MONODROMY GROUPS OF HURWITZ-TYPE PROBLEMS

DANIEL ALLCOCK AND CHRIS HALL

Abstract. We solve the Hurwitz monodromy problem for degree 4 covers. That is, the Hurwitz space $\mathcal{H}_{4,g}$ of all simply branched covers of $\mathbb{P}^1$ of degree 4 and genus g is an unramified cover of the space $\mathcal{P}_{2g+6}$ of $(2g+6)$-tuples of distinct points in $\mathbb{P}^1$. We determine the monodromy of $\pi_1(\mathcal{P}_{2g+6})$ on the points of the fiber. This turns out to be the same problem as the action of $\pi_1(\mathcal{P}_{2g+6})$ on a certain local system of $\mathbb{Z}/2$-vector spaces. We generalize our result by treating the analogous local system with $\mathbb{Z}/N$ coefficients, $3 \nmid N$, in place of $\mathbb{Z}/2$. This in turn allows us to answer a question of Ellenberg concerning families of Galois covers of $\mathbb{P}^1$ with deck group $(\mathbb{Z}/N)^2{:}S_3$.

A ramified cover C of $\mathbb{P}^1$ of degree d is said to have simple branching if the fiber over every branch point has $d-1$ distinct points. Another way to say this is that for each branch point p, the permutation of the sheets of the cover induced by a small loop around p is a transposition, i.e., a permutation of cycle-shape $21\ldots1$. An Euler characteristic argument (or the Hurwitz formula) shows that the number of branch points is $b := 2g + 2d - 2$, where g is the genus of C. Let $\mathcal{H}_{d,g}$ be the Hurwitz space, consisting of all such covers, up to isomorphism as covers. This is an irreducible smooth algebraic variety. There is an obvious map from $\mathcal{H}_{d,g}$ to the space $\mathcal{P}_b$ of unordered b-tuples of distinct points in $\mathbb{P}^1$. This is an unramified cover, so it induces a homomorphism from $G := \pi_1(\mathcal{P}_b)$ to the symmetric group on the points of a fiber. We determine the image in the case $d = 4$; this answers this case of a question posed explicitly in [9] and implicit in earlier work. We call this image G_2; the subscript reflects that this turns out to be the case $N = 2$ of a more general construction considered below.

Our formulation of the problem reflects its topological nature, but usually one thinks of $\mathcal{H}_{d,g}$ and $\mathcal{P}_b$ as irreducible algebraic varieties, so that the function field of $\mathcal{H}_{d,g}$ is a finite extension of that of $\mathcal{P}_b$. Then

---

Date: February 22, 2008.

2000 *Mathematics Subject Classification.* 14D05, 14H30, 20B25, 57M10.

First author partly supported by NSF grant DMS-0600112 and by the Friends of the Institute for Advanced Study.

G_2 is the Galois group of the associated Galois extension. Even the degree of this extension was unknown.

Theorem 1. *Let $g > 1$. Then monodromy group G_2 of $\mathcal{H}_{4,g} \to \mathcal{P}_{b=2g+6}$ fits into the split exact sequence*

$$(1) \qquad 1 \to \prod_{\Omega} \mathrm{PSp}(2g+2, \mathbb{Z}/2) \to G_2 \to \mathrm{PSp}(2g+4, \mathbb{Z}/3) \to 1,$$

where $\Omega = \mathbb{P}^{2g+3}(\mathbb{Z}/3)$ and $\mathrm{PSp}(2g+4, \mathbb{Z}/3)$ permutes the factors of the product in the obvious way.

Remark. The $g = 0, 1$ cases are exceptional. If $g = 0$ then the left term of (1) should be $3^{40}{:}2^{16}$ instead of S_3^{40}, and the sequence is nonsplit. If $g = 1$ then the left term should be $A_6^{364}{:}2^{168}$ rather than S_6^{364}, and we did not determine whether the sequence splits. (We use ATLAS notation for group structures [8].)

The fact that G_2 lies in a group fitting into an exact sequence like (1) is due to Eisenbud, Elkies, Harris and Speiser [9]; see also [7] and [15]. So our result says that G_2 is as large as possible. In section 1 we will review what we need from [9] and then prove the theorem.

In section 2 we treat two generalizations of this that are similar to each other. The degree 4 Hurwitz monodromy problem is very closely related to a certain local system of $\mathbb{Z}/2$-vector spaces over $\mathcal{P}_b$. Namely, $\mathcal{H}_{3,g+1}$ is also an unramified cover of $\mathcal{P}_b$, and over $\mathcal{H}_{3,g+1}$ there is a universal family $\mathcal{C}_{3,g+1}$ of simply branched 3-fold covers of $\mathbb{P}^1$. (Existence of this family is not hard to see, and is proven in great generality in [11].) We write π for the composition $\mathcal{C}_{3,g+1} \to \mathcal{H}_{3,g+1} \to \mathcal{P}_b$. If $N \geq 0$, then we consider the sheaf $\mathcal{V}_N := R^1\pi_*(\mathbb{Z}/N)$ on $\mathcal{P}_b$, which we recall is the sheaf associated to the presheaf $U \mapsto H^1(\pi^{-1}(U); \mathbb{Z}/N)$; the case $N = 0$ corresponds to $\mathbb{Z}$ coefficients. $\mathcal{V}_N$ is a local system of $\mathbb{Z}/N$-modules equipped with symplectic forms; the fiber over a point $p = (p_1, \dots, p_b) \in \mathcal{P}_b$ is $H^1(\pi^{-1}(p), \mathbb{Z}/N)$. This is the direct sum of the $H^1(C; \mathbb{Z}/N)$, where C varies over the points of $\mathcal{H}_{3,g+1}$ lying above p. As we explain in section 1, the monodromy of $\pi_1(\mathcal{P}_b)$ on $\mathcal{V}_2$ is exactly the Hurwitz monodromy group in degree 4, which we called G_2. So we define G_N as the monodromy group on $\mathcal{V}_N$. We have completely determined G_N when $3 \nmid N$, except for the cases $g = 0$ or 1 and the question of whether the exact sequence (2) below splits.

Theorem 2. *Suppose $3 \nmid N$ and $g \geq 0$ ($g > 1$ if N is even). Then the monodromy group G_N of $\mathcal{V}_N$ fits into an exact sequence*

$$(2) \qquad 1 \to \prod_{\Omega} \mathrm{Sp}(2g+2, \mathbb{Z}/N) \to G_N \to \mathrm{PSp}(2g+4, \mathbb{Z}/3) \to 1,$$

where Ω *and the action of* $\mathrm{PSp}(2g+4, \mathbb{Z}/3)$ *are as in theorem 1.*

Question. *What happens if* $3|N$*?* The most extreme case is G_0, the case of integer coefficients, which determines G_N for all N. The congruence subgroup property of $\mathrm{Sp}(2g, \mathbb{Z})$ probably reduces this to the determination of G_{3^n} for all n. But the congruence subgroup property requires $g > 1$, so it would only apply for $b \geq 8$.

