TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 295, Number 1, May 1986

IRREDUCIBILITY OF MODULI SPACES OF CYCLIC UNRAMIFIED COVERS OF GENUS g CURVES

R. BIGGERS AND M. FRIED[1]

ABSTRACT. Let $(C_1, \ldots, C_r, G) = (\mathbf{C}, G)$ be an r-tuple consisting of a transitive subgroup G of S_m and r conjugacy classes $C_1, \ldots, C_r$ of G. We consider the concept of the moduli space $\mathcal{H}(\mathbf{C}, G)$ of compact Riemann surface covers of the Riemann sphere of *Nielsen class* $(\mathbf{C}, G)$. The irreducibility of $\mathcal{H}(\mathbf{C}, G)$ is equivalent to the transitivity of a specific permutation representation of the *Hurwitz monodromy group* (§1), but there are few general tools to decide questions about this representation. Theorem 2 gives a class of examples of $(\mathbf{C}, G)$ for which $\mathcal{H}(\mathbf{C}, G)$ is irreducible. As an immediate corollary this gives an elementary proof and generalization of the irreduciblity of the moduli space of cyclic unramified covers of genus g curves (for which Deligne and Mumford [**DM**, Theorem 5.15] applied Teichmüller theory and Dehn's theorem). This contrasts with the examples of $(\mathbf{C}, G)$ in [**BFr**] for which $\mathcal{H}(\mathbf{C}, G)$ is reducible. These kinds of questions combined with the study of the existence of rational subvarieties of $\mathcal{H}(\mathbf{C}, G)$ have application to the realization of a group G as the Galois group of a regular extension of $\mathbb{Q}(t)$ [**Fr3**, §4].

1. Introduction to the fundamental moduli spaces. The most well-known moduli spaces of compact Riemann surfaces are the moduli spaces, denoted $\mathcal{M}_g$, of compact Riemann surfaces of genus $g \geq 1$ (in the case $g = 0$, $\mathcal{M}_g$ can be taken to be a point). Each point of $\mathcal{M}_g$ corresponds to exactly one isomorphism class of surfaces of genus g. Furthermore, $\mathcal{M}_g$ is a complex analytic set (actually, algebraic) with the following key property. Let $\Phi: \mathcal{X} \to \mathcal{P}$ be a family of compact Riemann surfaces of genus g. Here that will mean that $\mathcal{X}$ and $\mathcal{P}$ are compact analytic sets, that Φ is a complex analytic map, and that for each point $\mathfrak{p} \in \mathcal{P}$ the set $\{x \in \mathcal{X} \mid \Phi(x) = \mathfrak{p}\} = \mathcal{X}_\mathfrak{p}$, *the fiber over* $\mathfrak{p}$, naturally inherits the structure of a compact Riemann surface of genus g. Then the natural map,

$$\Phi: \mathcal{P} \to \mathcal{M}_g, \tag{1.1}$$

defined by $\mathfrak{p} \to [\mathcal{X}_\mathfrak{p}]$ (the isomorphism class of $\mathcal{X}_\mathfrak{p}$) is complex analytic. A succinct story, with references, on the *irreducibility of* $\mathcal{M}_g$ appears in [**Fu**].

Deligne and Mumford [**DM**, Theorem 5.15] prove the irreducibility of spaces ${}_n\mathcal{M}_g$, $n \geq 1$, $g \geq 2$, that generalize the classical moduli spaces, $\mathcal{C}_n$, of elliptic curves with level n structure. The irreducibility of $\mathcal{C}_n$ follows from the identification of it

Received by the editors February 2, 1985.
1980 *Mathematics Subject Classification.* Primary 14H10; Secondary 20C32, 30F20.
Key words and phrases. Riemann surface, moduli space, Hurwitz monodromy group, permutation representation.
[1]Manuscript written while the second author was a Lady Davis Research Professor visiting the Hebrew University in Jerusalem, Israel.

with the quotient of the complex upper half plane by the action of

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod(n) \right\}.$$

In the [**DM**] generalization, Teichmüller theory [**W**] and Dehn's theorem allow for a presentation of ${}_n\mathcal{M}_g$ as a quotient of a ball. These heavy tools limit the possibility of immediate generalization. This we give in a framework, considerably more elementary than that of [**DM**], that follows the classical tradition of [**Hu**].

For the sake of simplicity, but still allowing for fair comparison with [**DM**, Theorem 5.15] we generalize (Theorem 3) the proof of the irreducibility of ${}_o\mathcal{C}_{n,g}$, the *moduli space of cyclic unramified covers of degree n of genus g curves.* This corollary of [**DM**, Theorem 5.15] generalizes the irreducibility of the curves ${}_o\mathcal{C}_n$ that are classically identified with the quotient of the upper half plane by the group $\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{C}) \mid c \equiv 0 \bmod(n)\}$. In the special case $g = 4$ and 5, $n = 2$, this is an essential ingredient of the results of [**B**] on the number of components of the space of singular theta divisors of dimensions 4 and 5. Following a precise description of the spaces with which we shall deal, this section concludes with a paragraph of exposition on direct and general motivation for such irreducibility results through [**Fr2** and **Th**], connecting them to the classical inverse Galois group problem over $\mathbb{Q}$.

Riemann's existence theorem allows us to use combinatorial techniques in our analysis of moduli spaces. Each compact Riemann surface X can be presented as a cover $\varphi: X \to \mathbb{P}^1$ of the projective line. Let $z_1, \dots, z_r$ be a list of the distinct points of $\mathbb{P}^1$ over which φ is ramified, and let $m(\varphi) = m$ denote the degree of φ. For a given surface X, it can be difficult to describe the possible values of r and m. But, there is a one-one correspondence between the elements of the following two sets [**Fr1**, §1]:

(1.2) (a) the quotient of $\{\boldsymbol{\sigma} = (\sigma(1), \dots, \sigma(r)) \in (S_m)^r \mid \sigma(1)\sigma(2)\cdots\sigma(r) = 1$ and $\langle \sigma(1), \dots, \sigma(r) \rangle = G(\boldsymbol{\sigma})$ is a transitive subgroup of $S_m\}$ by the relation that equivalences $\boldsymbol{\sigma}$ and $\gamma^{-1} \cdot \boldsymbol{\sigma} \cdot \gamma = (\gamma^{-1} \cdot \sigma(1) \cdot \gamma, \dots, \gamma^{-1} \cdot \sigma(r) \cdot \gamma)$ for each $\gamma \in S_m$; and

(b) the quotient of $\{\varphi': X' \to \mathbb{P}^1$ of connected covers of degree m with branch locus in $\{z_1, \dots, z_r\}\}$ by the relation that equivalences $\varphi': X' \to \mathbb{P}^1$ and $\varphi' \circ \psi: X'' \to \mathbb{P}^1$ for $\psi: X'' \to X'$ an isomorphism.

Such a correspondence, however, depends on additional data, and cannot be regarded as functional.

