a pair of distinct knots with isomorphic fundamental groups. We show that $G_n(SK)$ and $G_n(GK)$ are non-isomorphic for all $n \geq 2$. This confirms a conjecture of Lin and Nelson, and shows that the isomorphism type of $G_n(K)$, $n \geq 2$, carries more information about K than the isomorphism type of the fundamental group. The appendix contains some results on representations of the trefoil group in $PSL(2, p)$ that are needed for the proof.

1. INTRODUCTION

Wada [8] and Kelly [5] independently introduced a family of link invariants $G_n(L)$ generalising the fundamental group of a link L in S^3 . These groups may be defined via Wirtinger-type presentations, with conjugation by the generator x_j corresponding to the over-arc replaced by conjugation by x_j^n , but also admit a description in terms of the peripheral system of L . The group $G_1(L)$ is simply the fundamental group of L , and the second description of G_n shows that $G_1(L)$ is a subgroup of $G_n(L)$ for each n .

The square knot SK and the granny knot GK are a well known example of a pair of distinct knots with isomorphic fundamental groups. They are therefore a natural choice for a pair of knots on which to test the strength of the invariant G_n . Lin and Nelson [6] report the results of computer experiments in which they were unable to distinguish $G_n(SK)$ and $G_n(GK)$ by counting homomorphisms to selected finite groups of orders as large as 360. Although they were not successful in distinguishing $G_n(SK)$ and $G_n(GK)$, they nevertheless conjectured that these groups were non-isomorphic for each $n \geq 2$. The purpose of this paper is to confirm their conjecture, and thereby show that the isomorphism types of the generalised knot groups carry more information about K than the isomorphism type of the fundamental group itself.

We will distinguish $G_n(SK)$ and $G_n(GK)$ for $n \geq 2$ by comparing the number of homomorphisms into suitably chosen finite groups. Our target groups will be wreath products over $PSL(2, p)$, and are described in Section 3. Our main result is the following theorem:

2000 *Mathematics Subject Classification.* Primary 57M27; secondary 20F38, 20G40.

Key words and phrases. Knot invariants, generalised knot group, Wirtinger presentation, trefoil knot, projective special linear group.

Theorem 1.1. *For each $n \geq 2$ there is a finite group H such that*

$$|\mathrm{Hom}(G_n(GK), H)| < |\mathrm{Hom}(G_n(SK), H)|.$$

Consequently, $G_n(GK)$ is not isomorphic to $G_n(SK)$ for $n \geq 2$.

Remark 1.2. Although our work confirms Lin and Nelson's conjecture that $G_n(SK)$ and $G_n(GK)$ are non-isomorphic for all $n \geq 2$, it also provides counterexamples to their initial claim that $|\mathrm{Hom}(G_n(SK), H)| = |\mathrm{Hom}(G_n(GK), H)|$ for all finite groups H . The source of the error lies in the statements about permutations used to prove Proposition 4.1 of arXiv versions 1 and 2 of their paper, which are incorrect. This claim has been withdrawn in the text of subsequent arXiv and the published versions of their paper, although it still appears in the abstract of the published version.

1.1. Update. Since this paper was written, Nelson and Neumann [7] have shown via topological methods that $G_2(K)$ determines the knot K up to reflection. They extend their result to $G_n(K)$, $n > 2$, using the Scott-Swarup JSJ decomposition for groups.

1.2. Organisation. The paper is organised as follows. In Section 2 we describe Wada and Kelly's generalised link groups, and obtain presentations for the generalised knot groups of the square and granny knots. We construct our target groups in Section 3, and establish some results that will be used in the proof of Theorem 1.1, which appears in Section 4. Finally, we include an appendix by David Savitt, which contains two results on $PSL(2, p)$ that are needed for the proof.

2. GENERALISED LINK GROUPS

2.1. Definition and presentations. The groups $G_n(L)$ may be defined in several different ways. Wada defines them via the closed braid form of L , using an action of the braid group B_m on the free group F_m that is compatible with the Markov moves. He observes that they admit a Wirtinger-type presentation, and gives a topological description of them as the fundamental group of a space associated with the link. Kelly, on the other hand, approaches them via the link quandle and the Wirtinger-type presentation. We will chiefly use Wada's topological description, as this leads to simpler calculations for the groups we are interested in.

To define $G_n(L)$ topologically we glue a torus to each boundary component of the exterior of L . We do this via the map $f : S^1 \times S^1 \rightarrow S^1 \times S^1$ given by $f(z_1, z_2) = (z_1^n, z_2)$, where z_1 represents the meridian and z_2 the longitude. The group $G_n(L)$ is defined to be the fundamental group of the resulting space, and is clearly an invariant of L .

To obtain a presentation for $G_n(L)$ we may take as generators elements x_i corresponding to each arc of the link diagram. This leads to a Wirtinger-type presentation, with a relation $x_k = x_j^n x_i x_j^{-n}$ at each left-handed crossing, and $x_k = x_j^{-n} x_i x_j^n$ at each right-handed crossing (see Fig. 1). However, we may also apply the Seifert-van Kampen Theorem to obtain a presentation of $G_n(L)$ from a presentation

$$\pi_1(S^3 \setminus L) = \langle g_1, \dots, g_m | r_1, \dots, r_p \rangle$$

as follows. Suppose that L has ℓ components, and let μ_i, λ_i be words in the generators representing a meridian-longitude pair of the i th component. If the torus glued to the i th boundary component has fundamental group $\langle \nu_i, \rho_i | \nu_i \rho_i = \rho_i \nu_i \rangle$,



FIGURE 1. The Wirtinger-type relations at left- and right-handed crossings.

then the gluing induces the identifications $\mu_i = \nu_i^n$, $\lambda_i = \rho_i$, and we conclude that $G_n(L)$ has a presentation

$$G_n(L) = \langle g_1, \dots, g_m, \nu_1, \dots, \nu_\ell | r_1, \dots, r_p, \nu_i^n = \mu_i, \lambda_i \nu_i = \nu_i \lambda_i, i = 1, \dots, \ell \rangle.$$

Thus, $G_n(L)$ is obtained from the fundamental group of L by adjoining an n th root of each meridian that commutes with the corresponding longitude. Note that, since μ_i and ν_i commute, we are not required to use zero-framed longitudes, and may freely replace λ_i with $\lambda'_i = \lambda_i \mu_i^k$ for any k .

When K is a knot the presentation above reduces to

$$G_n(K) = \langle g_1, \dots, g_m, \nu | r_1, \dots, r_p, \nu^n = \mu, \lambda \nu = \nu \lambda \rangle.$$

Let $\sqrt[n]{\mu}$ denote the set of n th roots of μ in $G_n(K)$, and let C be the centraliser of μ in $\pi_1(S^3 \setminus K)$. Then C acts on $\sqrt[n]{\mu}$ by conjugation, and in particular, when K is composite the longitude of each factor permutes the n th roots of μ . This action underlies the method by which we will distinguish $G_n(SK)$ and $G_n(GK)$.

Remark 2.1. Crisp and Paris [2] generalise Wada's representations of the braid groups and use their generalisations to define further group invariants of links. Given a group H and an element h of H their construction leads to an invariant $\Gamma_{(H,h)}$, such that G_n is the case $H = \mathbb{Z}$, $h = n$. Topologically, their construction replaces the attached tori with attached copies of $X \times S^1$, where $\pi_1(X) \cong H$ and each meridian is attached to a loop representing h . Careful attention is paid to the framing in attaching the S^1 factor to the boundary torus.

The ability of such an invariant to distinguish links depends on the extent to which it is able to remember the peripheral system. Conway and Gordon [1] define an extension of $\pi_1(S^3 \setminus K)$ that completely classifies knots up to oriented equivalence. Their construction allows them to recover the subgroups $\langle \mu \rangle$, $\langle \lambda \rangle$ as the images of the normalisers of certain subgroups of finite order. This method does not appear to be directly applicable to G_n , since it has no torsion, but might apply to $\Gamma_{(H,h)}$ for suitably chosen H and h .

Remark 2.2. When $n = 2$ the space used to define $G_n(L)$ topologically is a closed non-orientable 3-manifold. Nelson and Neumann's proof [7] that $G_2(K)$ determines K up to reflection uses the JSJ decomposition of this 3-manifold.

2.2. The square and granny knots. In this section we obtain presentations for the generalised knot groups of the square and granny knots. Our presentations may be obtained from those given in [6], but our derivation uses the Seifert-van Kampen

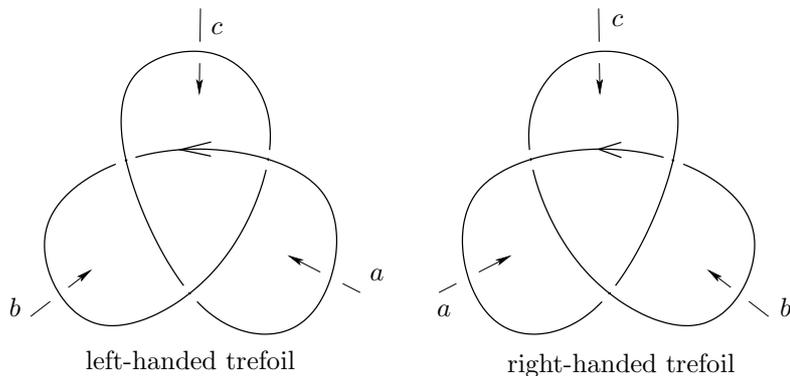


FIGURE 2. Generators for $\pi_1(S^3 \setminus K)$ for the left and right trefoils.

method described above, rather than the Wirtinger-type presentation, and is more direct.

The granny knot is the connect sum of two left- or two right-handed trefoils, while the square knot is the connect sum of a left- and a right-handed trefoil. The fundamental groups of these knots are therefore amalgamated free products of two copies of the trefoil group. Accordingly, we begin by fixing notation for the trefoil group T . We choose generators for T as shown in Fig. 2, so that for both the left and right trefoils we have

$$T \cong \langle a, b, c \mid ab = bc = ca \rangle \cong \langle a, c \mid aca = cac \rangle.$$

This may be put in the form

$$T \cong \langle x, y \mid x^3 = y^2 \rangle$$

by letting $x = ab$, $y = abc$, and we note that any two of a , c , x and y generate T . The 0-framed longitude corresponding to a of the right-handed trefoil is represented by $(bac)a^{-3}$, while that of the left-handed trefoil is represented by $(c^{-1}a^{-1}b^{-1})a^3$. Note that $x^3 = (bac)a^3$ and $x^{-3} = (c^{-1}a^{-1}b^{-1})a^{-3}$ respectively also represent longitudes corresponding to a , albeit with framings 6 and -6 .

To obtain presentations and longitudes of the square knot and granny knot groups we refer to Fig. 3. The group $\pi_1(S^3 \setminus (K_1 \# K_2))$ is given by

$$\pi_1(S^3 \setminus (K_1 \# K_2)) = \pi_1(S^3 \setminus K_1) *_{\langle \mu \rangle} \pi_1(S^3 \setminus K_2),$$

and has meridian and longitude $\mu = \mu_1 = \mu_2$, $\lambda = \lambda_1 \lambda_2$. Let

$$\tilde{T} = \langle d, e, f \mid de = ef = fd \rangle$$

be a second copy of T , with $w = de$, $z = def$, and identify the meridians a and d to get

$$\pi_1(SK) \cong \pi_1(GK) \cong \langle a, c, f \mid aca = cac, afa = faf \rangle.$$

Letting K_1 and K_2 be right- and left-handed trefoils respectively we may take $x^3 w^{-3} = (ca)^3 (fa)^{-3}$ as a longitude of SK ; and similarly, letting K_1 and K_2 be two right-handed trefoils, we may take $x^3 w^3 = (ca)^3 (fa)^3$ as a longitude of GK . It

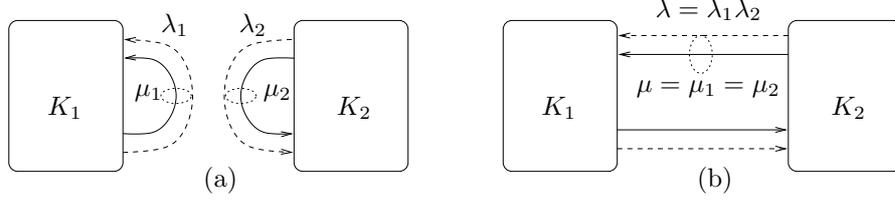


FIGURE 3. Meridian and longitude for the connect sum of two knots.

now follows that

$$\begin{aligned} G_n(SK) &\cong \langle a, c, f, \nu \mid aca = cac, afa = faf, \nu^n = a, x^3 w^{-3} \nu = \nu x^3 w^{-3} \rangle, \\ G_n(GK) &\cong \langle a, c, f, \nu \mid aca = cac, afa = faf, \nu^n = a, x^3 w^3 \nu = \nu x^3 w^3 \rangle, \end{aligned}$$

which we may re-write as

$$\begin{aligned} G_n(SK) &\cong \langle a, c, f, \nu \mid aca = cac, afa = faf, \nu^n = a, w^{-3} \nu w^3 = x^{-3} \nu x^3 \rangle, \\ G_n(GK) &\cong \langle a, c, f, \nu \mid aca = cac, afa = faf, \nu^n = a, w^3 \nu w^{-3} = x^{-3} \nu x^3 \rangle. \end{aligned}$$

We note that the only difference between the two presentations is the last relation, which relates the actions by conjugation of the longitudes of each factor on the n th roots of a .