Finally, we use theorem 2 to answer a question of Ellenberg [10], which we motivate by reinterpreting the Hurwitz monodromy problem. If $C \to \mathbb{P}^1$ is connected and simply branched of degree 4, then its associated Galois cover has deck group S_4. The Hurwitz monodromy can be regarded as the action of $\pi_1(\mathcal{P}_b)$ on the family of all Galois covers of $\mathbb{P}^1$ that have deck group S_4 and satisfy a condition which is a rephrasing of the simple branching of $C \to \mathbb{P}^1$. What makes the degree 4 case special is that S_4 is solvable: it is a semidirect product $2^2{:}S_3$. Ellenberg essentially asked: what happens when the 2^2 is replaced by an elementary abelian group p^2 for some prime $p > 3$? We show that the resulting monodromy group fits into a split exact sequence like (1), with $\mathbb{Z}/2$ replaced by $\mathbb{Z}/p$.

Here is a precise formulation of his question, in a more general context. Let X_N be the semidirect product $N^2{:}S_3$, with S_3 acting by permuting triples of elements of $\mathbb{Z}/N\mathbb{Z}$ with sum 0. Consider Galois covers of $\mathbb{P}^1$ with Galois group X_N and b branch points, such that the small loops around them correspond to involutions in X_N. When N is even we require further that these involutions have nontrivial image in S_3. Let $\mathcal{E}_N$ be the set of isomorphism classes of such covers; this is a local system of finite sets over $\mathcal{P}_b$, and Ellenberg's question can be phrased: what is the image $\bar{G}_N$ of the monodromy action of $G = \pi_1(\mathcal{P}_b)$ on a fiber of $\mathcal{E}_N$? This type of problem was considered by Biggers and Fried [5], who showed that $\bar{G}_N$ is transitive on the fiber, so $\mathcal{E}_N$ is irreducible. We can go further: for N prime to 3, we have completely determined the structure of $\bar{G}_N$, except for $b = 4$ or 6 when N is even. Theorem 2 fairly easily implies the following theorem:

Theorem 3. *Suppose* $3 \nmid N$ *and* $b > 4$ *(*$b > 8$ *if* N *is even). Then the monodromy group* $\bar{G}_N$ *of* $\mathcal{E}_N \to \mathcal{P}_b$ *fits into the split exact sequence*

$$1 \to \prod_{\Omega} \mathrm{PSp}(b-4, \mathbb{Z}/N) \to \bar{G}_N \to \mathrm{PSp}(b-2, \mathbb{Z}/3) \to 1, \tag{3}$$

where $\Omega = \mathbb{P}^{b-3}(\mathbb{Z}/3)$ *and* $\mathrm{PSp}(b-2, \mathbb{Z}/3)$ *permutes the factors of the product in the obvious way.*

Remarks. The expressions $\mathrm{Sp}(\dots)$ make sense because b always turns out to be even. Also, by $\mathrm{PSp}(b-4,\mathbb{Z}/N)$ we mean the quotient of $\mathrm{Sp}(b-4,\mathbb{Z}/N)$ by its center, which is an elementary abelian 2-group.

The first author is grateful to the University of Michigan, especially Prof. Dolgachev, for organizing support during the fall of 2007, when this project took form, and to the Institute for Advanced Study for its support in spring 2008. The second author is grateful to Jordan Ellenberg for asking the original question which led to this project and for pointing out how one can view it as a generalization of results in [3] and [14].

1. Proof of theorem 1

In this section we will review the relevant results of [9] and then prove theorem 1. The key feature of the $d=4$ case of the Hurwitz monodromy problem is that S_4 is solvable, so that a degree 4 cover $C\to\mathbb{P}^1$ determines a number of related covers of $\mathbb{P}^1$, shown in Figure 1. To organize them we will use subscripts to indicate their degrees over $\mathbb{P}^1$. If $C\to\mathbb{P}^1$ is connected and simply branched of degree 4, with b branch points $p_1,\dots,p_b$, then there is an associated surjection $\pi_1(C-\{p_i\})\to S_4$, well-defined up to conjugacy by an element of S_4, sending small loops around the p_i to transpositions. The corresponding Galois cover C_{24} has S_4 as its deck group, and we define $C_6:=C_{24}/V_4$ and $C_2:=C_{24}/A_4$, where V_4 is Klein's Viergruppe. C itself is C_{24}/S_3 for one of the four conjugate S_3's in S_4, so we could write C_4 for C. We will refer to the covers $C_{24}/D_8\to\mathbb{P}^1$, for the three conjugate D_8's in S_4, as "the 3 C_3's". As explained in [9, sec. 4], C_2 is hyperelliptic, $C_2\to\mathbb{P}^1$ has simple branching over the p_i, and $C_{24}\to C_6$ and $C_6\to C_2$ are unramified with deck groups 2^2 and 3. The genera of C_6 and C_2 are $3g+4$ and $g+2$. Each C_3 is simply branched over $\mathbb{P}^1$, with b branch points and genus $g+1$. These data can be obtained with the Hurwitz formula or by topological picture-drawing like that in Figure 2.

The interplay between these covers allows one to describe the fiber of $\mathcal{H}_{4,g}\to\mathcal{P}_b$ concretely. Each of the C_3's represents the same point of $\mathcal{H}_{3,g+1}$, and C_2 represents a point of $\mathcal{H}_{2,g+2}$, yielding a factorization of $\mathcal{H}_{4,g}\to\mathcal{P}_b$ as $\mathcal{H}_{4,g}\to\mathcal{H}_{3,g+1}\to\mathcal{H}_{2,g+2}=\mathcal{P}_b$. It is usually more convenient to work with Galois covers, so we remark that $C_4,C_4'\in\mathcal{H}_{4,g}$ are equivalent as covers (i.e., are the same point of $\mathcal{H}_{4,g}$) if and only if the Galois covers C_{24} and C_{24}' are. This follows from the conjugacy of index 4 subgroups of S_4. The same argument shows that $C_3,C_3'\in\mathcal{H}_{3,g+1}$ are equivalent if and only if the Galois covers C_6,C_6' are. Because