Let $(C_1, \dots, C_r, G) = (\mathbf{C}, G)$ be an r-tuple consisting of a transitive subgroup G of S_m and r conjugacy classes $C_1, \dots, C_r$ of G. Denote the set {equivalence classes of $\boldsymbol{\sigma} \in (S_m)^r$ | such that $G(\boldsymbol{\sigma}) = G$ and there exists $\beta \in S_r$ with $\sigma(\beta(i)) \in C_i$, $i = 1, \dots, r\}$ by $\mathrm{Ni}(\mathbf{C}, G)$, the *Nielsen class of* $(\mathbf{C}, G)$. We assume, from here on, that $(\mathbf{C}, G)$ is so chosen that $\mathrm{Ni}(\mathbf{C}, G)$ is nonempty.

We now list $r - 1$ operators $Q_1, \dots, Q_{r-1}$ that naturally act as permutations of the elements of $\mathrm{Ni}(\mathbf{C}, G)$ by a right-hand action. Indeed, Q_i maps the equivalence class of $\boldsymbol{\sigma} = (\sigma(1), \dots, \sigma(r))$ to the equivalence class of

$$(1.3) \quad (\boldsymbol{\sigma})Q_i = \big(\sigma(1), \dots, \sigma(i-1), \sigma(i) \cdot \sigma(i+1) \cdot \sigma(i)^{-1}, \sigma(i), \dots, \sigma(r)\big), \quad i = 1, \dots, r-1.$$

Our discussion continues with a brief review from [**BFr**, pp. 89–95]. Identify $\mathbb{P}^r$ with the quotient of the nonzero polynomials in x of degree at most r,

$$\left\{\sum_{j=0}^{r} a_j \cdot x^j \not\equiv 0 \mid a_j \in \mathbb{C},\ j = 0, \ldots, r\right\},$$

by the relation that equivalences $\sum_{i=0}^{r} a_i \cdot x^i$ and $\sum_{i=0}^{r} a \cdot a_i \cdot x^i$ for $a \in \mathbb{C} - \{0\}$.

Consider the natural map—the *Noether cover*—

$$\Phi_r \colon (\mathbb{P}^1)^r \to \mathbb{P}^r \tag{1.4}$$

that maps $(z_1, \ldots, z_r) \in (\mathbb{P}^1)^r$ to the equivalence class of $\prod_{j=1}^{p}(x - z_j)$ with the proviso that the factor $x - z_j$ is replaced by 1 if $z_j = \infty$. Let Δ_r be the subset of $(\mathbb{P}_1)^r$ consisting of points with two or more equal coordinates, and let D_r, the *discriminant locus of the Noether cover*, be the image of Δ_r under Φ_r. For $\mathbf{a}^0 \in \mathbb{P}^r - D_r$, the fundamental group, $\pi_1(\mathbb{P}^r - D_r, \mathbf{a}^0)$, is the quotient of the free group generated by elements $Q_1, \ldots, Q_{r-1}$ by the following list of relations [**FaBu**]:

$$\begin{aligned} &\text{(a)}\quad Q_i \cdot Q_j = Q_j \cdot Q_i, \qquad |i-j| \geq 2,\ 1 \leq i,j \leq r-1; \\ &\text{(b)}\quad Q_i \cdot Q_{i+1} \cdot Q_i = Q_{i+1} \cdot Q_i \cdot Q_{i+1}, \qquad 1 \leq i \leq r-1; \\ &\text{(c)}\quad Q_1 \cdots Q_{r-2} \cdot (Q_{r-1})^2 \cdot Q_{r-2} \cdots Q_1 = 1. \end{aligned} \tag{1.5}$$

From (1.5) the action given by (1.3) gives a permutation representation of $\pi_1(\mathbb{P}^r - D_r, \mathbf{a}^0)$ on the set $\mathrm{Ni}(\mathbf{C}, G)$. Let $Br_1, \ldots, Br_t$ be the distinct orbits of this action. Covering space theory associates to each Br_i an equivalence class of unramified covers

$$\mathcal{H}(Br_i) \to \mathbb{P}^r - D_r, \qquad i = 1, \ldots, t. \tag{1.6}$$

Define the (absolute) Hurwitz space $\mathcal{H}(\mathbf{C}, G)$ of $\mathrm{Ni}(\mathbf{C}, G)$ to be the disjoint union of the spaces $\mathcal{H}(Br_i)$, $i = 1, \ldots, t$. In [**BFr**, p. 104] (or [**Fr1**, §4] without the use of (1.5)) it is shown that $\mathcal{H}(\mathbf{C}, G)$ is a (coarse) moduli space for covers of Nielsen type $\mathrm{Ni}(\mathbf{C}, G)$ (i.e., covers $\varphi \colon X \to \mathbb{P}^1$ for which the $\boldsymbol{\sigma}$ given by (1.2)(a) is in $\mathrm{Ni}(\mathbf{C}, G)$). Then $\mathcal{H}(\mathbf{C}, G)$ is irreducible if and only if $t = 1$. Denote t by $\mathrm{Hur}(\mathbf{C}, G)$, the *Hurwitz number* of $(\mathbf{C}, G)$.

Theorem 2 of this paper shows that $\mathrm{Hur}(\mathbf{C}, G) = 1$ in the following case. Let S_m act on $(\mathbb{Z}/(n))^m$ by permutation of the coordinates. Denote the semidirect product of S_m and $(\mathbb{Z}/(n))^m$ by $(\mathbb{Z}/(n))^m \times^s S_m = \overline{G}$. Indicate elements of $\overline{G}$ by $(\alpha_1, \ldots, \alpha_m; \sigma) = (\boldsymbol{\alpha}; \sigma)$, $\alpha_k \in \mathbb{Z}/(n)$, $k = 1, \ldots, m$ and $\sigma \in S_m$. Let G be the subgroup of $\overline{G}$ consisting of $(\boldsymbol{\alpha}; \sigma)$ such that $\alpha_1 + \cdots + \alpha_m = 0$. Clearly G is normal in $\overline{G}$ and $\overline{G}$ may be regarded as a subgroup of $S_{m \cdot n}$. Then $\mathrm{Hur}(\mathbf{C}, G) = 1$ if $C_1 = C_2 = \cdots = C_r$ are the conjugacy class of $(\mathbf{0}; (1\ 2))$, $r \geq 4$ is an even integer and $m \geq 3$. The evenness of r assures that $\mathrm{Ni}(\mathbf{C}, G)$ is nonempty. Theorem 3 is a corollary, based on general principles, of Theorem 2.