3. THE TARGET GROUPS

3.1. Construction. We will use as target groups wreath products of the form

$$\mathcal{H}_p^{q,r} = \mathcal{D}_{q,r} \wr \mathbb{P}^1(\mathbb{F}_p) = (\mathcal{D}_{q,r})^{\mathbb{P}^1(\mathbb{F}_p)} \rtimes \mathbb{P}^1(\mathbb{F}_p),$$

where p, q, r are distinct primes, $\mathbb{P}^1(\mathbb{F}_p)$ is the projective line over the p -element field, and $\mathcal{D}_{q,r}$ is a semidirect product

$$\mathcal{D}_{q,r} = (\mathbb{Z}/q\mathbb{Z})^{r-1} \rtimes (\mathbb{Z}/r\mathbb{Z}).$$

We define these groups and some associated homomorphisms below.

To construct $\mathcal{D}_{q,r}$ we regard $V = (\mathbb{Z}/q\mathbb{Z})^{r-1}$ as the additive group of the finite field $\mathbb{F}_{q^{r-1}}$. The multiplicative group $\mathbb{F}_{q^{r-1}}^\times$ is cyclic of order $q^{r-1} - 1$, and so contains an element ζ of order r , because r divides $q^{r-1} - 1$ by Fermat's Theorem. We may therefore define multiplication in $\mathcal{D}_{q,r} = V \rtimes \mathbb{Z}/r\mathbb{Z}$ by

$$(v, i) \cdot (w, j) = (v + \zeta^i w, i + j).$$

We remark that when $r = 2$ we have $V = \mathbb{Z}/q\mathbb{Z}$, and $\zeta = -1$ of (multiplicative) order two in $(\mathbb{Z}/q\mathbb{Z})^\times$. Thus $\mathcal{D}_{q,2}$ is isomorphic to D_q , the dihedral group with $2q$ elements. The group $\mathcal{D}_{2,3}$ is also isomorphic to a familiar group, the alternating group A_4 . Under an isomorphism $\mathcal{D}_{2,3} \rightarrow A_4$ the normal subgroup $V = (\mathbb{Z}/2\mathbb{Z})^2$ maps onto the Klein 4-group generated by the permutations of order two.

To define the wreath product we regard vectors in $(\mathbb{F}_p)^2$ as rows, and use the faithful action of $PSL(2, p)$ on the projective line induced by the natural action of $SL(2, p)$ on row vectors by right multiplication. For convenience we will identify the point in $\mathbb{P}^1(\mathbb{F}_p)$ with homogeneous co-ordinates $[x : y]$ with the quotient $x/y \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$; under this identification the action of the class of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $PSL(2, p)$

is given by the fractional linear transformation $z \mapsto \frac{az + c}{bz + d}$. This right action on indices induces a *left* action of $PSL(2, p)$ on $(\mathcal{D}_{q,r})^{\mathbb{P}^1(\mathbb{F}_p)}$, and we define $\mathcal{H}_p^{q,r}$ to be the semidirect product of $(\mathcal{D}_{q,r})^{\mathbb{P}^1(\mathbb{F}_p)}$ by $PSL(2, p)$ defined by this action. Elements of $\mathcal{H}_p^{q,r}$ then have the form

$$\alpha = ((\alpha_0, \alpha_1, \dots, \alpha_{p-1}, \alpha_\infty), \hat{\alpha}),$$

where $\alpha_i \in \mathcal{D}_{q,r}$ for each i and $\hat{\alpha} \in PSL(2, p)$, and multiplication is given by

$$(\alpha\beta)_i = \alpha_i\beta_{i\hat{\alpha}}, \quad \widehat{\alpha\beta} = \hat{\alpha}\hat{\beta}.$$

Note that as permutations, $\hat{\alpha}$ and $\hat{\beta}$ are composed from left to right. We adopt the convention that α_i^{-1} means $(\alpha_i)^{-1}$, so that $(\alpha^{-1})_i = (\alpha_{i\hat{\alpha}^{-1}})^{-1} = \alpha_{i\hat{\alpha}^{-1}}^{-1}$.

The quotient map $\mathcal{D}_{q,r} \rightarrow \mathbb{Z}/r\mathbb{Z}$ induces a quotient map

$$\mathcal{H}_p^{q,r} \rightarrow \mathbb{Z}/r\mathbb{Z} \wr PSL(2, p).$$

We will write $[g]$ for the image of $g \in \mathcal{D}_{q,r}$ in $\mathbb{Z}/r\mathbb{Z}$, so that the map $\mathcal{H}_p^{q,r} \rightarrow \mathbb{Z}/r\mathbb{Z} \wr PSL(2, p)$ is given by

$$[\alpha] = (([\alpha_0], [\alpha_1], \dots, [\alpha_{p-1}], [\alpha_\infty]), \hat{\alpha}).$$

This map splits, and it will be convenient to distinguish a subgroup of $\mathcal{H}_p^{q,r}$ isomorphic to $\mathbb{Z}/r\mathbb{Z} \wr PSL(2, p)$. Fixing $\xi \in \mathcal{D}_{q,r}$ such that $[\xi] = 1 \in \mathbb{Z}/r\mathbb{Z}$ we let $\mathcal{A}_p^r = \langle \xi \rangle \wr PSL(2, p) \subseteq \mathcal{H}_p^{q,r}$.

Since $\mathbb{Z}/r\mathbb{Z}$ is abelian we may quotient further to get a well defined map

$$\mathcal{H}_p^{q,r} \rightarrow \mathbb{Z}/r\mathbb{Z} \wr PSL(2, p) \rightarrow \mathbb{Z}/r\mathbb{Z},$$

given by

$$[[\alpha]] = [\alpha_0] + [\alpha_1] + \dots + [\alpha_{p-1}] + [\alpha_\infty].$$

The subgroup $V \wr PSL(2, p)$ has a similarly defined map $\|\cdot\| : V \wr PSL(2, p) \rightarrow V$. We will use these abelianisations in Section 4.4.

To prove Theorem 1.1 we will choose p co-prime to n , q dividing n , and r co-prime to n and $|PSL(2, p)|$. These divisibility requirements reflect the roles that the factors $PSL(2, p)$, $(\mathbb{Z}/q\mathbb{Z})^{r-1}$ and $\mathbb{Z}/r\mathbb{Z}$ play in the proof. The $PSL(2, p)$ factor ensures that there are nontrivial homomorphisms $G \rightarrow \mathcal{H}_p^{q,r}$; the $(\mathbb{Z}/q\mathbb{Z})^{r-1}$ factor will give us many n th roots; and the $\mathbb{Z}/r\mathbb{Z}$ factor will exhibit the nontrivial action by $x^3, w^3 \in G$ on the roots of the meridian.

Remark 3.1. When $p = 5$ we have $PSL(2, 5) \cong A_5$, which was the group used by Fox [4] to show that the complements of the square and granny knots can be distinguished by their peripheral subgroups.

3.2. Example. As an aid to understanding we illustrate the above constructions in the case of $\mathcal{H}_3^{5,2}$. This group is not used in the proof of Theorem 1.1 (distinguishing $w^{\pm 3}$ will ultimately hinge on being able to distinguish $\pm 3k$ in $\mathbb{Z}/r\mathbb{Z}$), but has the advantage of being a small example with a simple geometric interpretation.

The permutation representation of $PSL(2, 3)$ on $\mathbb{P}^1(\mathbb{F}_3)$ induces an isomorphism between $PSL(2, 3)$ and A_4 . Since $\mathcal{D}_{5,2}$ is isomorphic to D_5 , we therefore have $\mathcal{H}_3^{5,2} \cong D_5 \wr A_4$. To give this group a geometric interpretation let \mathcal{P} be the group

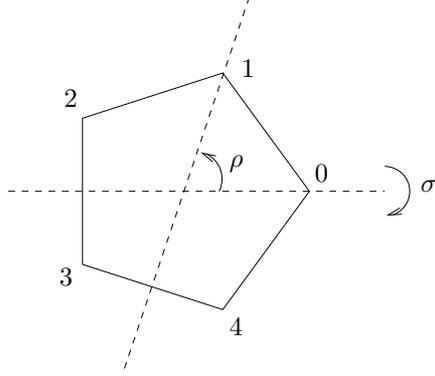


FIGURE 4. The vertex labelling of the pentagon, and generators for D_5 .

of symmetries of four regular pentagons. Label the vertices of each pentagon as in Fig. 4, and let

$$\rho = (0\ 1\ 2\ 3\ 4), \quad \sigma = (0)(1\ 4)(2\ 3)$$

be the indicated generators of D_5 . The labelling allows us to regard maps between distinct pentagons as elements of D_5 , and induces an isomorphism $\mathcal{P} \rightarrow D_5 \wr S_4$. Our group $\mathcal{H}_3^{5,2}$ may therefore be viewed as the subgroup of \mathcal{P} such that the underlying permutation of the polygons is even.

To illustrate the group operations in $\mathcal{H}_3^{5,2}$ define A, B, C in $SL(2, \mathbb{Z})$ by

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad C = AB = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix},$$

and let $\hat{\alpha}, \hat{\beta}, \hat{\gamma}$ be the corresponding projections to $PSL(2, 3)$. As fractional linear transformations we have

$$z \cdot \hat{\alpha} = z + 1, \quad z \cdot \hat{\beta} = -1/z, \quad z \cdot \hat{\gamma} = (z \cdot \hat{\alpha}) \cdot \hat{\beta} = -1/(z + 1),$$

giving

$$\hat{\alpha} = (0\ 1\ 2)(\infty), \quad \hat{\beta} = (0\ \infty)(1\ 2), \quad \hat{\gamma} = \hat{\alpha}\hat{\beta} = (0\ 2\ \infty)(1)$$

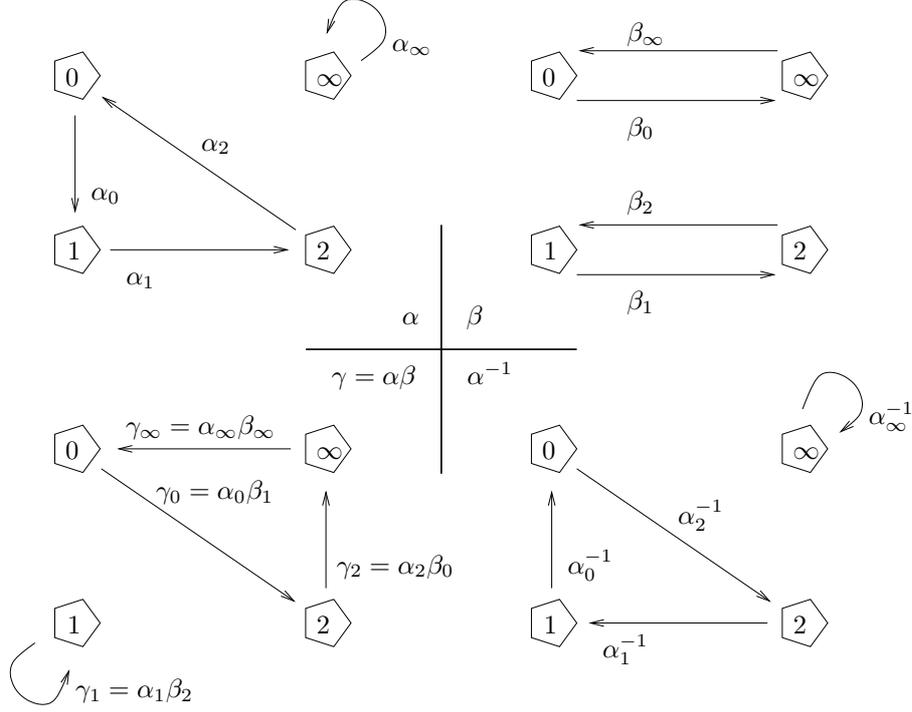
as permutations of $\{0, 1, 2, \infty\}$. Elements $\alpha, \beta \in \mathcal{H}_3^{5,2}$ permuting the pentagons according to $\hat{\alpha}, \hat{\beta}$ may therefore be visualised as in Fig. 5, where each arrow and label describes an isometry of pentagons. The product $\gamma = \alpha\beta$ is found by composing α and β from left to right, and inverses are found by reversing all arrows and inverting all labels. For example, if

$$\alpha = ((\rho, \rho^2\sigma, \rho^3, \rho^4\sigma), \hat{\alpha}), \quad \beta = ((\rho^3, \rho, \rho^4, \sigma), \hat{\beta}),$$

then

$$\begin{aligned} \gamma &= ((\rho \cdot \rho, \rho^2\sigma \cdot \rho^4, \rho^3 \cdot \rho^3, \rho^4\sigma \cdot \sigma), \hat{\alpha}\hat{\beta}) = ((\rho^2, \rho^3\sigma, \rho, \rho^4), \hat{\gamma}), \\ \alpha^{-1} &= ((\rho^{-3}, \rho^{-1}, (\rho^2\sigma)^{-1}, (\rho^4\sigma)^{-1}), \hat{\alpha}^{-1}) = ((\rho^2, \rho^4, \rho^2\sigma, \rho^4\sigma), \hat{\alpha}^{-1}). \end{aligned}$$