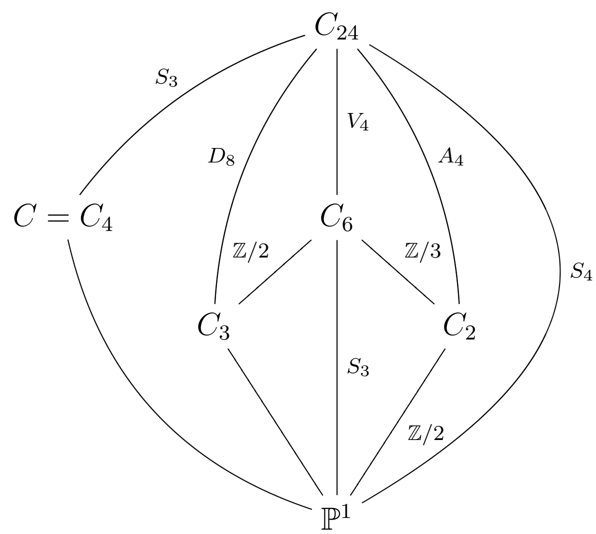

FIGURE 1. Covers associated to a degree 4 cover $C \to \mathbb{P}^1$.

of this, we will sometimes refer to (say) C_6 in order to specify a point of $\mathcal{H}_{3,g+1}$.

Now we describe the fibers of $\mathcal{H}_{2,g+2}$, $\mathcal{H}_{3,g+1}$ and $\mathcal{H}_{4,g}$ over a b-tuple $(p_1, \ldots, p_b) \in \mathcal{P}_b$ in terms of the possibilities for the Galois covers C_2, C_6 and C_{24}. There is only one C_2 with specified branch points $p_1, \ldots, p_b$. The unramified $\mathbb{Z}/3$-covers of C_2 that are Galois over $\mathbb{P}^1$ are in bijection with the hyperplanes h in $H_1(C_2; \mathbb{Z}/3)$ that are preserved by the hyperelliptic involution α of C_2. The condition that the Galois group be S_3 rather than $\mathbb{Z}/6$ is that α act on $H_1(C_2; \mathbb{Z}/3)/h$ by negation. Since α acts by negation on all of $H_1(C_2; \mathbb{Z}/3)$, these conditions on h are vacuous, and the possibilities for C_6 are in bijection with $\mathbb{P}H^1(C_2; \mathbb{Z}/3)$.

Once $C_6 \to \mathbb{P}^1$ is fixed, the possibilities for C_{24} are parameterized in a similar but more complicated way. The unramified covers of C_6 with deck group 2^2 that are Galois over $\mathbb{P}^1$ are in bijection with the codimension-two subspaces L of $H_1(C_6; \mathbb{Z}/2)$ which are preserved by $S_3 = \mathrm{Gal}(C_6/\mathbb{P}^1)$. And the condition for the Galois group to be S_4 rather than some other extension $2^2.S_3$ is that S_3 acts on $H_1(C_6; \mathbb{Z}/2)/L$ in the same way that $S_3 = S_4/V_4$ acts on V_4. Dualizing, the choices for C_{24} correspond to the subgroups $(\mathbb{Z}/2)^2$ of $H^1(C_6; \mathbb{Z}/2)$ which S_3 preserves and acts on by its 2-dimensional irreducible representation, which permutes triples of elements of $\mathbb{Z}/2$ with sum 0. We write $\mathbb{P}V(C_6)$

for this set of subspaces, the notation reflecting the fact that it is a projective space in a non-obvious way.

To see this, fix one of the three C_3's, and regard $H^1(C_3;\mathbb{Z}/2)$ as embedded in $H^1(C_6;\mathbb{Z}/2)$ under pullback. Every one of the 2-dimensional subspaces of $H^1(C_6;\mathbb{Z}/2)$ considered above contains a unique $\mathbb{Z}/2$ lying in $H^1(C_3;\mathbb{Z}/2)$, and every $\mathbb{Z}/2$ in $H^1(C_3;\mathbb{Z}/2)$ lies in a unique one of these 2-dimensional subspaces. So $\mathbb{P}V(C_6)$ is in bijection with $\mathbb{P}H^1(C_3;\mathbb{Z}/2)$. The three C_3's all give the same projective space structure, so the choices for C_{24}, given C_6, correspond to points of $\mathbb{P}V(C_6) \cong \mathbb{P}^{2g+1}(\mathbb{Z}/2)$. We can even be a little fancier and define $V(C_6)$ as the union of the three $H^1(C_3;\mathbb{Z}/2)$'s, modulo identification under the group $\mathbb{Z}/3$ of deck transformations. Then $\mathbb{P}V(C_6)$ is indeed the projectivization of $V(C_6)$.

In summary, once $p_1,\ldots,p_b$ are fixed, the possibilities for $C = C_4$ are in bijection with the ordered pairs (C_6, C_{24}), where C_6 corresponds to an element of $\mathbb{P}H^1(C_2;\mathbb{Z}/3)$ and C_{24} to an element of $\mathbb{P}V(C_6)$. All of these constructions can be carried out simultaneously for all b-tuples (this is the basic property of Hurwitz spaces). The result is that $\mathcal{H}_{4,g}$ is an unramified cover of $\mathcal{P}_b$, which factors as $\mathcal{H}_{4,g} \to \mathcal{H}_{3,g+1} \to \mathcal{P}_b$, with a fiber of the second map parameterizing the possible choices for C_6 (or equivalently C_3). The fiber of the first map over a chosen C_6 is $\mathbb{P}V(C_6) \cong \mathbb{P}^{2g+1}(\mathbb{Z}/2)$, parameterizing the possible choices for C_{24}, given C_6. So a fiber of $\mathcal{H}_{4,g}$ over $\mathcal{P}_b$ consists of $|\mathbb{P}^{2g+3}(\mathbb{Z}/3)|$ many copies of $\mathbb{P}^{2g+1}(\mathbb{Z}/2)$.

We are interested in the monodromy action of $G := \pi_1(\mathcal{P}_b)$ on this fiber. It obviously respects the symplectic structure on $H^1(C_2;\mathbb{Z}/3)$, and the stabilizer of C_6 preserves the symplectic structure on $V(C_6) = H^1(C_3;\mathbb{Z}/2)$. Therefore the image G_2 can be no larger than in (1).

Having reviewed the results of [9], we will now prove the theorem. We will write $\beta_1,\ldots,\beta_{b-1}$ for the standard generators for the spherical braid group on b strands, which is G.

Lemma 4. *The monodromy action of any β_i on a fiber $\mathbb{P}H^1(C_2;\mathbb{Z}/3)$ of $\mathcal{H}_{3,g+1} \to \mathcal{P}_b$ is a symplectic transvection, and G acts by the full projective symplectic group* $\mathrm{PSp}(2g+4,\mathbb{Z}/3)$.