The main theorem of [**Fr1**, §5] shows that under very mild group theoretic conditions on $(\mathbf{C}, G)$, the space $\mathcal{H}(\mathbf{C}, G)$ parametrizes a family of covers $\{\varphi_{\mathfrak{p}} \colon X_{\mathfrak{p}} \to \mathbb{P}^1 \mid \mathfrak{p} \in \mathcal{H}(\mathbf{C}, G)\}$ where the family, the map from the family to $\mathcal{H}(\mathbf{C}, G)$ and $\mathcal{H}(\mathbf{C}, G)$ are all algebraic sets defined over some cyclotomic field—*in the case that* $\mathrm{Hur}(\mathbf{C}, G) = 1$. It even gives the precise cyclotomic field K in question. Little, however, is known in the case that $\mathrm{Hur}(\mathbf{C}, G)$ exceeds 1, except that this can happen [**BFr**, §3]. If, furthermore, $\mathcal{H}(\mathbf{C}, G)$ contains a *K-rational subvariety* (even K-unirationality often suffices, as [**Fr3**, §4] explains), the K-rational points of this variety parametrize a family of curves $f(x,y) = 0$ defined over K for which $K(x,y)/K(x)$ is a regular Galois extension with group G. This is all sufficiently combinatorial to suggest a program for finding $\mathbf{C}$, given G, so as to get the cyclotomic field in question to be $\mathbb{Q}$. Thompson [**Th**] has stated such in the case that $r = 3$ (where $\mathcal{H}(\mathbf{C}, G)$ is covered by $(\mathbb{P}^1)^3 - \Delta_3$, and is always $\mathbb{Q}$-rational). This continues with work of Feit [**Fe**], Matzat [**Ma**] and Walter [**Wa**].

Since it is unlikely that a general technique will carry the program through with just the case $r = 3$, [**Fr3**, Theorem 4.2] states a condition that has produced nontrivial examples with $\mathcal{H}(\mathbf{C}, G)$ a rational variety for $r > 3$. It suggests a program that adds additional conditions to $\mathbf{C}$ to assure the rationality (and, when appropriate, $\mathbb{Q}$-rationality) of $\mathcal{H}(\mathbf{C}, G)$. Even in the case that $r = 4$, there are pairs $(\mathbf{C}, G)$ with $\mathcal{H}(\mathbf{C}, G)$ nonunirational (e.g., [**Fr2**, Theorem 3.3] gives an example where $\mathcal{H}(\mathbf{C}, G)$ maps surjectively to the modular curve ${}_o\mathcal{C}_n$; its genus exceeds o for n suitably large, and therefore a well-known generalization of Luroth's theorem shows that $\mathcal{H}(\mathbf{C}, G)$ is nonunirational). The argument of §3 of this paper, combined with [**HM**], shows that for $(\mathbf{C}, G)$ given in Theorem 2 with r suitably large, investigation of $\mathcal{H}(\mathbf{C}, G)$ is not amenable to any present day techniques that generalize the use of unirationality.

2. The group theory of moduli spaces of cyclic covers. Let $\varphi: X \to \mathbb{P}^1$ be a cover of degree m for which there are at least $m - 1$ points of X over each point of $\mathbb{P}^1$. If $\boldsymbol{\sigma}$ corresponds to this cover by (1.2)(a), then $\sigma(i)$ is a transposition, $i = 1, \ldots, r$. Such a cover is called *simple*. We are interested in the following situation. Let

$$X' \xrightarrow{\psi} X \xrightarrow{\varphi} \mathbb{P}^1 \tag{2.1}$$

be a sequence of covers of compact (connected) Riemann surfaces with these properties: the genus of X is g, φ is a simple cover of degree m; and ψ is an unramified Galois cover with group $\mathbb{Z}/(n)$. Our first theorem computes the Nielsen class of the cover $\varphi \circ \psi: X' \to \mathbb{P}^1$.

Let G be the subgroup of $\overline{G} = (\mathbb{Z}/(n))^m \times^s S_m$ given in §1. The *Galois closure* of $\varphi \circ \psi: X' \to \mathbb{P}^1$ is a Galois cover $\hat{\varphi}: \hat{X} \to \mathbb{P}^1$ of smallest possible degree such that there exists a sequence of covers

$$\hat{X} \xrightarrow{\hat{\psi}} X' \xrightarrow{\varphi\circ\psi} \mathbb{P}^1 \tag{2.2}$$

with $(\varphi \circ \psi) \circ \hat{\psi} = \hat{\varphi}$. Up to equivalence the Galois closure is unique.

THEOREM 1. *Suppose that $m \geq 3$ in the above notation. Then the Galois group of the Galois closure of $\varphi \circ \psi: X' \to \mathbb{P}^1$ given by (2.1) is isomorphic to G. If a correspondence given by (1.2) is set up, then this cover corresponds to $\boldsymbol{\sigma}' = (\sigma(1)', \ldots, \sigma(r)')$ where*

$$\sigma(i)' = \Big(0, \ldots, 0, \underset{\substack{\uparrow \\ j\text{th pos.}}}{\alpha}, 0, \ldots, 0, \underset{\substack{\uparrow \\ k\text{th pos.}}}{-\alpha}, 0, \ldots, 0; \sigma(i)\Big)$$

with $\sigma(i) = (j\ k) \in S_m$ *and* $\alpha \in \mathbb{Z}/(n)$ (j, k *and* α *dependent on* i), $i = 1, \ldots, r$, $\sigma(1)' \cdots \sigma(r)' = 1$ *and* $G(\boldsymbol{\sigma}') = G$. *In particular,* $r \geq 2m$, *and the cover is in the Nielsen class* $\mathrm{Ni}(\mathbf{C}, G)$ *with* $C_1 = C_2 = \cdots = C_r$, *where* C_1 *is the conjugacy class of* $\{\mathbf{0}; (1\ 2)\}$.

PROOF. The second of the three parts of the proof includes some notation for manipulation within the group $\overline{G}$ to which we will refer later.

PART A. *The Galois group of* $\hat{\varphi}: \hat{X} \to \mathbf{P}^1$. There is a notational simplification if we compute using the function fields of the Riemann surfaces. Let $\mathbb{C}(X)$ (resp., $\mathbb{C}(X')$, $\mathbb{C}(\hat{X})$) be the field of meromorphic functions on X (resp., X', $\hat{X}$). Also, let $\mathbb{C}(\mathbf{P}^1) = \mathbb{C}(z)$ for some indeterminate z. Then (the primitive element theorem), $\mathbb{C}(X) = \mathbb{C}(z, x)$ for some $x \in \mathbb{C}(X)$. Let $x = x_1, \ldots, x_m$ be the conjugates of x over $\mathbb{C}(z)$. Since $\mathbb{C}(X')/\mathbb{C}(X)$ is a cyclic extension with group $\mathbb{Z}/(n)$, we may choose $y = y_1 \in \mathbb{C}(X)$ so that $\mathbb{C}(X') = \mathbb{C}(z, x_1, y_1^{1/n})$. Thus, $\mathbb{C}(\hat{X}) = \mathbb{C}(z, x_1, y_1^{1/n}, \ldots, x_m, y_m^{1/n})$ with $y_1, \ldots, y_m$ the conjugates of y_1 over $\mathbb{C}(z)$.