The homomorphism $[\cdot] : \mathcal{H}_3^{5,2} \rightarrow \mathbb{Z}/2\mathbb{Z} \wr PSL(2, 3)$ records whether each map α_i preserves or reverses orientation, and $[[\cdot]]$ records a “net change of orientation”.

FIGURE 5. Visualising elements and group operations in $\mathcal{H}_3^{5,2}$.

With α , β and γ as above we have

$$\begin{aligned} [\alpha] &= ((0, 1, 0, 1), \hat{\alpha}), & [\beta] &= ((0, 0, 0, 1), \hat{\beta}), & [\gamma] &= ((0, 1, 0, 0), \hat{\gamma}), \\ [[\alpha]] &= 0, & [[\beta]] &= 1, & [[\gamma]] &= [[\alpha]] + [[\beta]] = 1. \end{aligned}$$

The homomorphism $\|\cdot\|$ mapping $V \wr PSL(2, 3) \cong \langle \rho \rangle \wr A_4$ onto $\langle \rho \rangle$ is similar to $[[\cdot]]$ and records a “net rotation”: if $\delta = ((\rho^3, \rho, 1, \rho^3), \hat{\delta})$ then $\|\delta\| = \rho^{3+1+0+3} = \rho^2$. Finally, to split $[\cdot]$ we may choose say $\xi = \sigma$; then $\mathcal{A}_3^2 = \langle \sigma \rangle \wr PSL(2, 3)$ is a subgroup of $\mathcal{H}_3^{5,2}$ mapped isomorphically onto $\mathbb{Z}/2\mathbb{Z} \wr PSL(2, 3)$ by $[\cdot]$.

Looking ahead to Section 3.4, observe that the isomorphism $\mathcal{P} \rightarrow D_5 \wr S_4$ depends on the choice of identification of each pentagon with the labelled pentagon of Fig. 4. From the perspective of $\mathcal{H}_3^{5,2}$, changing these identifications conjugates the group by an element δ such that $\hat{\delta} = 1$. For example, relabelling pentagons one and two so that α_0 and α_1 are the “identity” conjugates $\mathcal{H}_3^{5,2}$ by $((1, \alpha_0, \alpha_0 \alpha_1, 1), 1)$, and takes α to $((1, 1, \alpha_0 \alpha_1 \alpha_2, \alpha_\infty), \hat{\alpha})$. The composition $\alpha_0 \alpha_1 \alpha_2$ occurring here is a map from the zeroth pentagon to itself, and as such is well defined up to conjugacy under such relabellings. We will refer to such a composition around a cycle of $\hat{\alpha}$ as a *cycle-product*.

Let ε be an element of $\mathcal{H}_3^{5,2}$ such that $\hat{\varepsilon} = \hat{\alpha} = (0 \ 1 \ 2)$ and $\varepsilon_{i, \hat{\varepsilon}} = \varepsilon_i$ for all i . In other words, ε has the form $((\varepsilon_0, \varepsilon_0, \varepsilon_0, \varepsilon_\infty), \hat{\alpha})$. Using a similar relabelling to the above we find that ε is conjugate to $((1, 1, \varepsilon_0^3, \varepsilon_\infty), \hat{\alpha})$. Since the cycle-product $\alpha_0 \alpha_1 \alpha_2$ necessarily has a cube root η in D_5 , we may set $\varepsilon_0 = \eta$, $\varepsilon_\infty = \alpha_\infty$ and

conclude that α is conjugate to ε . The benefit of this is that certain calculations are simpler for ε than they are for α : for example, ε^k is simply $((\varepsilon_0^k, \varepsilon_0^k, \varepsilon_0^k, \varepsilon_\infty^k), \hat{\alpha}^k)$.

In Section 3.4 we will say that an element ε such that ε_i is constant on orbits of $\hat{\varepsilon}$ is in *standard form*. For α , β and γ as above we find that α is conjugate to $((\sigma, \sigma, \sigma, \rho^4 \sigma), \hat{\alpha})$, and γ is conjugate to $((\rho^4, \rho^3 \sigma, \rho^4, \rho^4), \hat{\gamma})$. Thus, both α and γ are conjugate to elements in standard form; in fact, α may be conjugated further to $((\sigma, \sigma, \sigma, \sigma), \hat{\alpha})$, so α is conjugate to an element of \mathcal{A}_3^2 in standard form. However, β cannot be conjugated to standard form, because the cycle-product $\beta_0 \beta_\infty = \rho^3 \sigma$ has no square root in D_5 . Our arguments in later sections will be simplified by showing that we can typically avoid this situation, and restrict our attention to elements in standard form.

3.3. The structure of $\mathcal{D}_{q,r}$. We will make use of the following facts about elements of $\mathcal{D}_{q,r}$ and representations of T in $\mathcal{D}_{q,r}$:

Lemma 3.2.

- (1) If $g \in \mathcal{D}_{q,r}$ then the order of g is 1, q , or r .
- (2) If $g, h \in \mathcal{D}_{q,r}$ commute then either $g, h \in V$, or g and h belong to the same cyclic subgroup of order r .
- (3) If $g = (v, 0)$ has order q then the conjugacy class of g is

$$\{(\zeta^i v, 0) \mid 0 \leq i \leq r-1\},$$

and if $g = (v, i)$ has order r then the conjugacy class of g is $\{h : [h] = i\}$.

- (4) If $\{q, r\} \neq \{2, 3\}$ then a homomorphism $\phi : T \rightarrow \mathcal{D}_{q,r}$ factors through \mathbb{Z} .

Proof. Since elements of V have order 1 or q , to prove part (1) it suffices to show that an element (v, i) with $i \neq 0$ has order r . This follows from the fact that ζ satisfies the equation

$$1 + \zeta^i + \zeta^{2i} + \dots + \zeta^{(r-1)i} = 0$$

in $\mathbb{F}_{q^{r-1}}$.

To prove part (2), suppose that $g = (v, i)$, $h = (w, j)$ commute and that $g \notin V$. We must show that $h \in \langle g \rangle$. The equation $gh = hg$ is

$$(v + \zeta^i w, i + j) = (w + \zeta^j v, i + j),$$

which gives $(1 - \zeta^j)v = (1 - \zeta^i)w$. Our assumption that $g \notin V$ is equivalent to $i \not\equiv 0 \pmod{r}$, which implies firstly that $1 - \zeta^i$ is nonzero in $\mathbb{F}_{q^{r-1}}$, and secondly that there is some $1 \leq k \leq r$ such that $j \equiv ki \pmod{r}$. Thus

$$\begin{aligned} w &= \frac{1 - \zeta^{ki}}{1 - \zeta^i} v \\ &= \frac{(1 - \zeta^i)(1 + \zeta^i + \zeta^{2i} + \dots + \zeta^{(k-1)i})}{1 - \zeta^i} v \\ &= (1 + \zeta^i + \zeta^{2i} + \dots + \zeta^{(k-1)i}) v, \end{aligned}$$

and it follows that $h = g^k$.

Part (2) implies that the stabiliser of $g \in \mathcal{D}_{q,r}$ has order q^{r-1} if g has order q , and order r if g has order r . Thus, the conjugacy class of g has size r if g has order q , and size q^{r-1} if g has order r . Part (3) now follows from the fact that the conjugacy class of $(v, 0)$ must contain the r element set consisting of the orbit of v under the action of $\langle \zeta \rangle$, and the fact that the conjugacy class of (v, i) is contained in the q^{r-1} element set $\{h : [h] = i\}$.

Finally, to prove part (4) we consider the image of $x^3 = y^2$, which generates the centre of T . By (2), if x^3 does not map to the identity then the image of ϕ lies in an abelian subgroup, and ϕ must factor through the abelianisation $T \rightarrow \mathbb{Z}$. On the other hand, if $\{q, r\} \neq \{2, 3\}$ and $\phi(x)^3 = \phi(y)^2 = 1$, then at least one of $\phi(x)$, $\phi(y)$ must be the identity, in which case the image of ϕ lies in the cyclic subgroup generated by the other. \square

3.4. The cycle-product and some consequences. In this section we gather some results on conjugacy classes, centralisers, and m th powers in $\mathcal{H}_p^{q,r}$ that will be needed in what follows. Our main tool for proving the results will be the cycle-product, which may be regarded as a kind of monodromy.

Given $\alpha \in \mathcal{H}_p^{q,r}$ and $i \in \mathbb{P}^1(\mathbb{F}_p)$ we define the *cycle-product of α at i* by

$$\pi_i(\alpha) = \prod_{k=0}^{\ell_i(\hat{\alpha})-1} \alpha_{i \cdot \hat{\alpha}^k} = \alpha_i \alpha_{i \cdot \hat{\alpha}} \alpha_{i \cdot \hat{\alpha}^2} \cdots \alpha_{i \cdot \hat{\alpha}^{\ell_i(\hat{\alpha})-1}},$$

where $\ell_i(\hat{\alpha})$ is the length of the disjoint cycle of $\hat{\alpha}$ containing i . The cycle-product is thus the ordered product, beginning at i , of α_j for j in the disjoint cycle of $\hat{\alpha}$ containing i . We note that the value of the cycle-product on a given cycle depends on the starting point i , but the conjugacy class does not, because $\pi_{i \cdot \hat{\alpha}}(\alpha) = \alpha_i^{-1} \pi_i(\alpha) \alpha_i$.

Given $\gamma \in \mathcal{H}_p^{q,r}$ we will say that γ is in *standard form* if

$$\gamma_{i \cdot \hat{\gamma}} = \gamma_i$$

for all i . If in addition $\pi_i(\gamma) = \gamma_i^{\ell_i(\hat{\gamma})} = 1$ if and only if $\gamma_i = 1$, we will say that γ is in *reduced standard form*. Our first two results generalise the example at the end of Section 3.2, and show that many elements of $\mathcal{H}_p^{q,r}$ are conjugate to an element in reduced standard form.