Proof. This is due to Cohen [7]; the key point is the following. Let L be a simple loop in $\mathbb{P}^1$ encircling p_i and p_{i+1} but none of the other branch points. Then L lifts to a closed loop $\tilde{L}$ on C_2. The monodromy of β_i on C_2 is a Dehn twist in $\tilde{L}$. (For a visual proof see figs. 5–7 of [4, ch. 1] and the surrounding text.) This acts on cohomology by a transvection.

For the second statement we appeal to Clebsch's theorem [6, pp. 224–225] that G is transitive on the sheets of $\mathcal{H}_{3,g+1} \to \mathcal{P}_b$, which is to

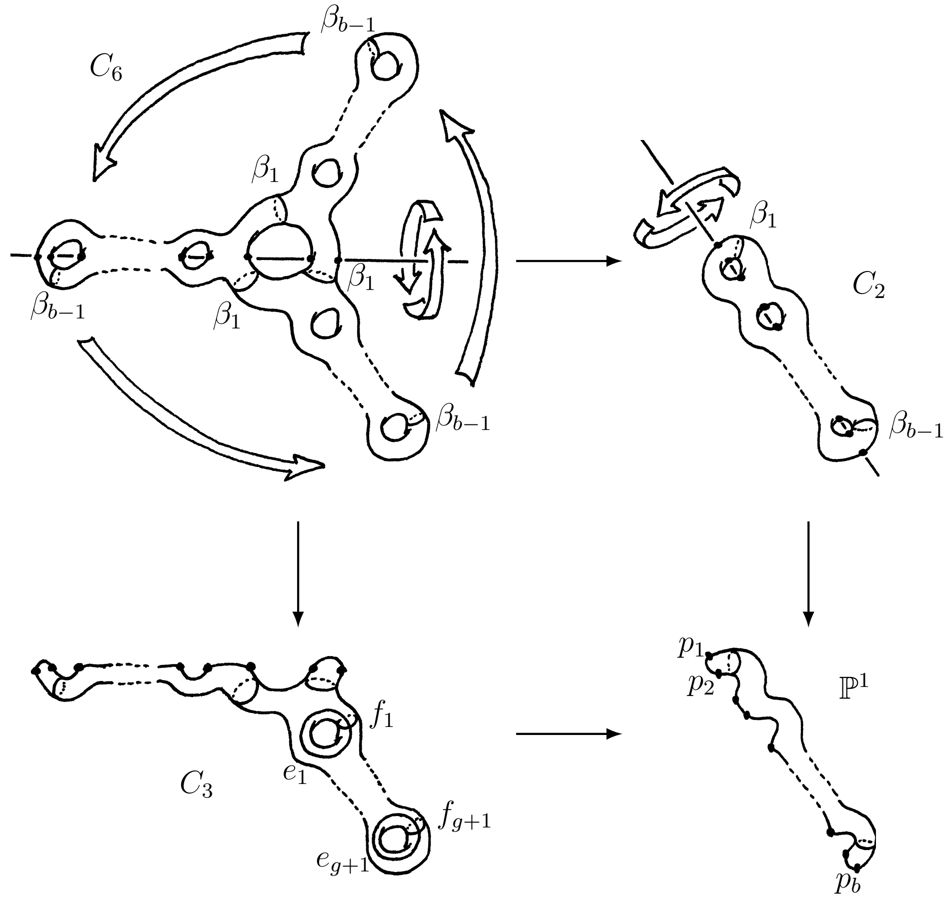

FIGURE 2. Covers of $\mathbb{P}^1$ associated to $C \to \mathbb{P}^1$.

say that it is transitive on $\mathbb{P}H^1(C_2; \mathbb{Z}/3)$. The G-conjugates of the β_i therefore give all the transvections, which are well-known to generate the symplectic group. □

Now pick a point of $\mathcal{H}_{3,g+1}$; this corresponds to a cover C_6 (equivalently, C_3) and also to an element of $\mathbb{P}H^1(C_2; \mathbb{Z}/3)$, say the one in which β_1 acts by a transvection. We will abbreviate $V(C_6)$ to V. Now we consider the subgroup H of G whose monodromy sends C_6 to itself, and the action of H on the fiber $\mathbb{P}V$ of $\mathcal{H}_{4,g}$ over C_6.

Lemma 5. *H contains β_1, which acts trivially on V, and $\beta_3, \dots, \beta_{b-1}$, which act by symplectic transvections. And H acts on V by the full projective symplectic group* $\mathrm{PSp}(V) \cong \mathrm{Sp}(2g+2, \mathbb{Z}/2)$.

Proof. Before beginning the proof proper we make V concrete. Figure 2 shows the maps $C_6 \to C_3 \to \mathbb{P}^1$ and $C_6 \to C_2 \to \mathbb{P}^1$. The picture of

$\mathbb{P}^1$ shows the branch points $p_1, \ldots, p_b$. The loop encircling p_1 and p_2 has a lift to C_2, marked β_1. We use this notation because β_1 acts on C_2 as a Dehn twist in that loop, which was called $\tilde{L}$ in the proof of lemma 4. Now, C_6 is defined as the cover of C_2 corresponding to the elements of $\pi_1(C_2)$ having trivial intersection (mod 3) with $\tilde{L}$, and is shown. The deck group acts by the obvious $\mathbb{Z}/3$ rotation. Next, there are 3 involutions in $S_3 = \mathrm{Gal}(C_6/\mathbb{P}^1)$, one of which is the $\mathbb{Z}/2$ rotation around the horizontal axis. The quotient C_3 is shown, together with the branch points of $C_6 \to C_3$ and a basis $e_1, f_1, \ldots, e_{g+1}, f_{g+1}$ of $H^1(C_3)$. If we indicate lifts of these loops to the 3 'arms' of C_6 by $e_j^{(i)}$ and $f_j^{(i)}$, for $i = 0, 1, 2$ and $j = 1, \ldots, g+1$, then up to relabeling, the pullback V^{01} of $H^1(C_3)$ is spanned by the $e_j^{(0)} + e_j^{(1)}$ and $f_j^{(0)} + f_j^{(1)}$. The other two C_3's give the same result but with different superscripts. The space V is the union of these three vector spaces, modulo cyclic permutation of the upper labels 0, 1 and 2.