Let ς_n be a primitive nth root of 1. The conjugates of $y_1^{1/m}$ over $\mathbb{C}(z)$ are exactly $\varsigma_n^\alpha \cdot y_j^{1/n}$, $j = 1, \ldots, m$, $\alpha \in \mathbb{Z}/(n)$. Let $\tau \in G(\mathbb{C}(\hat{X})/\mathbb{C}(z))$. Associate to τ the element $F(\tau) \in \overline{G}$ by the following formula: if τ maps $(x_j, \varsigma_n^\alpha \cdot y_j^{1/n})$ to $(x_k, \varsigma_n^\beta \cdot y_k^{1/n})$, then

$$F(\tau) = \left(\cdots, \underset{\substack{\uparrow \\ j\text{th pos.}}}{\beta - \alpha}, \ \ldots; \sigma \right) \quad \text{where } \sigma(j) = k,\ j = 1, \ldots, m. \tag{2.3}$$

Check that F is a group homomorphism that embeds $G(\mathbb{C}(\hat{X})/\mathbb{C}(z))$ into $\overline{G}$. Let $D(\varphi)$ be the set of branch points of the cover $\varphi: X \to \mathbf{P}^1$.

The correspondence of (1.2) arises by choosing a suitable set $\mathcal{L}_1, \ldots, \mathcal{L}_r$ of closed paths on $\mathbf{P}^1 - D(\varphi)$, all based at $z_0 \in \mathbf{P}^1 - D(\varphi)$, so that the homotopy classes of these paths generate the fundamental group $\pi_1(\mathbf{P}^1 - D(\varphi), z_0)$. Then the cover $\varphi: X \to \mathbf{P}^1$ corresponds to $(\sigma(1), \ldots, \sigma(r))$, where $\sigma(i)$ gives the effect of analytically continuing the functions $x_1, \ldots, x_m$ around the path $\mathcal{L}_i$. In more detail, express $x_1, \ldots, x_m$ as power series in a neighborhood of z_0. Then analytically continue each around $\mathcal{L}_i$ to get a permutation, $\sigma(i)$, of these power series expressions, $i = 1, \ldots, r$.

Since $X' \to X$ is unramified, the paths $\mathcal{L}_1, \ldots, \mathcal{L}_r$ suffice to compute $\boldsymbol{\sigma}'$ for the cover $\varphi \circ \psi: X' \to \mathbf{P}^1$, and $\sigma(i)'$ is of the same order as $\sigma(i)$, $i = 1, \ldots, r$. Because $\varphi: X \to \mathbf{P}^1$ is a simple branched cover, $\sigma(i)' = (\alpha_1, \ldots, \alpha_m; \sigma(i))$ is of order 2, and as an element in $S_{m \cdot n}$ it consists of n disjoint 2-cycles. For example, if $\sigma(i) = (j\ k)$, then a suitable notation would have

$$\sigma(i)' = (j \cdot n + 1\ \ k \cdot n + u_1)(j \cdot n + 2\ \ k \cdot n + u_2) \cdots ((j+1) \cdot n\ \ k \cdot n + u_n)$$

where $u_1, \ldots, u_n$ is a permutation of $1, 2, \ldots, n$ that is determined by u_1, $i = 1, \ldots, r$.

PART B. *Notation within the group* $\overline{G}$. In the notation of Part A we can write $\sigma(i)'$ as $(\alpha_1, \ldots, \alpha_m; (j\ k))$ with $\alpha_j = u_1 - 1 = \alpha$, $\alpha_k = -\alpha$ and $\alpha_l = 0$ for $l \neq j, k$. For future computations designate this element by $(\alpha_{jk}; (j\ k))$. More generally, write $(\alpha_{jk}; \sigma)$ for σ any element of S_m, where α_{jk} denotes the first part of $\sigma(i)'$.

Let $\mathrm{pr}: \overline{G} \to S_m$ denote the natural projection onto S_m. Thus $G(\mathbb{C}(\hat{X})/\mathbb{C}(P^1)) =$

$G(\boldsymbol{\sigma}')$ is a subgroup H of $\overline{G}$ with the following properties:

(2.4) (a) H is generated by elements of the form $(\alpha_{jk}; (j\ k))$;
(b) $\mathrm{pr}(H) = G(\boldsymbol{\sigma})$; and
(c) $H \cap ((\mathbb{Z}/(n))^m \times 1)$ projects surjectively onto any factor of $(\mathbb{Z}/(n))^m$.

Property (2.4)(a) implies that H is contained in G. Since $G(\boldsymbol{\sigma})$ is a transitive subgroup of S_m generated by 2-cycles, it is well known that $G(\boldsymbol{\sigma}) = S_m$. The conclusion that $H = G$ follows easily if we show that H contains $(\alpha_{12}; 1)$ for each $\alpha \in \mathbb{Z}/(n)$. Indeed, this gives $(\alpha_{1k}; 1) \in H$, $k = 2, \ldots, m$, and therefore $(-\alpha_2 - \cdots - \alpha_m, \alpha_2, \ldots, \alpha_m; 1) \in H$ for each $\alpha_2, \ldots, \alpha_m \in \mathbb{Z}/(n)$. Suppose that $\tau = (\beta_1, \ldots, \beta_m; \sigma) \in \overline{G}$. Explicitly compute the conjugate of $(\alpha_{jk}; (j\ k))$ by this element as

$$\begin{aligned}\tau \cdot (\alpha_{jk}; (j\ k)) \cdot \tau^{-1} &= (\beta_1, \ldots, \beta_m; \sigma) \cdot (\alpha_{jk}; (j\ k)) \cdot (-\beta_{\sigma(1)}, \ldots, -\beta_{\sigma(m)}; \sigma^{-1}) \\ &= ((\alpha + \beta_{\sigma(j)} - \beta_{\sigma(k)})_{\sigma(j)\sigma(k)}; (\sigma(j)\ \sigma(k))).\end{aligned}$$

PART C. *Conclusion of the proof.* Consider all conjugates of elements of $\{\sigma(1)', \ldots, \sigma(r)'\}$ (by elements of H) to elements of the form $(\alpha_{12}; (1\,2))$. Since $G(\boldsymbol{\sigma}) = S_m$, (2.5) gives at least one for each $\sigma(i)'$, $i = 1, \ldots, r$. Denote the collection of first coordinates so obtained by A. From $(\alpha'_{12}; (1\ 2)) \cdot (\alpha_{12}; (1\ 2)) = ((\alpha' - \alpha)_{12}; 1)$ and (2.4)(c) deduce that H contains $(\alpha_{12}; 1)$ for each $\alpha \in \mathbb{Z}/(n)$. This concludes the proof that $G(\boldsymbol{\sigma}') = G$.