Lemma 3.3. *Suppose that $\ell_i(\hat{\alpha})$ is co-prime to the order of $\pi_i(\alpha)$ for all i . Then α is conjugate to an element γ in reduced standard form such that $\hat{\gamma} = \hat{\alpha}$ and $\pi_i(\gamma)$ is conjugate to $\pi_i(\alpha)$ for all i .*

Proof. Let \mathcal{O} be a set of orbit representatives for the action of $\langle \hat{\alpha} \rangle$ on $\mathbb{P}^1(\mathbb{F}_p)$. Let $\beta = \delta \alpha \delta^{-1}$, where $\delta \in \mathcal{H}_p^{q,r}$ is defined by $\hat{\delta} = 1$ and

$$\delta_{j \cdot \hat{\alpha}^m} = \prod_{k=0}^{m-1} \alpha_{j \cdot \hat{\alpha}^k} = \alpha_j \alpha_{j \cdot \hat{\alpha}} \cdots \alpha_{j \cdot \hat{\alpha}^{m-1}}$$

for each $j \in \mathcal{O}$ and $1 \leq m \leq \ell_j(\hat{\alpha})$. Then $\hat{\beta} = \hat{\alpha}$, and

$$\beta_i = \delta_i \alpha_i \delta_{i \cdot \hat{\alpha}}^{-1} = \begin{cases} \pi_i(\alpha) & \text{if } i \in \mathcal{O}, \\ 1 & \text{otherwise.} \end{cases}$$

Let $j \in \mathcal{O}$. Since $\ell_j(\hat{\alpha})$ is co-prime to the order of $\pi_j(\alpha)$, there is $\eta_j \in \langle \pi_j(\alpha) \rangle$ such that $\eta_j^{\ell_j(\hat{\alpha})} = \pi_j(\alpha)$. Define $\gamma \in \mathcal{H}_p^{q,r}$ by $\hat{\gamma} = \hat{\alpha}$, and $\gamma_i = \eta_j$ if j represents the orbit of i . Then γ is in standard form, and $\pi_i(\gamma) = \pi_j(\gamma) = \pi_j(\alpha)$ for all $j \in \mathcal{O}$ and i in the orbit of j under $\hat{\alpha}$, so $\pi_i(\gamma)$ is conjugate to $\pi_i(\alpha)$ for all i . Moreover, γ is reduced, because $\gamma_i \in \langle \pi_i(\gamma) \rangle$ for all i . Since $\pi_j(\gamma) = \pi_j(\alpha)$ for all $j \in \mathcal{O}$, and \mathcal{O} is a set of orbit representatives for $\langle \hat{\gamma} \rangle$ acting on $\mathbb{P}^1(\mathbb{F}_p)$, the first paragraph implies that γ is conjugate to β , and hence to α . \square

Lemma 3.4. *Let α be an element of $\mathcal{H}_p^{q,r}$ in standard form such that α_i has order 1 or r for each i . Then α is conjugate to an element γ of \mathcal{A}_p^r in standard form. Moreover, if α is reduced then γ may be chosen to be reduced.*

Note that if α is in reduced standard form and $\pi_i(\alpha)$ has order 1 or r for all i , then α_i must have order 1 or r for all i also, so α satisfies the hypotheses of Lemma 3.4. We will use the lemma in this form in Section 4.3.

Proof. By Lemma 3.2, α_i is conjugate to $\xi^{[\alpha_i]}$ for each i . Since α is in standard form we may therefore choose $\beta_i \in \mathcal{D}_{q,r}$ for each i such that $\beta_{i,\hat{\alpha}} = \beta_i$ and $\beta_i \alpha_i \beta_i^{-1} \in \langle \xi \rangle$. Let $\gamma = \beta \alpha \beta^{-1}$, where $\beta = ((\beta_0, \beta_1, \dots, \beta_\infty), 1)$. Then

$$\gamma_i = \beta_i \alpha_i \beta_{i,\hat{\alpha}}^{-1} = \beta_i \alpha_i \beta_i^{-1} = \xi^{[\alpha_i]},$$

so $\gamma \in \mathcal{A}_p^r$. Moreover $\hat{\gamma} = \hat{\alpha}$, so

$$\gamma_{i,\hat{\gamma}} = \beta_{i,\hat{\alpha}} \alpha_i \beta_{i,\hat{\alpha}}^{-1} = \beta_i \alpha_i \beta_i^{-1} = \gamma_i,$$

and γ is still in standard form; and $\pi_i(\gamma) = \beta_i \pi_i(\alpha) \beta_i^{-1}$ for all i , so if α is reduced, so is γ . \square

We next study certain elements of the centraliser of an element in reduced standard form.

Lemma 3.5. *Let α be an element in reduced standard form, and suppose that γ commutes with α . If α_i is constant on orbits of $\hat{\gamma}$ then γ_i commutes with α_i for each i , and γ_i is constant on orbits of $\hat{\alpha}$.*

Proof. We have $(\alpha\gamma)_i = \alpha_i \gamma_{i,\hat{\alpha}}$, and $(\gamma\alpha)_i = \gamma_i \alpha_{i,\hat{\gamma}} = \gamma_i \alpha_i$. Thus $\alpha\gamma = \gamma\alpha$ implies

$$(3.1) \quad \gamma_{i,\hat{\alpha}} = \alpha_i^{-1} \gamma_i \alpha_i$$

for each i . If $\alpha_i = 1$ then we are done. Otherwise, we conjugate (3.1) by α_i repeatedly and use the fact that $\alpha_{i,\hat{\alpha}^j} = \alpha_i$ to get

$$\gamma_i = \gamma_{i,\hat{\alpha}^{\ell_i(\hat{\alpha})}} = \alpha_i^{-\ell_i(\hat{\alpha})} \gamma_i \alpha_i^{\ell_i(\hat{\alpha})}.$$

Now $\alpha_i^{\ell_i(\hat{\alpha})} \neq 1$, because $\alpha_i \neq 1$ and α is in reduced standard form. Therefore $\alpha_i^{\ell_i(\hat{\alpha})}$ generates $\langle \alpha_i \rangle$, because α_i has prime order. It follows that α_i and γ_i commute, and equation (3.1) becomes $\gamma_{i,\hat{\alpha}} = \gamma_i$, as required. \square

Finally, we give a necessary condition for $\alpha \in \mathcal{H}_p^{q,r}$ to be an m th power. We will use the condition in Section 4.3 with $m = n$, and again in Section 4.4, with $m = 2$ and 3.

Lemma 3.6. *Suppose that $\alpha = \gamma^m$ in $\mathcal{H}_p^{q,r}$. Then $\hat{\gamma}^m = \hat{\alpha}$, and*

$$\pi_i(\alpha) = (\pi_i(\gamma))^{m/\gcd(\ell_i(\hat{\gamma}), m)}.$$

In particular, the conjugacy class of $\pi_i(\alpha)$ is constant on orbits of $\hat{\gamma}$.

Proof. The equation $\alpha = \gamma^m$ gives $\hat{\alpha} = \hat{\gamma}^m$ and

$$\alpha_i = \prod_{k=0}^{m-1} \gamma_{i,\hat{\gamma}^k} = \gamma_i \gamma_{i,\hat{\gamma}} \gamma_{i,\hat{\gamma}^2} \cdots \gamma_{i,\hat{\gamma}^{m-1}}$$

for all i . Suppose that i belongs to a cycle of $\hat{\gamma}$ of length ℓ . Then i belongs to a cycle of $\hat{\alpha}$ of length $\ell' = \ell / \gcd(\ell, m)$, and

$$\pi_i(\alpha) = \prod_{s=0}^{\ell'-1} \alpha_{i \cdot \hat{\alpha}^s} = \prod_{s=0}^{\ell'-1} \alpha_{i \cdot \hat{\gamma}^{ms}} = \prod_{s=0}^{\ell'-1} \prod_{k=0}^{m-1} \gamma_{i \cdot \hat{\gamma}^{ms+k}} = \prod_{t=0}^{m\ell'-1} \gamma_{i \cdot \hat{\gamma}^t}.$$

Let $m' = m / \gcd(\ell, m)$. Then $m\ell' - 1 = \text{lcm}(\ell, m) - 1 = \ell m' - 1$, so

$$\prod_{t=0}^{m\ell'-1} \gamma_{i \cdot \hat{\gamma}^t} = \prod_{s=0}^{m'-1} \prod_{k=0}^{\ell-1} \gamma_{i \cdot \hat{\gamma}^{\ell s+k}} = \prod_{s=0}^{m'-1} \pi_i(\gamma) = (\pi_i(\gamma))^{m'},$$

giving $\pi_i(\alpha) = (\pi_i(\gamma))^{m/\gcd(\ell, m)}$, as required. The last statement follows from the fact that $\ell_i(\hat{\gamma})$ and the conjugacy class of $\pi_i(\gamma)$ are constant on orbits of $\hat{\gamma}$. \square

4. PROOF OF THEOREM 1.1

4.1. Strategy. As observed by Lin and Nelson [6] in the case $K = SK$ or GK , every homomorphism from $G_n(K)$ to a group H arises as a compatible choice of a homomorphism from $G_1(K)$ to H and an n th root of the image of the meridian. Given a map $\rho : G_1(K) \rightarrow H$ and an element η of H , we will say that (ρ, η) is a *map-root pair* for K in H if $\eta^n = \rho(\mu)$. Clearly, a map-root pair defines a homomorphism $\tilde{\rho} : G_n(K) \rightarrow H$ precisely when it satisfies the compatibility condition

$$\rho(\lambda)\eta = \eta\rho(\lambda).$$

Since $G_1(SK)$ and $G_1(GK)$ are both isomorphic to

$$G = \langle a, c, f \mid aca = cac, afa = faf \rangle,$$

with common meridian a , map-root pairs for GK and SK in $\mathcal{H}_p^{q,r}$ co-incide. A pair (ρ, η) is compatible for SK if

$$\rho(x^3 w^{-3})\eta = \eta\rho(x^3 w^{-3}),$$

and it is compatible for GK if

$$\rho(x^3 w^3)\eta = \eta\rho(x^3 w^3).$$

We may regard a homomorphism $\rho : G \rightarrow \mathcal{H}_p^{q,r}$ as a pair of homomorphisms $\rho_c, \rho_f : T \rightarrow \mathcal{H}_p^{q,r}$ such that $\rho_c(a) = \rho_f(a)$, using the fact that

$$G = \langle a, c \rangle *_{\langle a \rangle} \langle a, f \rangle \cong T *_{\langle a \rangle} T.$$

Given $\alpha \in \mathcal{H}_p^{q,r}$, let

$$\mathcal{C}(\alpha) = \{\beta \in C_{\mathcal{H}_p^{q,r}}(\alpha) : \hat{\beta} = 1\}.$$

We define an action of $\mathcal{C}(\alpha)$ on map-root pairs $(\rho, \eta) = ((\rho_c, \rho_f), \eta)$ such that $\rho(a) = \alpha$ by $\beta \cdot (\rho, \eta) = (\beta \cdot \rho, \eta)$, where

$$\beta \cdot (\rho_c, \rho_f) = (\rho_c, \beta\rho_f\beta^{-1}).$$

We prove Theorem 1.1 by showing that, for suitably chosen p, q and r ,

- (I) for any map-root pair (ρ, η) for SK and GK in $\mathcal{H}_p^{q,r}$, the orbit of (ρ, η) under the action of $\mathcal{C}(\rho(a))$ contains at least as many compatible pairs for SK as it does for GK ; and
- (II) there are compatible map-root pairs (ρ, η) for SK in $\mathcal{H}_p^{q,r}$ such that the orbit of (ρ, η) under the action of $\mathcal{C}(\rho(a))$ contains no pairs that are compatible for GK .

The prime r will be chosen so that r is co-prime to n and $|PSL(2, p)|$. This implies that r is co-prime to 6, because 6 divides the order of $PSL(2, p)$ for all p . The primes p and q will be chosen depending on n as follows:

- (1) If n is not divisible by 30 then we let p be the least prime co-prime to n , and let q be any prime dividing n . In this case $p = 2, 3$ or 5 , $PSL(2, p)$ is isomorphic to S_3, A_4 or A_5 , and r is co-prime to $6n$ if $p = 2$ or 3 , or to $30n$ if $p = 5$.
- (2) If 30 divides n then we may choose $q \geq 5$ dividing n , and we choose p co-prime to n such that $PSL(2, p)$ has no elements of orders 4, 5, 9, or q .

For p co-prime to 2 we have

$$|PSL(2, p)| = \frac{1}{2}p(p-1)(p+1),$$

so $PSL(2, p)$ has no elements of orders 5, 9 or q if $p \not\equiv 0$ or $\pm 1 \pmod{5, 9}$ or q . To show that we may avoid elements of order 4 we use the fact that -1 is a sum of two squares mod p . If $a^2 + b^2 = -1$ in $\mathbb{Z}/p\mathbb{Z}$ then the matrices

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$$

belong to $SL(2, p)$, and for $p \geq 3$ their images in $PSL(2, p)$ generate a subgroup K isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If p is congruent to 3 or 5 mod 8 then $|PSL(2, p)| \equiv 4 \pmod{8}$, so K is a Sylow 2-subgroup and there are no elements of order 4. Sufficient conditions on p in case (2) may thus be expressed in terms of congruence conditions modulo 5, 8, 9 and q , and Dirichlet's Theorem guarantees that we may choose p as required.