Now, β_1 lies in H, so it lifts to C_6; "the" action on C_6 is only well-defined up to composition with deck transformations. But these act trivially on V, by the definition of V, so the action of β_1 on V may be computed from any one of the three lifts of β_1. One of these lifts is the composition of the Dehn twists in the three loops marked β_1. This obviously leaves the $e_j^{(i)}$ and $f_j^{(i)}$ unperturbed, so β_1 acts trivially on V.

The same analysis applies to β_{b-1}, one of whose lifts to C_6 is the composition of the three indicated Dehn twists. Its restriction to V^{01} is the transvection in $f_{g+1}^{(0)} + f_{g+1}^{(1)}$ (with respect to the symplectic form pulled back from C_3, not the one on $H^1(C_6)$). This proves that β_{b-1} acts on V as a transvection. The argument is the same for $\beta_3, \ldots, \beta_{b-2}$.

We remark that up to this point, the argument works perfectly well with $\mathbb{Z}$ coefficients in place of $\mathbb{Z}/2$.

Finally, we again use Clebsch's transitivity theorem, this time applied to the fibers of $\mathcal{H}_{4,g} \to \mathcal{P}_b$, to deduce that H acts transitively on the fiber of $\mathcal{H}_{4,g}$ over the point of $\mathcal{H}_{3,g+1}$ corresponding to C_6. This fiber is $\mathbb{P}V$. Since the image of H contains a transvection and is transitive on $\mathbb{P}V$, it contains all transvections, hence equals $\mathrm{PSp}(V)$. □

Now we will consider the kernel K of $G \to \mathrm{PSp}(2g+4, \mathbb{Z}/3)$ and its image K_2 in G_2, which is a subgroup of the direct product appearing in (1). We will improve the previous lemma by showing that K has the same surjectivity properties we just established for H; then we will show that this is a fierce restriction on K_2.

Lemma 6. *The projection of K_2 to any factor of $\prod_\Omega \mathrm{PSp}(2g+2,\mathbb{Z}/2)$ is surjective.*

Proof. Because G permutes the factors transitively, it suffices to treat any one, say $\mathrm{PSp}(V)$. Now, K is normal in H, and H surjects to $\mathrm{PSp}(V)$, so the image of K is a normal subgroup of $\mathrm{PSp}(V)$. It also contains the transvection β_{b-1}^3. Therefore it contains all transvections, hence all of $\mathrm{PSp}(V)$. □

If S is a group, then we call a subgroup of a product of copies of S diagonally embedded if it projects isomorphically to each factor. The language expresses the fact that it is *the* diagonal subgroup, up to automorphisms of the factors.

Lemma 7. *Let S be a nonabelian simple group, Ω a finite set, and K_2 a subgroup of $\prod_\Omega S$ that surjects to each factor. Then $K_2 \cong S^n$ for some n, and there is a partition $\Omega = \Omega_1 \coprod \cdots \coprod \Omega_n$, such that the ith factor of K_2 is diagonally embedded in $\prod_{\Omega_i} S$, for each i.*

Proof. We first remark that a product of copies of a nonabelian simple group is a product in only one way, since the factors are the normal simple subgroups. We will also use the following standard fact [17, ch. 2, thm. 4.19]: if A, A' are groups, then the subgroups J of $A \times A'$ are in bijection with the 5-tuples (B, B', C, C', ϕ) where B and B' are subgroups of A and A', C and C' are normal subgroups of B and B', and ϕ is an isomorphism $B/C \cong B'/C'$. (B and B' are the projections of J to A and A', C and C' are the intersections of J with the factors, and J is the preimage of the graph of ϕ under $B \times B' \to B/C \times B'/C'$.)

The proof is by induction on $|\Omega|$, the case of a singleton being trivial. So suppose $|\Omega| > 1$, choose a point $\omega \in \Omega$, and define $\Omega' := \Omega - \{\omega\}$. We apply the above with $A = \prod_{\{\omega\}} S \cong S$, $A' = \prod_{\Omega'} S$ and $J = K_2 \subseteq A \times A'$. By the assumed surjectivity, B surjects to A, and B' surjects to each factor of $\prod_{\Omega'} S$. By induction, $B' \cong S^m$ for some m, and there is a partition $\Omega' = \Omega'_1 \coprod \cdots \coprod \Omega'_m$ such that the ith factor of B' is diagonally embedded in $\prod_{\Omega'_i} S$. Now, because $B \cong S$ is simple, C is either all of B or is trivial. In the first case, $B'/C' \cong B/C = 1$, so $C' = B'$ also. Then $K_2 = B \times B' \cong S^{m+1}$, with its ith factor diagonally embedded in $\prod_{\Omega_i} S$, where $\Omega_1 = \Omega'_1, \ldots, \Omega_m = \Omega'_m$, $\Omega_{m+1} = \{\omega\}$.

In the second case, $B'/C' \cong B/C \cong S$, so $K_2 \subseteq B' \times B = S^m \times S$ is the graph of a surjection $B' \to B$. Because S is nonabelian simple, any normal subgroup of S^m is the product of some of the given factors. Therefore the kernel of $B' \to B$ consists of $m-1$ factors of S^m, say all but the first. We conclude that $K_2 \subseteq B' \times B$ is generated by a diagonally embedded copy of S in each of $\prod_{\Omega'_2} S, \ldots, \prod_{\Omega'_m} S$, together with the graph of an isomorphism from a diagonally embedded copy of S in $\prod_{\Omega_1'} S$ to $B = \prod_{\{\omega\}} S \cong S$. It follows that $K_2 \cong S^m$, with its ith factor diagonally embedded in $\prod_{\Omega_i} S$, where $\Omega_1 = \Omega_1' \cup \{\omega\}$ and $\Omega_2 = \Omega_2', \ldots, \Omega_m = \Omega_m'$. □

Proof of theorem 1: We will write S for $\mathrm{PSp}(2g+2, \mathbb{Z}/2)$. We know by lemma 4 that G_2 surjects to $\mathrm{PSp}(2g+4, \mathbb{Z}/3)$, so to establish the exact sequence it suffices to show that K_2 is the full direct product $\prod_\Omega S$. Since $g > 1$, S is simple. It follows from lemmas 6 and 7 that there is a partition $\Omega = \Omega_1 \coprod \cdots \coprod \Omega_n$ such that $K_2 \cong S^n$, its ith factor being diagonally embedded in $\prod_{\Omega_i} S$. Now, G's action on K_2 permutes the factors of K_2, in a manner compatible with G's action on Ω. Therefore G respects the partition. But $\mathrm{PSp}(2g+4, \mathbb{Z}/3)$ acts primitively on Ω, so either all the Ω_i are singletons or else there is only one Ω_i. In the first case we have $K_2 = \prod_\Omega S$, as desired. So we must rule out the case where K_2 is isomorphic to S and is diagonally embedded in $\prod_\Omega S$. We will do this by exhibiting a nontrivial element of K_2 with trivial projection to one factor. By lemma 5, β_1^3 acts trivially on V. On the other hand, β_1^3 is G-conjugate to β_{b-1}^3, whose image in $\mathrm{PSp}(V)$ is nontrivial, by the same lemma.