We are done if we show that the conjugacy class of $(\alpha_{ij}; (i\ j))$ contains $(\mathbf{0}; (1\ 2))$. This uses that $m \geq 3$. Choose $\sigma \in S_m$ so that $\sigma(j) = 1$, $\sigma(k) = 2$ and choose $\beta_1 = -\alpha$, $\beta_2 = 0$, $\beta_3 = \alpha$ and $0 = \beta_4 = \cdots = \beta_m$. Now apply (2.5). □

Identify $\mathbb{Z}/n$ with the group generated by $(1\ 2 \cdots n)$ in S_n. This identification is compatible with the Galois theory of Theorem 1. Then the normalizer of G in $(S_n)^m \times^s S_m$ is $(N_n)^m \times^s S_m$, where N_n is the normalizer of $\langle(1\ 2 \cdots n)\rangle$ in S_n. Clearly N_n is the semidirect product $\mathbb{Z}/(n) \times^s (\mathbb{Z}(n))^*$ of $\mathbb{Z}/(n)$ and the invertible elements of $\mathbb{Z}/(n)$. These groups too, may be regarded as subgroups of $S_{m \cdot n}$.

DEFINITION 1. Call a sequence of the type given by (2.1) a *simple by cyclic sequence of type* (m, r, n).

EXAMPLE 1. *The case* $m = 2$. This case was excluded by Theorem 1. The proof, up to the point of showing that the Galois group is G, still holds. But, if n is even, then an application of (2.5) shows that $(0_{12}; (1\ 2))$ and $(1_{12}; (1\ 2)) = (1, -1; (1\ 2))$ are in distinct conjugacy classes of G. □

3. Irreducibility of spaces of simple by cyclic sequences. From Theorem 1 we may identify the space of simple by cyclic sequences of type (m, r, n), $m \geq 3$, with the covers $\gamma' \colon X' \to \mathbb{P}^1$ of Nielsen type $\mathrm{Ni}(\mathbf{C}, G)$, where $\deg(\gamma') = m \cdot n$ and G and $\mathbf{C}$ are given in the statement of the theorem. Here is a typical representative of a class in $\mathrm{Ni}(\mathbf{C}, G)$:

$$\begin{aligned}(3.1)\quad \boldsymbol{\sigma}' = ((\mathbf{0}; (1\ 3)), (\mathbf{0}; (1\ 3)), \ldots, (\mathbf{0}; (1\ m)), (\mathbf{0}; (1\ m)); (1_{12}; (1\ 2)), (1_{12}; (1\ 2)), \\ (\mathbf{0}; (1\ 2)), \ldots, (\mathbf{0}; (1\ 2)), (\mathbf{0}; (1\ 2)), (\mathbf{0}; (1\ 2))).\end{aligned}$$

In words, the first $2(m-2)$ entries generate $\mathbf{0} \times S_{m-1}$, where S_{m-1} is the subgroup of S_m that fixes 2; the next two entries are both $(1_{12}; 1\ 2)) = (1, -1, 0, \ldots, 0; (1\ 2))$; and the final $r - 2 \cdot (m-1)$ entries are repetitions of $(0; (1\ 2))$.

From §1 the irreducibility of the space of simple by cyclic sequences of type (m, r, n) or, equivalently, of the space $\mathcal{H}(\mathbf{C}, G)$ follows if for $\boldsymbol{\sigma}'' \in \mathrm{Ni}(\mathbf{C}, G)$ we show the existence of $\tau \in (N_n)^m \times^s S_m$ (end of §2) and $Q \in \pi_1(\mathbf{P}^r - D_r, \mathbf{a}^0)$ such that

$$(\tau \cdot \boldsymbol{\sigma}'' \cdot \tau^{-1})Q = \boldsymbol{\sigma}'. \tag{3.2}$$

The special case with $n = 1$ has been a part of many papers [**Fu**], and, in the main, it goes back to Clebsch [**C**]. We state it here, but, for completeness, include a brief proof in an appendix. Note again that r is of necessity even in the next result so that $\mathrm{Ni}(\mathbf{B}, S_m)$ is nonempty.

PROPOSITION 1. *The space $\mathcal{H}(\mathbf{B}, S_m)$ is irreducible, where $\mathbf{B} = (B_1, \ldots, B_r)$ and $B_1 = \cdots = B_r$ with B_1 the conjugacy class of $(1\ 2)$ in S_m.*

Following the next three lemmas we state the main theorem.

LEMMA 1. *Denote the element*

$$(0, \ldots, 0,\ \underset{\substack{\uparrow \\ k\text{th pos.}}}{(v, u)},\ 0, \ldots, 0; \sigma)$$

with $\sigma \in S_m$ and $(v, u) \in (\mathbb{Z}/(n)) \times^s \mathbb{Z}/(n)^*$ by $((v, u)_k; \sigma)$. By generalization of (2.5), $((v, u)_k; 1) \cdot (\alpha'_{ij}; (i\ j)) \cdot ((v, u)_k; 1)^{-1}$ is equal to the following expression:

$$\begin{aligned} &\text{(a) } ((u \cdot \alpha' + v)_{ij}; (i\ j)) \textit{ if } k = i; \\ &\text{(b) } ((u^{-1} \cdot \alpha' - u^{-1} \cdot v)_{ij}; (i\ j)) \textit{ if } k = j; \textit{ or} \\ &\text{(c) } (\alpha'_{ij}; (i\ j)) \textit{ if } k \neq i, j. \end{aligned} \tag{3.3}$$

PROOF. This follows from the natural action of N_n on $\mathbb{Z}/(n)$ (as at the end of §2, $(v, u) \in N_n$ maps $\alpha' \in \mathbb{Z}/(n)$ to $u \cdot \alpha' + v$). □

LEMMA 2. *Let $\sigma'_i = (c_{12}^{(i)}; (1\ 2)) \in G$, $i = 1, 2, \ldots, r'$. Assume that $\sigma'_1 \cdots \sigma'_{r'} = (\mathbf{0}; 1)$. Then $\sum_{i=1}^{r'} (-1)^i \cdot c^{(i)} = 0$. Assume further that $n = p \cdot n_1$, where p is a prime, and if $n_1 > 1$, then*

$$c^{(1)} \equiv c^{(2)} \equiv 1 \bmod(n_1) \quad \textit{and} \quad c^{(j)} \equiv 0 \bmod(n_1), \quad j = 3, \ldots, r'. \tag{3.4}$$

Then there exists $Q \in \pi_1(\mathbf{P}^{r'} - D_{r'}, \mathbf{a}^0)$ such that $(\boldsymbol{\sigma}')Q = \boldsymbol{\sigma}''$ with $\sigma''_i = (d_{12}^{(i)}; (1\ 2))$, $i = 1, \ldots, r'$, with these properties:

(3.5) (a) *$d^{(1)} \equiv d^{(2)} \bmod(n)$ and $d^{(j)} \equiv 0 \bmod(n)$, $j = 3, \ldots, r'$, if $n_1 > 1$; and*
(b) *there exists $t \geq 0$ such that $d^{(1)} \equiv d^{(2)} \equiv \cdots \equiv d^{(t)} \bmod(p)$ and $d^{(j)} \equiv 0 \bmod(p)$, $j = t + 1, \ldots, r'$, if $n_1 = 1$.*