The conditions on p, q and r are chosen in part so that the order of a nontrivial n th power in $PSL(2, p)$ satisfies the following lemma. In particular, the lemma shows that when n is divisible by 30 we may use Proposition A.5. This will be important when we study the image of the longitude in Section 4.4.

Lemma 4.1. *Let $\tau^n = \phi \neq 1$ in $PSL(2, p)$. Then the orders of τ and ϕ are co-prime to both q and r . If $30 \nmid n$ then $p = 2, 3$ or 5 , and*

$$\text{ord}(\tau) = \text{ord}(\phi) = \begin{cases} 2 \text{ or } 3 & \text{if } p = 2 \text{ and } \gcd(3, n) = 1, \\ p & \text{otherwise.} \end{cases}$$

If $30 \mid n$ then $\text{ord}(\phi) > 6$.

Proof. The fact that $\text{ord}(\tau)$ and $\text{ord}(\phi)$ are co-prime to r is immediate from the fact that r is co-prime to $|PSL(2, p)|$; the fact that they are co-prime to q comes from the fact that $PSL(2, p)$ has no elements of order q if $30 \mid n$, and no elements of order q^2 when $30 \nmid n$.

The statements about $\text{ord}(\tau)$ and $\text{ord}(\phi)$ when $30 \nmid n$ are proved by explicitly considering the orders of elements in $PSL(2, p)$. If $p = 5$ then an element of $PSL(2, 5) \cong A_5$ has order 1, 2, 3 or 5. Since we use $p = 5$ exactly when n is divisible by 6 but not by 5, a nontrivial n th power and its root must both have order 5. Similar arguments apply when $p = 2$ or 3 .

Finally, if $30 \mid n$ then n is divisible by 6, so ϕ is a sixth power. In this case $2 \leq \text{ord}(\phi) \leq 6$ is impossible, because otherwise some power of τ would have order 4, 5 or 9, contrary to the choice of p . \square

4.2. Overview. In order to prove statements (I) and (II) we must calculate the n th roots of the image of the meridian, and the possible images of the longitudes x^3, w^3 of the two factor knots. We do this in Sections 4.3 and 4.4 respectively, and then prove statements (I) and (II) in Section 4.5. In Sections 4.3 and 4.4 we will restrict our attention to n th powers in $\mathcal{H}_p^{q,r}$ that project to nontrivial elements of $PSL(2, p)$, as n th powers that project to the identity are easily handled separately. The calculations will be simplified by first showing that up to conjugacy, such an n th power is an element of \mathcal{A}_p^r in reduced standard form. We assume throughout that p, q and r are chosen as described in the preceding section.

The results and arguments of the following sections are fairly technical, and it will be helpful to have an overview of the ideas underlying the proof. These are most readily seen when $\rho(a) = \alpha = \eta^n$ is in reduced standard form, and the order of $\hat{\eta}$ is co-prime to n . We outline the argument in this case. Under these conditions $\hat{\eta}$ is a power of $\hat{\alpha}$, so the orbits of $\hat{\alpha}$ and $\hat{\eta}$ co-incide. Lemma 3.5 thus implies that η is in standard form, and we therefore have

$$\alpha_i = (\eta^n)_i = (\eta_i)^n$$

in $\mathcal{D}_{q,r}$. Since n is divisible by q but not by r , either α_i is of order r and η_i is the unique n th root of α_i in $\langle \alpha_i \rangle$, or $\alpha_i = 1$ and $\eta_i \in V$. Thus, n th roots η of α with $\text{ord } \hat{\eta}$ co-prime to n are parametrised by V^c , where c is the number of cycles of $\hat{\eta}$ on which $\alpha_i = 1$.

To calculate the possible values of $\varepsilon = \rho(x^3)$ we will use Theorem A.1, which shows that either $\hat{\varepsilon} = \hat{\alpha}^6$, or $\hat{\varepsilon} = 1$. Since ε commutes with α , Lemma 3.5 implies that ε_i is constant on orbits of $\hat{\alpha}$, and commutes with α_i for all i . When $\hat{\varepsilon} = \hat{\alpha}^6$ we will be able to show that in fact $\varepsilon = \alpha^6$, and when $\hat{\varepsilon}$ is trivial Proposition A.5 will allow us to show that $[\varepsilon_i]$ is constant. Consequently, in the latter case $[\varepsilon_i]$ is equal to the average value $[[\varepsilon]]/(p+1)$, which is equal to $6[[\alpha]]/(p+1)$. The same arguments apply to $\delta = \rho(w^3)$, so the action on V^c induced by ε or δ acting on the roots of α by conjugation is either trivial, or is given by multiplication by $\zeta^{6[[\alpha]]/(p+1)}$. Writing the compatibility conditions in the form

$$\delta^{-1}\eta\delta = \varepsilon^{-1}\eta\varepsilon, \quad \delta\eta\delta^{-1} = \varepsilon^{-1}\eta\varepsilon,$$

it is easily checked that for such roots either both, neither, or only the left condition (that for SK) will be satisfied. The strict inequality in Theorem 1.1 will come from showing that this last case can in fact occur.

In general, ε and δ will be as described above, but $\hat{\eta}$ need not be a power of $\hat{\alpha}$, so η need not be in standard form. As a result, the set parametrising the n th roots of α that project to a given element of $PSL(2, p)$ can be more complicated. The product V^c will nevertheless still occur as a factor, with ε and δ acting as above again playing an important role in determining compatibility. However, it will no longer be the case that a compatible pair for GK is necessarily compatible for SK , necessitating our use of the $\mathcal{C}(\alpha)$ -action as an accounting device.

4.3. The image and roots of the meridian. In this section we characterise up to conjugacy solutions to the pair of equations $\eta^n = \alpha, \hat{\alpha} \neq 1$. This determines the possible values of the image and root of the meridian in a map-root pair (ρ, η) with $\widehat{\rho(a)} \neq 1$. In what follows we will use $1/n$ to denote the multiplicative inverse of n in $\mathbb{Z}/r\mathbb{Z}$.

Lemma 4.2. *If α is an n th power in $\mathcal{H}_p^{q,r}$ such that $\hat{\alpha} \neq 1$, then α is conjugate to an element of \mathcal{A}_p^r in reduced standard form.*

Lemma 4.3. *Let α be an element of \mathcal{A}_p^r in reduced standard form such that $\hat{\alpha} \neq 1$, and suppose that τ is an n th root of $\hat{\alpha}$ in $PSL(2,p)$. Then α has an n th root $\eta \in \mathcal{H}_p^{q,r}$ such that $\hat{\eta} = \tau$ if and only if α_i is constant on orbits of τ . If so, then η_i is constant on orbits of $\hat{\alpha}$. Let σ be a disjoint cycle of τ of length ℓ , let $d = \gcd(\ell, n)$, and let $j \in \mathbb{P}^1(\mathbb{F}_p)$ belong to σ . Then η_i is completely determined on σ by the values of $\eta_j, \eta_{j \cdot \tau}, \dots, \eta_{j \cdot \tau^{d-1}}$. The possible values for these elements are given by the solutions to*

$$(4.1) \quad \prod_{k=0}^{d-1} \eta_{j \cdot \tau^k} = \eta_j \eta_{j \cdot \tau} \cdots \eta_{j \cdot \tau^{d-1}} = \alpha_j^{d/n}$$

in $\langle \xi \rangle$ if $\alpha_j \neq 1$, and the solutions to

$$(4.2) \quad \prod_{k=0}^{d-1} \eta_{j \cdot \tau^k} = \eta_j \eta_{j \cdot \tau} \cdots \eta_{j \cdot \tau^{d-1}} \in V$$

in $\mathcal{D}_{q,r}$ if $\alpha_j = 1$.

Note that when $d = 1$ (i.e., when τ is a power of $\hat{\alpha}$), Lemma 4.3 asserts that α does have n th roots η such that $\hat{\eta} = \tau$, and that any such root is in standard form. Equations (4.1) and (4.2) reduce respectively to $\eta_j = \alpha_j^{1/n}$ and $\eta_j \in V$, in agreement with our treatment of this case in Section 4.2.

Proof. If $\eta^n = \alpha$ then by Lemma 3.6 we have

$$\pi_i(\alpha) = (\pi_i(\eta))^{n/\gcd(n, \ell_i(\hat{\eta}))}.$$

Now q divides n but not $\ell_i(\hat{\eta})$, by Lemma 4.1, so $\pi_i(\alpha)$ is a q th power in $\mathcal{D}_{q,r}$. Therefore $\pi_i(\alpha)$ has order 1 or r for each i . Since $\ell_i(\hat{\alpha})$ is co-prime to r for all i , Lemmas 3.3 and 3.4 imply that α is conjugate to an element of \mathcal{A}_p^r in reduced standard form. This proves Lemma 4.2

We now suppose that α is an element of \mathcal{A}_p^r in reduced standard form, and that η is an n th root of α such that $\hat{\eta} = \tau$. Let σ , ℓ and d be as in the statement of the lemma. Then σ^n consists of d disjoint cycles of length ℓ/d , so if i belongs to σ we have

$$\pi_i(\alpha) = \alpha_i^{\ell/d} = \xi^{\ell[\alpha_i]/d}.$$

By Lemma 3.6 the conjugacy class of $\pi_i(\alpha)$ is constant on σ , so $\ell[\alpha_i]/d$ is constant on σ by Lemma 3.2. Since ℓ is co-prime to r this implies that $[\alpha_i]$, and hence $\alpha_i = \xi^{[\alpha_i]}$, is constant on σ .

We have now proved the ‘‘only if’’ direction of Lemma 4.3; we prove the ‘‘if’’ direction by solving the equation $\eta^n = \alpha$ with $\hat{\eta} = \tau$ under the assumption that α_i is constant on orbits of τ . By Lemma 3.5 η_i must be constant on orbits of $\hat{\alpha}$, and η_i must commute with α_i , because η commutes with $\eta^n = \alpha$. If j belongs to σ then $\{j, j \cdot \tau, \dots, j \cdot \tau^{d-1}\}$ forms a complete set of $\hat{\alpha}$ -orbit representatives for the orbit of j under σ , so η is completely determined on σ by $\eta_j, \eta_{j \cdot \tau}, \dots, \eta_{j \cdot \tau^{d-1}}$.

Now

$$\alpha_j = (\eta^n)_j = \prod_{k=0}^{n-1} \eta_{j \cdot \tau^k} = \left(\prod_{k=0}^{d-1} \eta_{j \cdot \tau^k} \right)^{n/d} = H^{n/d}.$$

Suppose first that $\alpha_j \neq 1$. Then η_{j,τ^k} must belong to $\langle \xi \rangle$ for all k , by Lemma 3.2, and therefore H is a solution to $H^{n/d} = \alpha_j$ in $\langle \xi \rangle$. This has the unique solution $H = \alpha_j^{d/n}$, so $\eta_j, \eta_{j,\tau}, \dots, \eta_{j,\tau^{d-1}}$ are a solution to (4.1) in $\langle \xi \rangle$, as claimed.

On the other hand, if $\alpha_j = 1$ then the condition $\eta_i \alpha_i = \alpha_i \eta_i$ places no restriction on η_i on σ . H is thus a solution to $H^{n/d} = 1$ in $\mathcal{D}_{q,r}$. Now n is co-prime to r , by construction, and ℓ is co-prime to q , by Lemma 4.1, so n/d is divisible by q but not by r . It follows that H must have order 1 or q , so H belongs to V .

We have now shown that if η exists, then it must be as given in the Lemma. Conversely, let \mathcal{O} be a set of orbit representatives for τ acting on $\mathbb{P}^1(\mathbb{F}_p)$, and suppose that we are given an appropriate solution to equation (4.1) or (4.2) for each $j \in \mathcal{O}$. Define η_i on the rest of $\mathbb{P}^1(\mathbb{F}_p)$ by extending it to be constant on orbits of $\hat{\alpha}$, and let $\eta = ((\eta_0, \dots, \eta_\infty), \tau)$. Then $(\eta^n)_j = \alpha_j$ for each $j \in \mathcal{O}$, and $(\eta^n)_{j,\tau^m}$ is conjugate to $(\eta^n)_j$ by $\prod_{k=0}^{m-1} \eta_{j,\tau^k}$ for each j and m . The conjugating element belongs to the centraliser of α_j , so $(\eta^n)_{j,\tau^m} = \alpha_j = \alpha_{j,\tau^m}$, and we conclude that $\eta^n = \alpha$. To complete the proof we note that equations (4.1) and (4.2) have r^{d-1} and $|\mathcal{D}_{q,r}|^{d-1} \cdot |V|$ solutions respectively, so α does indeed have an n th root with shape τ under the hypothesis. \square

4.4. The image of the longitude. We next characterise the possibilities for the image of the longitude x^3, w^3 of each factor knot, under the assumption that $\rho(a) = \alpha$ has the form considered in Section 4.3.