Finally, we show that the sequence (1) splits. Because K_2 has no center, a standard result [17, ch. 2, thm. 7.11] shows that the structure of G_2 is determined by the homomorphism $G_2/K_2 \to \mathrm{Out}(K_2)$. Since S is a nonabelian simple group with trivial outer automorphism group, $\mathrm{Out}(K_2) = \mathrm{Sym}(\Omega)$. Also, the homomorphism $\mathrm{PSp}(2g+4, \mathbb{Z}/3) \to \mathrm{Sym}(\Omega)$ is the permutation action on Ω. Since there is exists a split extension giving this homomorphism, and the homomorphism determines G_2, G_2 must split. □

In the cases $g = 0, 1$, lemma 7 no longer applies because the groups $\mathrm{PSp}(2, \mathbb{Z}/2) \cong S_3$ and $\mathrm{PSp}(4, \mathbb{Z}/2) \cong S_6$ are not simple; they are extensions of $\mathbb{Z}/2$ by the simple group $S' = [S, S]$. One can describe the permutation representation of $\pi_1(\mathcal{P}_b)$ on the fiber f $\mathcal{H}_{4,g} \to \mathcal{P}_b$ in a manner suitable for computer calculation, and for $g = 0$ we discovered $|G_2| = 3^{40}.2^{16}|\mathrm{PSp}(4, \mathbb{Z}/3)|$, so $K_2 = 3^{40}.2^{16} \subseteq S_3^{40}$. For $g = 1$ the calculation exceeded our available computing power, so we proceeded as follows. An argument as in the proof of theorem 1 shows that $K_2' := K_2 \cap \prod_\Omega S'$ is either the full direct product $\prod_\Omega S'$ or is isomorphic to S' and is diagonally embedded in $\prod_\Omega S'$. (K_2' turns out to be the commutator subgroup of K_2, justifying the notation. This also holds in the $g = 0$ case.) A computer-aided calculation shows that K_2' is the full direct product $\prod_\Omega S'$. The crucial step is an analogue of lemma 6 for K_2'. Namely, while β_i^3 lies in K_2, it does not lie in K_2' because transvections lie outside S'. Nonetheless, an explicit calculation shows that $[\beta_1^3, \beta_2^3]$ is a non-trivial element of K_2' which projects trivially to at least one factor S', hence $K_2' = \prod_\Omega S'$.

As described below, we wrote down an explicit faithful permutation representation of G_2/K_2', which was within reach of computer calculation. We found that G_2/K_2' is $2^{16}.\mathrm{PSp}(4, \mathbb{Z}/3)$ for $g = 0$ and $2^{168}.\mathrm{PSp}(6, \mathbb{Z}/3)$ for $g = 1$. Although we already knew this when $g = 0$, in this representation we could show that extension is not split, which was out of reach before killing K_2'. We did not apply sufficient computing power to determine whether or not it splits for $g = 1$. We carried out our computer calculations using GAP [12].

To describe our representation of G_2/K_2' we recall from [9, Section 1] the (faithful) permutation representation of G_2 on the collection Σ of S_4-orbits of b-tuples $(\sigma_1, \ldots, \sigma_b)$ of 2-cycles in S_4 such that $\sigma_1 \cdots \sigma_b = 1$ and $\langle \sigma_1, \ldots, \sigma_b \rangle = S_4$. Here, β_i acts by replacing σ_i by σ_{i+1} and σ_{i+1} by $\sigma_{i+1}^{-1} \sigma_i \sigma_{i+1}$ and leaving all other σ_j invariant, and S_4 acts by simultaneous conjugation on all elements of a b-tuple.

In a similar fashion we may identify Ω with the S_3-orbits of b-tuples of 2-cycles in S_3 so that if we fix an isomorphism $S_3 \cong S_4/V_4$, then the induced map $\Sigma \to \Omega$ is G_2-equivariant. If we fix $\omega \in \Omega$ to be the point corresponding to C_6 and write Σ_ω for the fiber over ω, then we may identify Σ_ω with $\mathbb{P}V$ and $S = \mathrm{PSp}(V)$ with the factor of $\prod_\Omega S$ over ω.

If we write H_2 for the stabilizer in G_2 of ω, then the representation $G_2 \to \mathrm{Sym}(\Omega)$ is equivalent to the left representation of G_2 on G_2/H_2. Moreover, if we write H_2^* for the kernel of the composite map $H_2 \to S \to \mathbb{Z}/2$, then K_2' is the intersection of all G_2-conjugates of H_2^* and hence is the kernel of the left representation of G_2 on $\Omega' = G_2/H_2^*$. In particular, given a set of coset representatives of G_2/H_2^* and a black box for identifying when two elements of G_2 lie in the same coset, it is easy to compute the representation $G_2 \to \mathrm{Sym}(\Omega')$: β_i takes the coset $\alpha_j H_2^*$ to the coset $\beta_i \alpha_j H_2^*$.

To construct representatives one takes a known subset $\alpha_1, \ldots, \alpha_m$, computes $\beta_i \alpha_j H_2^*$ for $i = 1, \ldots, b-1$ and $j = 1, \ldots, m$, adds any new cosets which arise to the known subset, and repeats until no new cosets are constructed.

To construct the black box observe that the elements γ_1, γ_2 represent the same coset if and only if $\gamma = \gamma_1^{-1}\gamma_2$ lies in H_2^*, and the latter occurs if and only if γ both stabilizes ω and lies in the kernel of $H_2 \to \mathbb{Z}/2$. Using the representation $G_2 \to \mathrm{Sym}(\Omega)$ one can compute whether γ stabilizes ω and if it does one can compute the parity of the image of

γ in $\mathrm{Sym}(\Sigma_\omega)$. This completes the construction of the faithful permutation representation of G_2/K_2'.