PROOF. For $u \geq 1$ we first compute the effect of $(Q_u)^m$ on $\boldsymbol{\sigma}'$. The uth and $(u+1)$th entries of $(\boldsymbol{\sigma}')Q_u$, are, respectively, $((2 \cdot c^{(u)} - c^{(u+1)})_{12}; (1\ 2))$ and $(c_{12}^{(u)}; (1\ 2))$; the uth and $(u+1)$th entries of $(\boldsymbol{\sigma}')Q_u^2$ are $((3 \cdot c^{(u)} - 2 \cdot c^{(u+1)})_{12}; (1\ 2))$ and $((2 \cdot c^{(u)} - c^{(u+1)})_{12}; (1\ 2)), \ldots$; and the uth and $(u+1)$th entries of $(\boldsymbol{\sigma}')(Q_u)^m$ are

$$\begin{aligned} &((m \cdot (c^{(u)} - c^{(u+1)}) + c^{(u)})_{12}; (1\ 2)) \quad \text{and} \\ &(((m-1) \cdot (c^{(u)} - c^{(u+1)}) + c^{(u)})_{12}; (1\ 2)). \end{aligned} \tag{3.6}$$

Use $\langle c\rangle$ to denote the (additive) subgroup of $\mathbf{Z}/(n)$ generated by c. After an application of an element Q' of $\pi_1(\mathsf{P}^{r'} - D_{r'}, \mathbf{a}^0)$ to $\boldsymbol{\sigma}'$ we may assume that there is an integer t for which $c^{(j)} \equiv 0 \bmod(n)$ for $j \geq t+1$. Furthermore, assume that Q' has been chosen so that t is as small as possible. In particular, $c^{(1)}, \dots, c^{(t)}$ are not congruent to 0 mod(n). From this point on we will work with elements of $\pi_1(\mathsf{P}^{r'} - D_{r'}, \mathbf{a}^0)$ that affect only the coordinate entries $1, \dots, t$.

First assume that $n_1 > 1$. Suppose that $t > 2$. Then apply (3.6) to the case $u = 2$. Since $c^{(2)} - c^{(3)}$ is a unit mod(n), we may choose m so that $m\cdot(c^{(u)} - c^{(u+1)}) + c^{(u)} \equiv 0 \bmod(n)$. Furthermore, there exists an element $Q'' \in \pi_1(\mathsf{P}^{r'} - D_{r'}, \mathbf{a}^0)$ that moves only the coordinate entries $2, \dots, t$, and which moves the second coordinate entry, otherwise unchanged, to the tth coordinate. Thus, the last $r' - t + 1$ coordinate entries of $(Q_2)^m \circ Q''$ applied to $\boldsymbol{\sigma}'$ are of the form $(\mathbf{0}; (1\ 2))$, contrary to our assumption about t. This concludes the proof of (3.5)(a) under the assumption that $n_1 > 1$. Now assume that $n_1 = 1$ and that p is a prime.

Assume that there exists $i < t$ such that $d^{(i)} \not\equiv d^{(i+1)} \bmod(p)$. Then $d^{(i)} - d^{(i+1)}$ is a unit mod(p). The same argument as in the preceding paragraph then applies with $i = u$. This gives (3.5)(b) and the lemma. □

LEMMA 3 [**BFr**, LEMMA 3.8]. *Let $\boldsymbol{\sigma} \in (S_{m'})^{r'}$ with $G(\boldsymbol{\sigma})$ transitive and $\sigma(1)\cdots\sigma(r') = 1$. Let $\tau \in G(\boldsymbol{\sigma})$. Then there exists $Q \in \pi_1(\mathsf{P}^{r'} - D_{r'}, \mathbf{a}^0)$ such that $\tau^{-1}\cdot\boldsymbol{\sigma}\cdot\tau = (\boldsymbol{\sigma})Q$.*

THEOREM 2. *Let* $\mathrm{Ni}(\mathbf{C}, G)$ *be the Nielsen class which contains the equivalence class represented by $\boldsymbol{\sigma}'$ of* (3.1). *Then* $\mathrm{Hur}(\mathbf{C}, G) = 1$. *In particular, the space of equivalence classes of simple by cyclic sequences of type (m, r, n), with even $r \geq 2m$ and $m \geq 3$, is irreducible.*

PROOF. As discussed above, we must establish (3.2). From Proposition 1, there exist $Q' \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ and $\tau_1 \in \mathbf{0} \times S_m$ such that

$$(3.7)\quad (\tau_1\cdot\boldsymbol{\sigma}''\cdot\tau_1^{-1})Q' = ((\alpha_{13}^{(3)}; (1\ 3)), (\beta_{13}^{(3)}; (1\ 3)), \dots, (\alpha_{1m}^{(m)}; (1\ m))(\beta_{1m}^{(m)}; (1\ m)); \\ (\gamma_{12}^{(1)}; (1\ 2)), \dots, (\gamma_{12}^{(r-2\cdot(m-2))}; (1\ 2))).$$

Write out that the product of the entries of (3.7) is $(\mathbf{0}, 1)$. The first coordinate gives these expressions in order:

$$(3.8)\quad \begin{aligned} &\text{(a) } \alpha^{(3)} - \beta^{(3)} + \alpha^{(4)} - \beta^{(4)} + \cdots + \alpha^{(m)} - \beta^{(m)} \\ &\qquad + \textstyle\sum_{j=1}^{r-2\cdot(m-2)} (-1)^{j-1}\cdot\gamma^{(j)} \equiv 0 \bmod(n); \\ &\text{(b) } \textstyle\sum_{j=1}^{r-2\cdot(m-2)} (-1)^j\cdot\gamma^{(j)} \equiv 0 \bmod(n); \text{ and} \\ &\text{(c) } \alpha^{(k)} - \beta^{(k)} \equiv 0 \bmod(n),\ k = 3, \dots, m. \end{aligned}$$

With no loss therefore assume that

$$(3.9)\quad \boldsymbol{\sigma}'' = ((\alpha_{13}^{(3)}; (1\ 3)), (\alpha_{13}^{(3)}; (1\ 3)), \dots, (\alpha_{1m}^{(m)}; (1\ m)), (\alpha_{1m}^{(m)}; (1\ m)); \\ (\gamma_{12}^{(1)}; (1\ 2)), \dots, (\gamma_{12}^{(r-2\cdot(m-2))}; (1\ 2))) \\ \text{with } \sum_j (-1)^j\cdot\gamma^{(j)} \equiv 0 \quad \bmod(n).$$

For simplicity of notation, denote $r - 2\cdot(m-2)$ by r' throughout the remainder. The rest of the proof divides into four parts.

PART A. *Conjugation by elements of* $\overline{G}$. Apply Lemma 1 in the case that $(v,u)_k = (-\alpha^{(k)}, 0)_k$, which we denote just by $(-\alpha^{(k)})_k$. Therefore if we conjugate (3.9) by the product of $((-\alpha^{(j)})_j; 1)$, $j = 3, \dots, m$, and by $((-\gamma^{(r')})_2; 1)$, we may assume that $\boldsymbol{\sigma}''$ is

$$(3.10)\quad ((\mathbf{0};(1\ 3)),(\mathbf{0};(1\ 3)),\dots,(\mathbf{0};(1\ m)),(\mathbf{0};(1\ m));(\gamma_{12}^{(1)};(1\ 2)),\dots,\\ (\gamma_{12}^{(r'-1)};(1\ 2)),(\mathbf{0};(1\ 2))),\quad \text{with } \gamma^{(1)}-\gamma^{(2)}+\dots+(-1)^{r'}\cdot\gamma^{(r'-1)}\equiv 0 \\ \mod(n).$$

Also, the conditions of (2.4) imply that $\gamma^{(1)}, \dots, \gamma^{(r'-1)}$ generate $\mathsf{Z}/(n)$. For the moment we assume that the conclusion of the theorem holds if n is a prime.