Lemma 4.4. *Let α be an element of \mathcal{A}_p^r in reduced standard form such that $\hat{\alpha}$ is nontrivial and has an n th root in $PSL(2, p)$. Suppose that $\rho : T \rightarrow \mathcal{H}_p^{q,r}$ is a homomorphism such that $\rho(a) = \alpha$, and let $\varepsilon = \rho(x^3)$. If p, q and r are chosen as in Section 4.1 then either $\varepsilon = \alpha^6$, or*

- (1) $\hat{\varepsilon} = 1$;
- (2) ε_i is constant on orbits of $\hat{\alpha}$;
- (3) the conjugacy class of ε_i is constant on $\mathbb{P}^1(\mathbb{F}_p)$;
- (4) $[\varepsilon_i] = \frac{6}{p+1} [[\alpha]]$ for all i ; and
- (5) $\varepsilon_i = \xi^{6[[\alpha]]/(p+1)}$ if $\alpha_i \neq 1$.

Proof. We begin by noting that ε commutes with α , because x^3 generates the centre of T . Let $\chi = \rho(x), \psi = \rho(y)$, so that $\varepsilon = \chi^3 = \psi^2$. Then $\hat{\chi}^3 = \hat{\psi}^2 = \hat{\varepsilon}$ in $PSL(2, p)$, so by Theorem A.1 either $\hat{\varepsilon} = 1$, or $\hat{\chi}$ and $\hat{\psi}$ are powers of $\hat{\psi}\hat{\chi}^{-1} = \hat{\alpha}$. In the latter case $\hat{\varepsilon} = \hat{\alpha}^6$, so in either case α_i is constant on orbits of $\hat{\varepsilon}$ and we may apply Lemma 3.5. We conclude that ε_i is constant on orbits of $\hat{\alpha}$ and commutes with α_i for all i . Since $\alpha_i \in \langle \xi \rangle$ for each i , it follows from Lemma 3.2 that ε_i is a power of ξ whenever α_i is nontrivial.

The two cases now diverge, and we treat each in turn. Suppose first that $\hat{\chi}$ and $\hat{\psi}$ are not powers of $\hat{\alpha}$. Then $\hat{\varepsilon}$ is the identity, and $\hat{\chi}$ and $\hat{\psi}$ must be of orders 3 and 2 respectively, or else they would be powers of $\hat{\alpha}$. Since $\hat{\varepsilon} = 1$ we have $\pi_i(\varepsilon) = \varepsilon_i$ for all i , so by Lemma 3.6 the conjugacy class of ε_i is constant on the orbits of both $\hat{\chi}$ and $\hat{\psi}$.

We claim that in this case $\hat{\chi}$ and $\hat{\psi}$ generate $PSL(2, p)$, so that the conjugacy class of ε_i is in fact constant on $\mathbb{P}^1(\mathbb{F}_p)$. Indeed, this is immediate from Proposition A.5 and Lemma 4.1 when 30 divides n . When 30 does not divide n the group $PSL(2, p)$ is isomorphic to S_3, A_4 or A_5 , and $\langle \hat{\chi}, \hat{\psi} \rangle$ contains elements of orders 2

and 3. Additional, when $p = 5$ it contains an element of order 5, by Lemma 4.1. It is easily seen that in all three cases $\hat{\chi}$ and $\hat{\psi}$ generate $PSL(2, p)$.

Since the conjugacy class of ε_i is constant on $\mathbb{P}^1(\mathbb{F}_p)$, so is the value of $[\varepsilon_i]$. To evaluate this common value we use the abelianisation $\mathcal{H}_p^{q,r} \rightarrow \mathbb{Z}/r\mathbb{Z}$. On one hand we have

$$[[\varepsilon]] = \sum_{k \in \mathbb{P}^1(\mathbb{F}_p)} [\varepsilon_k] = (p+1)[\varepsilon_i],$$

and on the other we have $[[\varepsilon]] = 6[[\alpha]]$, because a generates the abelianisation of T . Since $p+1$ divides $|PSL(2, p)|$, which is co-prime to r , we may divide by $p+1$ mod r to get $[\varepsilon_i] = \frac{6}{p+1}[[\alpha]]$ for all i , as claimed. Statement (5) now follows from this and the last sentence of the first paragraph.

We now turn our attention to the case where $\hat{\chi}$ and $\hat{\psi}$ are powers of $\hat{\alpha}$. In this case ρ maps T into the subgroup $\mathcal{D}_{q,r} \wr \langle \hat{\alpha} \rangle$. If $\sigma_1, \dots, \sigma_m$ are the disjoint cycles of $\hat{\alpha}$, of lengths ℓ_1, \dots, ℓ_m , then this subgroup may be regarded as a subgroup of the direct product

$$\prod_{k=1}^m \mathcal{D}_{q,r} \wr \langle \sigma_k \rangle = \prod_{k=1}^m (\mathcal{D}_{q,r})^{\ell_k} \rtimes \langle \sigma_k \rangle.$$

Moreover, ρ may be regarded as a product of maps ρ_k to each factor. We may therefore consider each disjoint cycle separately. In what follows we will use σ_k to denote both the cycle and the set of points of $\mathbb{P}^1(\mathbb{F}_p)$ moved by this cycle.

Since α_i and ε_i are constant on σ_k , the abelianisation $[[\cdot]] : \mathcal{D}_{q,r} \wr \langle \sigma_k \rangle \rightarrow \mathbb{Z}/r\mathbb{Z}$ gives $[[\varepsilon|_{\sigma_k}]] = \ell_k[\varepsilon_i] = 6[[\alpha|_{\sigma_k}]] = 6\ell_k[\alpha_i]$. Hence $[\varepsilon_i] = 6[\alpha_i]$ on σ_k , because ℓ_k is co-prime to r . If α_i is nontrivial on σ_k then this equality implies

$$\varepsilon_i = \xi^{[\varepsilon_i]} = \xi^{6[\alpha_i]} = \alpha_i^6 = (\alpha^6)_i,$$

where the last equality uses the fact that α is in standard form. However, if $\alpha_i = 1$ on σ_k then we may only conclude at this stage that $\varepsilon_i \in V$, and we will need to work a little harder to show that in fact $\varepsilon_i = 1$.

By way of contradiction, suppose that $\varepsilon_i = v \in V$ on σ_k , and that v is nontrivial. We claim that ρ_k maps T into the subgroup $V \wr \langle \sigma_k \rangle$. To prove this we need only show that the image of x lies in this subgroup, because a and x generate T . To do so we first note that ε is in reduced standard form, because $\ell_i(\varepsilon)$ divides $\ell_i(\hat{\alpha})$ for all i , and $\ell_i(\hat{\alpha})$ is co-prime to qr , by Lemma 4.1. Since ε and χ commute, and ε_i is constant on orbits of $\hat{\chi}$, we may apply Lemma 3.5 to conclude that χ_i commutes with ε_i for all i . On σ_k this means that $\chi_i \in V$ for all i , by Lemma 3.2, and the claim is proved.

It follows that the abelianisation $\|\cdot\| : V \wr \langle \sigma_k \rangle \rightarrow V$ given by summing β_i over σ_k is defined on $\rho_k(T)$. Applying this map we get

$$\|\varepsilon|_{\sigma_k}\| = \ell_k v = 6\|\alpha|_{\sigma_k}\| = 0.$$

Thus v is the identity after all, because ℓ_k is co-prime to q . Consequently $\varepsilon_i = 1 = \alpha_i^6$ on σ_k , and we are done. \square

We refine Lemma 4.4 when $[[\alpha]] = 0$:

Lemma 4.5. *Let $\alpha, \rho, \varepsilon$ and p, q, r be as in Lemma 4.4, and suppose that $[[\alpha]] = 0$ but that $\varepsilon \neq \alpha^6$. If α_i is nontrivial for some i or if $p+1$ is co-prime to q then $\varepsilon = 1$.*

Proof. Since $\varepsilon \neq \alpha^6$, ε is described by statements (1–5) of Lemma 4.4, and $\varepsilon_i \in V$ for all i . If α_i is nontrivial for some i then statements (5), (3) and (1) imply that $\varepsilon = 1$, and we are done. We therefore assume that $\alpha_i = 1$ for all i , but that $\varepsilon \neq 1$.

Since ε_i is constant on orbits of $\hat{\alpha}$ and conjugate to ε_0 for all i , there is $\beta \in \mathcal{H}_p^{q,r}$ such that β_i is constant on orbits of $\hat{\alpha}$, $\beta_i \varepsilon_i \beta_i^{-1} = \varepsilon_0$ for all i , and $\hat{\beta} = 1$. Define $\rho' : T \rightarrow \mathcal{H}_p^{q,r}$ by $\rho'(g) = \beta \rho(g) \beta^{-1}$. Then $\rho'(a) = \alpha$, but $\rho'(x^3) = \varepsilon'$, where $\hat{\varepsilon}' = 1$ and $\varepsilon'_i = \varepsilon_0$ for all i . We now have ε'_i constant on orbits of $\widehat{\rho'(x)}$, and the argument proceeds analogously to the corresponding case in Lemma 4.4 when $\hat{\varepsilon} = \hat{\alpha}^6$. If ε_0 is nontrivial then Lemmas 3.5 and 3.2 show that ρ' maps T into $V \wr PSL(2, p)$, and the abelianisation gives

$$\|\varepsilon'\| = (p+1)\varepsilon_0 = 6\|\alpha\| = 0$$

in V . Thus ε_0 is trivial after all, because $p+1$ is nonzero mod q , and we are done. \square

Since $p \not\equiv -1 \pmod{q}$ when $30 \mid n$, the exceptions to Lemma 4.5 are when $\alpha_i = 1$ for all i and $p = 2, q = 3$; $p = 3, q = 2$; or $p = 5, q = 2$ or 3 . We show that in these cases ε commutes with any n th root η of α . In each case Lemma 4.1 shows that $\hat{\alpha}$ and $\hat{\eta}$ have order p , and it is easily checked that $\hat{\eta}$ must be a power of $\hat{\alpha}$. If $\alpha_i = 1$ for all i then Lemmas 4.3 and 4.4 show that η_i and ε_i belong to V for all i . In addition, ε_i is constant on orbits of $\hat{\eta}$, because these co-incide with the orbits of $\hat{\alpha}$. Therefore

$$(\eta\varepsilon)_i = \eta_i \varepsilon_{i \cdot \hat{\eta}} = \eta_i \varepsilon_i = \varepsilon_i \eta_i = (\varepsilon\eta)_i,$$

and since $\hat{\eta}\hat{\varepsilon} = \hat{\eta} = \hat{\varepsilon}\hat{\eta}$, ε and η commute, as claimed.

4.5. Proof of Theorem 1.1. We now combine the results of the preceding sections and prove Theorem 1.1 in the following form.

Theorem 4.6 (Theorem 1.1, refined). *Let $n \geq 2$ and suppose that p, q and r are chosen as in Section 4.1. Then*

$$|\mathrm{Hom}(G_n(GK), \mathcal{H}_p^{q,r})| < |\mathrm{Hom}(G_n(SK), \mathcal{H}_p^{q,r})|.$$

Proof. Let (ρ, η) be a map-root pair for GK and SK in $\mathcal{H}_p^{q,r}$. As outlined in Section 4.1, we first show that the orbit of (ρ, η) under the action of $\mathcal{C}(\rho(a))$ contains at least as many compatible pairs for SK as it does for GK . In the simplest cases we will do this by showing that a pair is compatible for GK if and only if it is compatible for SK , but in the most important case it will be necessary to consider the group action.