2. Proof of theorems 2 and 3

We first introduce a little notation for talking about $\mathcal{V}_N$. Choosing a point of $\mathcal{H}_{3,g+1}$ means choosing a simply branched cover $C_3 \to \mathbb{P}^1$, or equivalently the associated Galois cover $C_6 \to \mathbb{P}^1$. We define $V_N(C_6)$ to be $H^1(C_3; \mathbb{Z}/N)$, or more intrinsically as the union of the pullbacks to $H^1(C_6; \mathbb{Z}/N)$ of the three $H^1(C_3; \mathbb{Z}/N)$'s, modulo identifications by the action of $\mathbb{Z}/3$. For fixed $(p_1, \ldots, p_b) \in \mathcal{P}_b$, the fiber of $\mathcal{V}_N$ is $\oplus_{C_3} V_N(C_6)$, where the sum extends over the points $C_3 \in \mathcal{H}_{3,g+1}$ lying above $(p_1, \ldots, p_b)$. When $N = 2$, $V_2(C_6)$ is just $V(C_6)$ from section 1, giving the relation to the Hurwitz monodromy problem.

Now we can discuss the monodromy. The map $G \to \mathrm{PSp}(2g+4, \mathbb{Z}/3)$ is the same as in the previous section, corresponding to the action on $\Omega = \mathbb{P}H^1(C_2; \mathbb{Z}/3)$. As before, we write K for the kernel, which acts on $\mathcal{V}_N$ by a subgroup of $P_N := \prod_\Omega \mathrm{Sp}(2g+2, \mathbb{Z}/N)$. Also, we saw in lemma 4 that β_1 acts on $H^1(C_2; \mathbb{Z}/3)$ as a transvection, so it distinguishes an element of Ω. We write H for the G-stabilizer of this point, C_6 for the corresponding S_3-cover of $\mathbb{P}^1$, and V_N for $V_N(C_6) \cong (\mathbb{Z}/N)^{2g+2}$.

Lemma 8. *If $g \geq 0$ and $N \geq 0$, then H acts on V_N as $\mathrm{Sp}(V_N)$.*

Proof. It suffices to prove this in the case $N = 0$, i.e., with $\mathbb{Z}$ coefficients. A'Campo [2, Thm. 1(2)] studied a particular representation of the braid group $B_{\mu+1}$, μ even, into $\mathrm{Sp}(\mu, \mathbb{Z})$. We have a representation of $B_{b-2} = \langle \beta_3, \ldots, \beta_{b-1} \rangle \subseteq H$ into $\mathrm{Sp}(2g+2, \mathbb{Z})$. (Recall that $b = 2g+6$.) In both cases the braid generators act by transvections in primitive lattice vectors (this uses lemma 5, whose proof goes through perfectly well over $\mathbb{Z}$). These representations are essentially unique, since the transvections in two nonproportional vectors braid if and only if pairing the vectors yields ± 1. Therefore our representation contains his, with $\mu = 2g+2$, and we even have an extra generator. He proves that the image of his representation contains the level 2 congruence subgroup of $\mathrm{Sp}(2g+2, \mathbb{Z})$ so the image of ours does too. (One can show that our extra generator doesn't enlarge the image of the representation.)

Since the image of H contains the level 2 congruence subgroup of $\mathrm{Sp}(2g+2, \mathbb{Z})$, all we have to show is that H surjects to $\mathrm{Sp}(2g+2, \mathbb{Z}/2)$. We did this in lemma 6. □

Lemma 9. *If $g \geq 0$ and $3 \nmid N$, then the projection of K to any factor of $P_N = \prod_\Omega \mathrm{Sp}(2g+2, \mathbb{Z}/N)$ is surjective.*

Proof. Follow the proof of lemma 6; the only modification needed is that depending on one's definition of a transvection, β_{b-1}^3 might not be one. But regardless of this choice of definition, the cyclic group β_{b-1}^3 generates does contain a transvection. □

Proof of theorem 2: It suffices to prove that K surjects to P_N, and by the Chinese remainder theorem it suffices to treat the case where N is a prime power p^n. First we treat the case $N = p$. Under our hypothesis on g, $\mathrm{PSp}(2g+2, \mathbb{Z}/p)$ is a nonabelian simple group. Then the argument for theorem 1 implies that K surjects to the central quotient $\prod_\Omega \mathrm{PSp}(2g+2, \mathbb{Z}/p)$ of P_p. Since $\mathrm{Sp}(2g+2, \mathbb{Z}/p)$ is a nonsplit extension of $\mathrm{PSp}(2g+2, \mathbb{Z}/p)$, K surjects to P_p.

Now we suppose $N = p^n$ for $n > 1$. We write Γ for the level p^{n-1} congruence subgroup of $\mathrm{Sp}(2g+2, \mathbb{Z}/p^n)$ and assume inductively that K surjects to $P_{p^{n-1}}$. So we must show that $G_N \cap \prod_\Omega \Gamma$ is all of $\prod_\Omega \Gamma$. Now, Γ is an elementary abelian p-group, and the action of $\mathrm{Sp}(2g+2, \mathbb{Z}/p^n)$ on it factors through $\mathrm{Sp}(2g+2, \mathbb{Z}/p)$, whose action on Γ is equivalent to the adjoint action on $\mathfrak{sp}(2g+2, \mathbb{Z}/p)$. First we suppose $p > 2$, so that this action is irreducible. Observe that the action of P_p on $\prod_\Omega \Gamma$ is by the direct sum of $|\Omega|$ many distinct irreducible representations of P_p. Since G_N surjects to P_p, $G_N \cap \prod_\Omega \Gamma$ is an invariant subspace, so it is the product of some of the factors of $\prod_\Omega \Gamma$. It also surjects to each factor, by lemma 9, so it must be the product of all of them. This finishes the proof for $p \neq 2$.

The same argument works for $p = 2$, even though Γ is no longer irreducible under $\mathrm{Sp}(2g+2, \mathbb{Z}/2)$. The scalar matrix $1 + 2^{n-1}$ in $\Gamma \cong \mathfrak{sp}(2g+2, \mathbb{Z}/2)$ is invariant, the quotient by the span of this vector is irreducible, and there is no invariant complement. This last property is key, because it implies that the only P_p-invariant subspace of $\prod_\Omega \Gamma$ that projects onto each factor is the whole product. So the argument still applies. □

Now we explain the application of theorem 2 to Ellenberg's question. As in the previous section, we will indicate degrees of covers of $\mathbb{P}^1$ by subscripts. Suppose $3 \nmid N$ and $C_{6N^2} \in \mathcal{E}_N$, i.e., C_{6N^2} is a Galois cover of $\mathbb{P}^1$ with Galois group $X_N = N^2{:}S_3$ and b branch points, and the small loops around them permute the sheets by involutions in X_N with nontrivial image in S_3. Then b must be even because the product of the b loops in $\mathbb{Z}/2 = S_3/3$ must be trivial. Analogously to section 1, we define C_6 as C_{6N^2}/N^2, C_2 as $C_6/3$ and the three C_3's as the quotients of C_6 by the 3 involutions in S_3. These are exactly the same covers we met in section 1 and they fit into a diagram similar to Figure 1.