PART B. *Induction on* n. Assume that n is not a prime and write n as $p \cdot n_1$ with $n_1 > 1$. By the induction assumption, the conclusion of the theorem holds for n_1. Reduce the entries of (3.10) $\mod(n_1)$ to conclude that there exists $Q^{(3)} \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ such that the last r' entries of $Q^{(3)}$ applied to $\boldsymbol{\sigma}''$ (given by (3.10)) satisfy hypothesis (3.4). Thus Lemma 2 gives an element of $\pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ that acts only on the last r' coordinates of $(\boldsymbol{\sigma}'')Q^{(3)}$ to give $\boldsymbol{\sigma}'$, except for the possibility that the $(2m-4)+1$ and $(2m-4)+2$ entries are both $(c;(1\ 2))$. In this case apply Lemma 1 by conjugating $(\boldsymbol{\sigma}'', Q_3)$ by $((0, c^{-1})_2; 1)$. This concludes the theorem if n is not a prime.

PART C. *The case that* $n = p$ *is a prime.* Again apply Lemma 2, but this time under the assumption that $n_1 = 1$. Thus, according to (3.5)(b), we may assume that

(3.11)

$$\gamma^{(1)} \equiv \gamma^{(2)} \equiv \dots \equiv \gamma^{(t)} \mod(p) \qquad \text{and} \qquad \gamma^{(j)} \equiv 0 \mod(p), \quad j = t+1, \dots, r'.$$

Note that since $\gamma^{(1)} - \gamma^{(2)} + \dots + (-1)^{t-1} \cdot \gamma^{(t)} \equiv 0 \mod(p)$, t must be even. Let $m' = 2 \cdot (m-2)$. Apply $Q_{m'} \circ Q_{m'+1} \circ \dots \circ Q_{m'+t}$ to (3.10) to get

(3.12)(a)

$$(\dots,(\mathbf{0};(1\ m)),(-\gamma_{2m}^{(1)};(2\ m)),\dots,(-\gamma_{2m}^{(1)};(2\ m)),(\mathbf{0};(1\ m)),(\mathbf{0};(1\ 2)),\dots),$$

where the first $(\mathbf{0};(1\ m))$ is in the $m'-1$ position and the second is in the $m'+t$ position: then apply conjugation by $(-\gamma_m^{(1)}; 1)$ (as in the notation of Part A) to get

(3.12)(b)

$$(\dots,(\gamma_{1m}^{(1)};(1\ m)),(\mathbf{0};(2\ m)),\dots,(\mathbf{0};(2\ m)),(\gamma_{1m}^{(1)};(1\ m)),(\mathbf{0};(1\ 2)),\dots);$$

and finally apply $Q^{(4)} \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ that moves the two coordinate entries of the form $(\gamma_{1m}^{(1)};(1\ m))$ out to the positions $r-1$ and r and leaves all other entries of the form $(\mathbf{0};(i\ j))$. As in Part B, Lemma 1 allows us to assume $\gamma^{(1)} = 1$. Lemma 3 allows us to apply $Q^{(3)} \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ to achieve the effect of conjugation by $(2\ m)$. Therefore assume that $\boldsymbol{\sigma}''$ has these properties:

(3.13) (a) $\sigma(i)''$ is of the form $(\mathbf{0};(j\ k))$ (with j and k dependent on i), $i = 1, \dots, r-2$;

(b) the second entries in $\sigma(1)'', \dots, \sigma(r-2)''$ generate S_m; and

(c) $\sigma(r-1)'' = \sigma(r)'' = (1_{12};(1\ 2))$, and therefore $\sigma(1)'' \cdots \sigma(r-2)'' = (\mathbf{0}; 1)$.

PART D. *Application of Proposition* 1. Apply Proposition 1 to $\sigma(1)'', \dots,$ $\sigma(r-2)''$ to find $Q^{(6)} \in \pi_1(\mathsf{P}^{r-2} - D_{r-2}, \mathbf{a}^0)$ and $\gamma \in S_m$ such that

(3.14)
$$(\gamma^{-1} \cdot (\sigma(1)'', \dots, \sigma(r-2)'') \cdot \gamma) Q^{(6)} = ((\mathbf{0}; (1\ 3)), (\mathbf{0}; (1\ 3)), \dots, (\mathbf{0}; (1\ m)), (\mathbf{0}; (1\ m)), (\mathbf{0}; (1\ 2)), \dots, (\mathbf{0}; (1\ 2))).$$

Indeed, Lemma 3 allows us to assume that $\gamma = 1$. With the natural interpretation of $Q^{(6)}$ in $\pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ it is now an easy matter to find $Q^{(7)}$ and apply it to $(\boldsymbol{\sigma}'')Q^{(6)}$, with $\boldsymbol{\sigma}''$ given by (3.13), to get $\boldsymbol{\sigma}'$. This concludes the proof of the theorem. □

Let ${}_o\mathcal{C}_{n,g}$ be the moduli space of cyclic unramified covers of genus g curves as discussed in §1. There is a natural map from the space $\mathcal{H}(\mathbf{C}, G)$ of simple by cyclic sequences of type (m, r, n): the point $\mathfrak{p} \in \mathcal{H}(\mathbf{C}, G)$ represented by the sequence $X' \xrightarrow{\psi} X \xrightarrow{\varphi} \mathsf{P}^1$ of (2.1) goes to the point of ${}_o\mathcal{C}_{n,g}$ that is represented by the cover $X' \xrightarrow{\psi} X$. From the moduli property this map is complex analytic. It is an old argument, repeated, say, in [**Fr1**, §1], that if $m \geq 2g - 1$, every Riemann surface of genus g can be presented as a simple cover of P^1 of degree m. Thus, in this case, the map from $\mathcal{H}(\mathbf{C}, G)$ to ${}_o\mathcal{C}_{n,g}$ is surjective. Connectness of the manifold $\mathcal{H}(\mathbf{C}, G)$ (and of the complement in it of each finite type analytic subset of codimension 1) from Theorem 2 therefore gives the following:

THEOREM 3. *The moduli space* ${}_o\mathcal{C}_{n,g}$ *of cyclic unramified covers of genus* g *curves is irreducible.*

For a given positive integer m, $m(g) = [(g+3)/2]$ is the smallest integer m for which every curve X of genus g has a covering map $\varphi: X \to \mathsf{P}^1$ of degree m [**KL**]. Actually, if m is suitably large compared to g, then the technique of Theorem 3 shows that the irreducibility of the space $\mathcal{H}(\mathbf{C}, G)$ follows from [**DM**, Theorem 5.15]. But Theorem 3 does not give Theorem 2 in the case that $m < [(g+3)/2]$.