4.5.1. Trivial induced maps to $PSL(2, p)$. Suppose first that $\widehat{\rho(a)} = 1$. Since the conjugacy class of a generates G , this implies that the induced homomorphism $\hat{\rho} : G \rightarrow PSL(2, p)$ is trivial. Thus ρ may be regarded as a homomorphism $G \rightarrow (\mathcal{D}_{q,r})^{r+1}$, and as such is a product of homomorphisms $G \rightarrow \mathcal{D}_{q,r}$. Since r is coprime to 6 we have $\{q, r\} \neq \{2, 3\}$, so by Lemma 3.2 part (4) each map $G \rightarrow \mathcal{D}_{q,r}$ factors through \mathbb{Z} . Consequently, the product $\rho : G \rightarrow (\mathcal{D}_{q,r})^{r+1}$ factors through \mathbb{Z} also. We therefore have $\rho(f) = \rho(c) = \rho(a)$, so $\mathcal{C}(\rho(a))$ fixes (ρ, η) , and additionally $\rho(x^3) = \rho(w^3) = \rho(a^6)$. Since η commutes with $\eta^n = \rho(a)$, it commutes with both $\rho(x^3)$ and $\rho(w^3)$. Thus (ρ, η) is a compatible pair for both GK and SK .

4.5.2. *Nontrivial induced maps to $PSL(2, p)$.* Now suppose that $\widehat{\rho(a)} \neq 1$. Then by Lemma 4.2 there is $\beta \in \mathcal{H}_p^{g,r}$ such that $\alpha = \beta\rho(a)\beta^{-1}$ is an element of \mathcal{A}_p^r in reduced standard form. Since $\mathcal{C}(\alpha) = \beta\mathcal{C}(\rho(a))\beta^{-1}$, and (ρ', η) is compatible for GK or SK if and only if $(\beta\rho'\beta^{-1}, \beta\eta\beta^{-1})$ is, it suffices to prove (I) under the assumption that $\rho(a) = \alpha$. Let $\varepsilon = \rho(x^3)$, $\delta = \rho(w^3)$. Then the compatibility conditions are

$$\varepsilon\delta^{-1}\eta = \eta\varepsilon\delta^{-1} \quad \text{for } SK, \quad \varepsilon\delta\eta = \eta\varepsilon\delta \quad \text{for } GK,$$

and the possible values for ε and δ are described by Lemma 4.4. We consider two cases, according to whether or not at least one of ε , δ equals α^6 .

4.5.3. *Case 1: at least one of ε , δ equals α^6 .* Since this property is preserved by the action of $\mathcal{C}(\alpha)$, we may simply show that such a pair is compatible for GK if and only if it is compatible for SK . But this is immediate from the compatibility conditions, which may be expressed in the form

$$\delta^{\mp 1}\eta\delta^{\pm 1} = \varepsilon^{-1}\eta\varepsilon.$$

At least one of ε and δ commutes with η , so each compatibility condition is satisfied if and only if the other commutes with η also.

4.5.4. *Case 2: $\varepsilon \neq \alpha^6 \neq \delta$.* If $[[\alpha]] = 0$ then Lemma 4.5 and the paragraph that follows it show that both ε and δ commute with η . Thus any such map-root pair is compatible for both GK and SK . In what follows we therefore assume that $[[\alpha]] \neq 0$. By Lemma 4.3 α_i is constant on orbits of $\hat{\eta}$, and we consider separately those cycles of $\hat{\eta}$ on which α_i is nontrivial and those where $\alpha_i = 1$.

Let σ be a cycle of $\hat{\eta}$ on which $\alpha_i \neq 1$, and let i belong to σ . Then $\eta_i \in \langle \xi \rangle$, by Lemma 4.3, and

$$\varepsilon_i = \varepsilon_{i \cdot \hat{\eta}} = \delta_i = \delta_{i \cdot \hat{\eta}} = \xi^{6[[\alpha]]/(p+1)},$$

by Lemma 4.4. Hence

$$(\eta\varepsilon\delta^{\pm 1})_i = \eta_i\varepsilon_{i \cdot \hat{\eta}}\delta_{i \cdot \hat{\eta}}^{\pm 1} = \eta_i\varepsilon_i\delta_i^{\pm 1} = \varepsilon_i\delta_i^{\pm 1}\eta_i = (\varepsilon\delta^{\pm 1}\eta)_i.$$

This shows that such cycles present no obstruction to compatibility for either SK or GK .

Suppose then that σ is a cycle of $\hat{\eta}$ of length ℓ on which $\alpha_i = 1$, and let $d = \gcd(\ell, n)$. The action of $\mathcal{C}(\alpha)$ on (ρ, η) allows us to vary δ but not ε , so we will treat ε as fixed and regard δ as a variable to solve for. If i belongs to σ then compatibility for SK requires

$$\varepsilon_i\delta_i^{-1}\eta_i = \eta_i\varepsilon_{i \cdot \hat{\eta}}\delta_{i \cdot \hat{\eta}}^{-1},$$

so δ_i must satisfy the recurrence relation

$$(4.3) \quad \delta_{i \cdot \hat{\eta}} = \eta_i^{-1}\delta_i\varepsilon_i^{-1}\eta_i\varepsilon_{i \cdot \hat{\eta}}.$$

Given the value of δ_i as an initial condition this has the unique solution

$$(4.4) \quad \delta_{i \cdot \hat{\eta}^m} = \left(\prod_{k=0}^{m-1} \eta_{i \cdot \hat{\eta}^k} \right)^{-1} \delta_i \varepsilon_i^{-1} \left(\prod_{k=0}^{m-1} \eta_{i \cdot \hat{\eta}^k} \right) \varepsilon_{i \cdot \hat{\eta}^m}.$$

Similarly, compatibility for GK requires that δ_i satisfies the recurrence relation

$$(4.5) \quad \delta_{i \cdot \hat{\eta}} = \varepsilon_{i \cdot \hat{\eta}}^{-1}\eta_i^{-1}\varepsilon_i\delta_i\eta_i,$$

which for each initial condition has the unique solution

$$(4.6) \quad \delta_{i \cdot \hat{\eta}^m} = \varepsilon_{i \cdot \hat{\eta}^m}^{-1} \left(\prod_{k=0}^{m-1} \eta_{i \cdot \hat{\eta}^k} \right)^{-1} \varepsilon_i \delta_i \left(\prod_{k=0}^{m-1} \eta_{i \cdot \hat{\eta}^k} \right).$$

We now consider the question of when the solutions (4.4) and (4.6) are well defined on σ . Since i and $i \cdot \hat{\eta}^m$ belong to the same orbit of $\hat{\alpha}$ if and only if $d \mid m$, for (4.4) to be well defined we must have $\delta_{i \cdot \hat{\eta}^d} = \delta_i$, or

$$\delta_i \varepsilon_i^{-1} = \left(\prod_{k=0}^{d-1} \eta_{i \cdot \hat{\eta}^k} \right)^{-1} \delta_i \varepsilon_i^{-1} \left(\prod_{k=0}^{d-1} \eta_{i \cdot \hat{\eta}^k} \right).$$

But the product in parentheses belongs to V , by Lemma 4.3, and likewise $\delta_i \varepsilon_i^{-1} \in V$, by Lemma 4.4, which shows that $[\delta_i \varepsilon_i^{-1}] = 0$. Thus any solution to (4.3) is well defined on σ . However, the corresponding condition for GK is

$$\varepsilon_i \delta_i = \left(\prod_{k=0}^{d-1} \eta_{i \cdot \hat{\eta}^k} \right)^{-1} \varepsilon_i \delta_i \left(\prod_{k=0}^{d-1} \eta_{i \cdot \hat{\eta}^k} \right),$$

and now $\varepsilon_i \delta_i$ has order r : Lemma 4.4 gives $[\varepsilon_i \delta_i] = 12[[\alpha]]/(p+1)$, and this is nonzero because r is co-prime to 6. Thus, by Lemma 3.2 a solution to (4.5) is well defined on σ exactly when the product in parentheses is 1.

We next consider the action of $\mathcal{C}(\alpha)$. If $\beta \in \mathcal{C}(\alpha)$ then $\hat{\beta} = 1$, and by Lemma 3.5 β_i is constant on orbits of $\hat{\alpha}$, and belongs to $\langle \xi \rangle$ whenever $\alpha_i \neq 1$. Conversely, it is easily checked that any such β belongs to $\mathcal{C}(\alpha)$. Thus, when $\alpha_i = 1$, the action of $\mathcal{C}(\alpha)$ allows δ_i to be chosen independently within its conjugacy class $\{h \in \mathcal{D}_{q,r} : [h] = 6[[\alpha]]/(p+1)\}$, subject only to the condition that $\delta_{i \cdot \hat{\alpha}} = \delta_i$. Consequently, every solution to (4.3) or (4.5) within this conjugacy class may be realised by the action of $\mathcal{C}(\alpha)$ on ρ . Since any solution is completely determined by the initial condition δ_i , and (4.4) and (4.6) are both conjugate to δ_i , there are $|V|$ such solutions.

It follows from the above that compatibility of a pair (ρ, η) for which $\varepsilon \neq \alpha^6 \neq \delta$ is completely determined by the values of δ_i on cycles of $\hat{\eta}$ where $\alpha_i = 1$. If there are no such cycles then $\beta \cdot (\rho, \eta)$ is compatible for both SK and GK for all $\beta \in \mathcal{C}(\alpha)$. Otherwise, let c be the number of such cycles, and let t be the number on which the corresponding product $\prod_{k=0}^{d-1} \eta_{i \cdot \hat{\eta}^k}$ is trivial. Then the above discussion shows that there are

$$S(\rho, \eta) = [\text{Stab}_{\mathcal{C}(\alpha)}(\delta) : \text{Stab}_{\mathcal{C}(\alpha)}(\rho)] \cdot |V|^c$$

compatible pairs for SK in the orbit of (ρ, η) , and $S(\rho, \eta)$ compatible pairs for GK if $t = c$, and none otherwise. In each case there are at least as many compatible pairs for SK in the orbit as there are for GK , and we have established statement (I) of Section 4.1.

4.5.5. *Realisation.* We have now shown that

$$|\text{Hom}(G_n(GK), \mathcal{H}_p^{q,r})| \leq |\text{Hom}(G_n(SK), \mathcal{H}_p^{q,r})|.$$

To show that the inequality is strict we exhibit map-root pairs (ρ, η) realising the case above in which no pair in the orbit is compatible for GK .

Define X, Y, A in $SL(2, \mathbb{Z})$ by

$$X = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad A = YX^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

and let $\hat{\chi}, \hat{\psi}, \hat{\alpha}$ be the corresponding projections from $SL(2, \mathbb{Z})$ to $PSL(2, p)$. Then $X^3 = -I = Y^2$, so $x \mapsto \hat{\chi}, y \mapsto \hat{\psi}$ define a homomorphism $T \rightarrow PSL(2, p)$ such that $a \mapsto \hat{\alpha}$. The corresponding fractional linear transformations are $z \mapsto 1/(1-z), z \mapsto -1/z$, and $z \mapsto z+1$, of orders 3, 2 and p respectively.

Define $\chi, \psi \in \mathcal{H}_p^{q,r}$ by $\chi_i = \xi^2$ for all i , and

$$\psi_i = \begin{cases} \xi^4 & \text{if } i = 0, \\ \xi^2 & \text{if } i = \infty, \\ \xi^3 & \text{otherwise.} \end{cases}$$

Then $(\chi^3)_i = \xi^6$ for all i , and likewise $(\psi^2)_i = \xi^6$ for all i , because 0 and ∞ belong to the disjoint cycle $(0 \ \infty)$ of $\hat{\psi}$. Thus $x \mapsto \chi, y \mapsto \psi$ defines a homomorphism $\rho' : T \rightarrow \mathcal{H}_p^{q,r}$, and we extend ρ' to G by defining $\rho'(f) = \rho'(c)$.

Now

$$(\rho'(a))_i = (\psi\chi^{-1})_i = \psi_i(\chi^{-1})_{i \cdot \hat{\psi}} = \psi_i\chi_{i \cdot \hat{\psi}\hat{\chi}^{-1}}^{-1} = \psi_i\chi_{i \cdot \hat{\alpha}}^{-1} = \psi_i\chi_{i+1}^{-1},$$

so

$$\rho'(a) = ((\xi^2, \xi, \dots, \xi, 1), \hat{\alpha}).$$

The cycle-products are $\pi_i(\rho'(a)) = \xi^{p+1}$ for $i \neq \infty$, and $\pi_\infty(\rho'(a)) = 1$. We may therefore conjugate ρ' by a suitably chosen β with $\hat{\beta} = 1$ to get a homomorphism $\rho : G \rightarrow \mathcal{H}_p^{q,r}$ such that

$$\rho(a) = \alpha = ((\xi^{(p+1)/p}, \dots, \xi^{(p+1)/p}, 1), \hat{\alpha})$$

and

$$\rho(x^3) = \rho(w^3) = ((\xi^6, \dots, \xi^6), 1).$$

Since n is co-prime to p it has a multiplicative inverse $k \pmod p$, so by Lemma 4.3

$$\eta_v = ((\xi^{(p+1)/np}, \dots, \xi^{(p+1)/np}, v), \hat{\alpha}^k)$$

is an n th root of α for all $v \in V$. The argument above shows that $\beta \cdot (\rho, \eta_v)$ is a compatible map-root pair for SK for all $\beta \in \mathcal{C}(\alpha)$ and $v \in V$, but is never compatible for GK unless $v = 1$. This completes the proof. \square

APPENDIX A. SOLUTIONS TO $x^3 = y^2$ IN $PSL(2, \mathbb{F}_q)$, BY DAVID SAVITT¹

Let p be a prime and q a power of p .