We define the projectivization $\mathbb{P}V_N(C_6)$ as the set of direct summands $\mathbb{Z}/N$ of $V_N(C_6)$. The arguments of section 1, with $\mathbb{Z}/N$ in place of $\mathbb{Z}/2$, imply that C_{6N^2} corresponds to an element of $\mathbb{P}V_N(C_6)$, and that the fiber of $\mathcal{E}_N \to \mathcal{P}_b$ over $p \in \mathcal{P}_b$ is in bijection with the set of pairs (C_6, C_{6N^2}), where C_6 corresponds to an element of $\Omega = \mathbb{P}H^1(C_2; \mathbb{Z}/3) \cong \mathbb{P}^{b-3}(\mathbb{Z}/3)$ and C_{6N^2} to an element of $\mathbb{P}V_N(C_6)$. That is, the fiber is $\coprod_\Omega \mathbb{P}^{b-5}(\mathbb{Z}/N)$. It is clear that the action of G on this set is determined by its action on $\oplus_\Omega V(C_6)$, which is exactly the fiber of $\mathcal{V}_N$. Indeed, the action is given by projectivizing the action on each summand, so the monodromy group $\bar{G}_N$ is got from (2) by replacing Sp by PSp.

Proof of theorem 3: We have already explained why $\bar{G}_N$ is the quotient of G_N by the center of $K_N = \prod_\Omega \mathrm{Sp}(b-4, \mathbb{Z}/N)$, so all we have to do is show that the sequence splits. By the Chinese remainder theorem, it suffices to treat the case with N a prime power p^n. We appeal to a theorem of Gross and Kovács [13, Cor. 4.4] which describes the structure of extensions like (3) in terms of the stabilizer of one factor of the product. We fix $\omega \in \Omega$ and let $\bar{H}_N \subseteq \bar{G}_N$ be its stabilizer. Their result asserts that (3) splits if and only if

$$1 \to \prod_{\omega' \in \Omega} S \Big/ \prod_{\omega' \neq \omega} S \to \bar{H}_N \Big/ \prod_{\omega' \neq \omega} S \to \bar{H}_N \Big/ \prod_{\omega' \in \Omega} S \to 1,$$

does, where $S = \mathrm{PSp}(b-4, \mathbb{Z}/p^n)$. This sequence has the form

$$1 \to \mathrm{PSp}(b-4, \mathbb{Z}/p^n) \to\ ?\ \to 3{\cdot}3^{b-4}{:}\mathrm{Sp}(b-4, \mathbb{Z}/3) \to 1,$$

the right term being a maximal parabolic subgroup of $\mathrm{PSp}(b-2, \mathbb{Z}/3)$. Since the left term is centerless, the structure of the extension is given by the natural homomorphism from the right term to $\mathrm{Out}(S)$, which is solvable. Since the right term is perfect, this map is trivial, so the sequence splits, so (3) does too.

($\mathrm{Out}(S)$ is known exactly, cf. [16] for the case $b \geq 10$ and [1] for the case $b \geq 6$ with N odd. But it is much easier to see solvability than to work the group out exactly.) □

Remark. Since we know $\bar{G}_N$, we recover the result of Biggers and Fried [5] that G is transitive on the fiber of $\mathcal{E}_N \to \mathcal{P}_b$, which is the same as the irreducibility of $\mathcal{E}_N$. On the other hand, when $N \neq 0$ one could use their result to prove an analogue of lemma 8 without relying on A'Campo's theorem. Namely, H acts on $\mathbb{P}V$ as $\mathrm{PSp}(V_N)$; one mimics the proof of lemma 5, using their transitivity result in place of Clebsch's. One can then use this to prove lemma 8 itself (for $N \neq 0$).

References

[1] E. Abe, "Automorphisms of Chevalley groups over commutative rings," (Russian), *Algebra i Analiz* **5** (1993), no. 2, 74–90; translation in *St. Petersburg Math. J.* **5** (1994), no. 2, 287–300.

[2] N. A'Campo, "Tresses, monodromie et le groupe symplectique," *Comment. Math. Helv.* **54** (1979), no. 2, 318–327.

[3] J.D. Achter, R. Pries, "The integral monodromy of hyperelliptic and trielliptic curves," *Math. Annalen* **338** (2007), no. 1, 187–206.

[4] V. I. Arnol′d, S. M. Guseĭn-Zade and A. N. Varchenko, *Singularities of differentiable maps. Vol. II.*, Birkhäuser, 1988.

[5] R. Biggers and M. Fried, "Irreducibility of moduli spaces of cyclic unramified covers of genus g curves", *Trans. A.M.S.,* **295** (1986) no. 1, 59–70.

[6] A. Clebsch, "Zur Theorie der Riemann'schen Fläche," *Math. Ann.* **6** (1873), no. 2, 216–230.

[7] D. B. Cohen, "The Hurwitz monodromy group," *J. Algebra* **32** (1974), no. 3, 501–517.

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups,* Oxford University Press, 1985.

[9] D. Eisenbud, N. Elkies, J. Harris, R. Speiser, "On the Hurwitz scheme and its monodromy," *Compositio Math.* **77** (1991), no. 1, 95–117.

[10] J. Ellenberg, personal communication, July 2007.

[11] W. Fulton, "Hurwitz schemes and irreducibility of moduli of algebraic curves", *Ann. Math.* **90** (1969) no. 3, 542–575.

[12] The GAP Group, *GAP – Groups, Algorithms, and Programming*, version 4.4.10, 2007. (http://www.gap-system.org)

[13] F. Gross and L. Kovács, On normal subgroups which are direct products, *J. Alg.* **90** (1984) 133–168.

[14] C. Hall, "Big symplectic or orthogonal monodromy modulo ℓ," *Duke Math. J.* **141** (2008), no. 1, 179–203.

[15] C. MacLachlan, "On representations of Artin's braid group," *Michigan Math. J.* **25** (1978), no. 2, 235–244.

[16] V. M. Petechuk, "Isomorphisms of symplectic groups over commutative rings", *Algebra and Logic,* **22** (1983), no. 5, 397–405.

[17] M. Suzuki, *Group theory. I.*, Grundlehren der Mathematischen Wissenschaften **247**, Springer-Verlag, Berlin-New York, 1982.

Department of Mathematics, University of Texas, Austin
E-mail address: `allcock@math.utexas.edu`
URL: `http://www.math.utexas.edu/~allcock`

Department of Mathematics, University of Michigan, Ann Arbor
E-mail address: `hallcj@umich.edu`