Appendix—Proof of Proposition 1. As in the proof of Theorem 2, the proof of Proposition 1 amounts to showing that if $\boldsymbol{\sigma}' \in \mathrm{Ni}(\mathbf{B}, S_m)$ (with r even and of necessity $\geq 2 \cdot (m-1)$), then there exists $\tau \in S_m$ and $Q \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ such that

$$(\text{A.1})\quad (\tau \cdot \boldsymbol{\sigma}' \cdot \tau^{-1})Q = \boldsymbol{\sigma} = ((1\ m), (1\ m), (1\ m-1), (1\ m-1), \dots, (1\ 3), (1\ 3), (1\ 2), \dots, (1\ 2)).$$

Our choice of $\boldsymbol{\sigma}$ is for the sake of efficiency of proof, rather than for it to match the choices in Theorem 2. Furthermore, Lemma 3 allows us to take $\tau = 1$ and even to conjugate by an element of S_m whenever it is desirable.

First note that we can find $Q^{(1)} \in \pi_1(\mathsf{P}^r - D_r, \mathbf{a}^0)$ so that $(\boldsymbol{\sigma}')Q^{(1)} = ((1\ j_1), (1\ j_2), \dots, (1\ j_t), \sigma(t+1)'', \dots, \sigma(r)'') = \boldsymbol{\sigma}''$, where none of $\sigma(t+1)'', \dots, \sigma(r)''$ contain the integer 1. If the integers $j_1, \dots, j_t$ are all distinct, then the product of the first t coordinate entries of $(\boldsymbol{\sigma}')Q^{(1)}$ is $(1\ j_1\ j_2 \cdots j_t)$. It is thus clearly impossible for the products of all coordinate entries $(\boldsymbol{\sigma}')Q^{(1)}$ to be 1.

Without loss we may therefore move the two identical cycles containing 1 together at the beginning to assume that $j_1 = j_2$. There are two possibilities for the group $\mathcal{H}$ generated by $\sigma(3)'', \dots, \sigma(r)''$:

(A.2) (a) $\mathcal{H} = S_m$; or
(b) $\mathcal{H}$ is the subgroup of S_m that fixes either 1 or j_1.

In case (A.2)(a) we assume that $j_1 = 2$. Transfer the first two coordinate entries, unchanged, down to the right-hand side to assume that

$$\boldsymbol{\sigma}'' = (\sigma(1)'', \dots, \sigma(r-2)'', (1\ 2), (1\ 2)).$$

This is now set up for an induction on r: find $Q^{(2)} \in \pi_1(\mathbf{P}^{r-2} - D_{r-2}, \mathbf{a}^0)$ such that $(\sigma(1)'', \dots, \sigma(r-2)'')Q^{(2)}$ is (A.1) with two fewer (1 2) terms on the right-hand side. With an interpretation of $Q^{(2)} \in \pi_1(\mathbf{P}^r - D_r, \boldsymbol{\alpha}^0)$ (as in Part D of the proof of Theorem 2) we are done if (A.2)(a) holds.

If (A.2)(b) holds, assume with no loss that $j_1 = m$ and that $\mathcal{H}$ acts as S_{m-1} on $\{1, 2, \dots, m-1\}$: $\boldsymbol{\sigma}'' = ((1\ m), (1\ m), \sigma(3)'', \dots, \sigma(r)'')$. Again we are set up for an induction on r (with m changed to $m-1$): find $Q^{(3)} \in \pi_1(\mathbf{P}^{r-2} - D_{r-2}, \mathbf{a}^0)$ such that $(\sigma(3)'', \dots, \sigma(r)'')Q^{(3)}$ is (A.1) with the first two terms on the left side missing. Conclude as in case (A.1)(a).

References

[B] A. Beauville, *Prym varieties and Schottky's Problem*, Invent. Math. **41** (1977), 149–196.

[BFr] R. Biggers and M. Fried, *Relations between moduli spaces of covers of $\mathbf{P}^1$ and representations of the Hurwitz monodromy group*, J. Reine Angew. Math. **335** (1982), 87–121.

[C] A. Clebsch, *Zür Theorie der Riemann'schen Fläche*, Math. Ann. **6** (1872), 216–230.

[DM] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Etudes Sci. Publ. Math. No. 36 (1967), 75–100.

[FaBu] E. Fadell and J. Buskirk, *The braid groups of E^2 and S^2*, Duke Math. J. **29** (1962), 243–257.

[Fe] W. Feit and P. Fong, *Rational rigidity of $G_2(p)$ for any prime $p > 5$*, Proc. Rutgers Group Theory 1983–84, edited by D. Gorenstein, R. Lyons, M. O'Nan, C. Sims, M. Aschbacher and W. Feit, Cambridge Univ. Press, 1984, pp. 323–326.

[Fr1] M. Fried, *Fields of definition of function fields and Hurwitz families and groups as Galois groups over* **Q**, Comm. Algebra **5** (1977), 17–86.

[Fr2] ——, *Galois groups and complex multiplication*, Trans. Amer. Math. Soc. **235** (1978), 141–162.

[Fr3] ——, *On reduction of the inverse Galois group problem to simple groups*, Proc. Rutgers Group Theory 1983–84, edited by D. Gorenstein, R. Lyons, M. O'Nan, C. Sims, M. Aschbacher and W. Feit, Cambridge Univ. Press, 1984, pp. 289–301.

[Fu] W. Fulton, *On the irreducibility of the moduli space of curves*, Appendix to the paper of Harris and Mumford, Invent. Math. **67** (1982), 87–88.

[HM] J. Harris and D. Mumford, *On the Kodaira dimension of the moduli space of curves*, Invent. Math. **67** (1982), 23–86.

[Hu] A. Hurwitz, *Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), 1–61.

[KL] S. Kleiman and D. Laksov, *Another proof of the existence of special divisors*, Acta Math. **132** (1974), 163–175.

[Ma] B. H. Matzat, *Realisierung Endlicher Gruppen als Galoisgruppen*, Manuscripta Math. **51** (1985), 253–265.

[Th] J. G. Thompson, *Some finite groups which appear as* Gal(L/K) *where* $K \subseteq Q(\mu_m)$, J. Algebra **89** (1984), 437–499.

[W] A. Weil, *Modules des surfaces de Riemann*, Sém. Bourbaki, 168, 1957–58.

[Wa] J. Walter, *Classical groups as Galois groups*, Proc. Rutgers Group Theory 1983–84, edited by D. Gorenstein, R. Lyons, M. O'Nan, C. Sims, M. Aschbacher and W. Feit, Cambridge Univ. Press, 1984.

DEPARTMENT OF MATHEMATICS, CLARK COLLEGE, ATLANTA, GEORGIA 30314

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, CALIFORNIA 92717