Theorem A.1. *Suppose $x, y \in PSL(2, \mathbb{F}_q)$ satisfy $x^3 = y^2$. Then either $x^3 = y^2 = 1$, or else there exists $z \in PSL(2, \mathbb{F}_q)$ such that $x = z^2$ and $y = z^3$.*

Proof. First we observe that it suffices to prove the same statement with \mathbb{F}_q replaced throughout by an algebraic closure $\overline{\mathbb{F}}_p$. Indeed, let G be the subgroup generated by x and y . If there exists $z \in PSL(2, \overline{\mathbb{F}}_p)$ such that $z^2 = x$ and $z^3 = y$, then $z = yx^{-1}$ automatically lies in G , hence in $PSL(2, \mathbb{F}_q)$. The advantage of the statement with

¹Department of Mathematics, The University of Arizona, 617 N. Santa Rita Avenue, Tucson AZ 85721, USA. Email: savitt@math.arizona.edu

\mathbb{F}_q replaced by $\overline{\mathbb{F}}_p$ is that its truth is evidently unchanged if one conjugates G (and therefore x, y) by an element of $PSL(2, \overline{\mathbb{F}}_p)$.

We recall the following theorem of Dickson that classifies the finite subgroups of $PSL(2, \overline{\mathbb{F}}_p)$.

Theorem A.2. [3, Secs. 255, 260] *If G is a finite subgroup of $PGL(2, \overline{\mathbb{F}}_p)$, then one of the following holds:*

- (i) G is conjugate to $PGL(2, \mathbb{F}_{p^m})$ or $PSL(2, \mathbb{F}_{p^m})$ for some $m > 0$;
- (ii) G is conjugate to a subgroup of the upper triangular matrices;
- (iii) G is isomorphic to A_4 , S_4 , A_5 , or the dihedral group D_n of order $2n$ for some $n > 1$ not divisible by p .

We proceed case by case.

Case (i). By the first paragraph, we may without loss of generality assume that G is equal to $PSL(2, \mathbb{F}_{p^m})$ or $PGL(2, \mathbb{F}_{p^m})$.

Suppose first that $G = PSL(2, \mathbb{F}_{p^m})$. If $p^m = 2, 3$ we can check the claim directly. If $p^m \geq 4$ then $PSL(2, \mathbb{F}_{p^m})$ is a simple group. But $H = \langle x^3 \rangle = \langle y^2 \rangle$ is clearly a normal subgroup (it is invariant under conjugation by both x and y , which generate G) and it cannot be equal to G . Therefore $x^3 = y^2 = 1$ in this case.

Next suppose $G = PGL(2, \mathbb{F}_{p^m})$. Again if $p^m = 2, 3$ we check the claim directly, while if $p^m > 3$ then the only nontrivial normal subgroup of $PGL(2, \mathbb{F}_{p^m})$ is $PSL(2, \mathbb{F}_{p^m})$ and we can proceed as in the previous paragraph.

Case (ii). By the first paragraph we may assume that x, y are upper triangular. Let X, Y be lifts of x, y to $GL(2, \overline{\mathbb{F}}_p)$, so that $X^3\eta = Y^2$ for a nonzero constant η . Multiplying this equation through by η^2 gives $(\eta X)^3 = (\eta Y)^2$; replacing X, Y by $\eta X, \eta Y$, we may therefore assume that $X^3 = Y^2$.

Let X_{11}, Y_{11} be the upper left entries of X, Y respectively. Since X, Y are upper triangular we see $X_{11}^3 = Y_{11}^2$. Since $\overline{\mathbb{F}}_p^\times$ is a direct limit of cyclic groups, there exists $a \in \overline{\mathbb{F}}_p^\times$ such that $X_{11} = a^2$ and $Y_{11} = a^3$. We may argue similarly for the lower right entries, so that X, Y have the form

$$X = \begin{pmatrix} a^2 & \mu \\ 0 & b^2 \end{pmatrix}, \quad Y = \begin{pmatrix} a^3 & \nu \\ 0 & b^3 \end{pmatrix}.$$

The condition that $X^3 = Y^2$ is now simply the condition that their upper right entries are equal, which one computes to be

$$(A.1) \quad (a^2 + ab + b^2)(a^2 - ab + b^2)\mu = (a + b)(a^2 - ab + b^2)\nu.$$

Observe that

$$a^6 - b^6 = (a - b)(a + b)(a^2 + ab + b^2)(a^2 - ab + b^2).$$

If any of the final three factors on the right vanishes, then $a^6 = b^6$, and moreover the equality (A.1) must become $0 = 0$. Therefore X^3, Y^2 are both scalar and $x^3 = y^2 = 1$.

If none of the final factors on the right vanishes, then we may define

$$\lambda = \frac{\mu}{a + b} = \frac{\nu}{a^2 + ab + b^2}$$

and it is easy to check that

$$X = \begin{pmatrix} a & \lambda \\ 0 & b \end{pmatrix}^2, \quad Y = \begin{pmatrix} a & \lambda \\ 0 & b \end{pmatrix}^3.$$

Hence there exists $Z \in GL(2, \overline{\mathbb{F}}_p)$ such that $X = Z^2$ and $Y = Z^3$, and the same is true for x, y .

Case (iii). We consider each of the groups A_4, S_4, A_5, D_n in turn.

Subcase $G \cong A_4$. The elements of A_4 have the following shape:

g	g^2	g^3
1	1	1
(1 2)(3 4)	1	(1 2)(3 4)
(1 2 3)	(1 3 2)	1

From the table, the only way a square may equal a cube is if both are the identity. Note that if we take x to be any 3-cycle and y to be any (2, 2)-cycle then x, y do indeed generate A_4 .

Subcase $G \cong S_4$. The elements of S_4 have the following shape:

g	g^2	g^3
1	1	1
(1 2)	1	(1 2)
(1 2)(3 4)	1	(1 2)(3 4)
(1 2 3)	(1 3 2)	1
(1 2 3 4)	(1 3)(2 4)	(1 4 3 2)

From the table, if $x^3 = y^2$ then either $x^3 = y^2 = 1$, or else y is a 4-cycle and $x = x^3 = y^2$ is a (2, 2)-cycle. In the latter case we could take $z = y^{-1}$, but in fact the latter case is ruled out as in this case x, y would not generate S_4 . Note that if $x^3 = y^2 = 1$ then x, y generate S_4 if and only if they are simultaneously conjugate to $x = (1 2 3), y = (1 4)$.

Subcase $G \cong A_5$. The elements of A_5 have the following shape:

g	g^2	g^3
1	1	1
(1 2)(3 4)	1	(1 2)(3 4)
(1 2 3)	(1 3 2)	1
(1 2 3 4 5)	(1 3 5 2 4)	(1 4 2 5 3)

From the table, if $x^3 = y^2$ then either $x^3 = y^2 = 1$, or else x, y are both 5-cycles and $x = y^{-1}$. As with S_4 , the latter case is ruled out by hypothesis. Note that if $x^3 = y^2 = 1$ then x, y generate A_5 if and only if they are simultaneously conjugate to $y = (1 2)(3 4), x = (1 3 5)$.

Subcase $G \cong D_n$. Recall that the group D_n has presentation

$$\langle r, s \mid s^2 = r^n = 1, sr = r^{-1}s \rangle.$$

Since x, y generate D_n and $x^3 = y^2$, it is easily checked that $y = sr^\ell$ for some ℓ and $x^3 = y^2 = 1$. Note that in this case x, y generate a group of order 6, so the only possibility for n is $n = 3$. Moreover, S_3 is generated by any element of order 3 together with any element of order 2. \square

Remark A.3. In case (ii) we can actually say somewhat more, namely that as long as $a^2 - ab + b^2 \neq 0$ then we are always in the abelian case (i.e., there exists z such that $x = z^2$ and $y = z^3$). It remains only to check this claim when either $a + b$ or $a^2 + ab + b^2$ is zero. Note that not both can be zero, or else $ab = (a + b)^2 - (a^2 + ab + b^2) = 0$, which is impossible. If, for instance, $a + b = 0$, then $\mu = 0$ in equation (A.1). We may still define $\lambda = \nu/(a^2 + ab + b^2)$ and check that

$$X = \begin{pmatrix} a & \lambda \\ 0 & b \end{pmatrix}^2, \quad Y = \begin{pmatrix} a & \lambda \\ 0 & b \end{pmatrix}^3.$$

The case $a^2 + ab + b^2$ is analogous.

Remark A.4. The final sentence of each subcase of case (iii) shows that whenever one finds S_3, A_4, S_4 , or A_5 as a subgroup of $PSL(2, \mathbb{F}_q)$, it is possible to choose x, y that generate this subgroup and satisfy $x^3 = y^2 = 1$.

Proposition A.5. *Suppose $x, y \in PSL(2, \mathbb{F}_p)$ satisfy $x^3 = y^2$. If there does not exist $z \in PSL(2, \mathbb{F}_p)$ such that $x = z^2$ and $y = z^3$, and if $\text{ord}(yx^{-1}) > 6$, then $\langle x, y \rangle = PSL(2, \mathbb{F}_p)$; in particular this group acts transitively on $\mathbb{P}^1(\mathbb{F}_p)$.*

Proof. By Theorem A.1 we have $x^3 = y^2 = 1$. Let $G = \langle x, y \rangle$. If we are in case (ii) of Dickson's theorem, then by Remark A.3 we have $a^2 - ab + b^2 = 0$. Then a/b is a primitive 6th root of unity (note that the hypotheses of this Proposition imply $p \neq 2, 3$) and the order of yx^{-1} is 6, contrary to hypothesis. Similarly, if we are in any of the subcases of case (iii), then the possible cycle types of x, y are spelled out in the proof of Theorem A.1, and one checks in each case that the order of yx^{-1} is at most 5.

Therefore we are in case (i), and G is conjugate to $PGL(2, \mathbb{F}_{p^m})$ or $PSL(2, \mathbb{F}_{p^m})$. But G is a subgroup of $PSL(2, \mathbb{F}_p)$ and certainly cannot have order larger than the order of $PSL(2, \mathbb{F}_p)$. We conclude that $G = PSL(2, \mathbb{F}_p)$. \square

ACKNOWLEDGEMENT

Christopher Tuffley thanks David Savitt for providing the results on $PSL(2, p)$ in the Appendix, and for other helpful discussions about $PSL(2, p)$.

REFERENCES

- [1] J. H. Conway and C. McA. Gordon, A group to classify knots, *Bull. London Math. Soc.*, **7** (1975) 84–86.
- [2] J. Crisp and L. Paris, Representations of the braid group by automorphisms of groups, invariants of links, and Garside groups, *Pacific J. Math.*, **221** No. 1 (2005) 1–27.
- [3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* (Teubner, Leipzig, 1901).
- [4] R. H. Fox, On the complementary domains of a certain pair of inequivalent knots, *Nederl. Akad. Wetensch. Proc. Ser. A*, **55** = *Indagationes Math.*, **14** (1952) 37–40.
- [5] A. J. Kelly, Groups from link diagrams, Ph. D. Thesis, U. Warwick (1990).

- [6] X.-S. Lin and S. Nelson, On generalized knot groups, *J. Knot Theory Ramifications*, **17** No. 3 (2008) 263–272. E-print arXiv:math.GT/0407050v4.
- [7] S. Nelson and W. D. Neumann, The 2-generalized knot group determines the knot, arXiv:0804.0807 (2008).
- [8] M. Wada, Group invariants of links, *Topology*, **31** No. 2 (1992) 399–406.

INSTITUTE OF FUNDAMENTAL SCIENCES, MASSEY UNIVERSITY, PRIVATE BAG 11 222, PALMERSTON NORTH 4442, NEW ZEALAND
E-mail address: C.Tuffley@massey.ac.nz