Compositio Mathematica **77**: 95–117, 1991.

On the Hurwitz scheme and its monodromy

DAVID EISENBUD[1], NOAM ELKIES[2], JOE HARRIS[2] and ROBERT SPEISER[3]

[1]*Brandeis University, Waltham MA, 02254, U.S.A.;* [2]*Harvard University, Cambridge MA, 02138, U.S.A.;* [3]*Brigham Young University, Provo UT, 84602, U.S.A.*

Received 14 November 1989; accepted 12 February 1990

Summary

In this paper all varieties will be projective and defined over $\mathbb{C}$. We will prove two results on the Hurwitz scheme of branched coverings of $\mathbb{P}^1$.

The first may be paraphrased by saying that 'maps of a curve to $\mathbb{P}^1$ are usually determined by their branch points.' More precisely, the map $\mathscr{H}_{d,g} \to \mathscr{M}_g \times \mathscr{P}_b$ from the Hurwitz scheme of d-fold coverings of $\mathbb{P}^1$ by a curve of genus g to the product of the moduli space of curves of genus g and the scheme of sets of $b = 2g + 2d - 2$ points of $\mathbb{P}^1$, taking a point in the Hurwitz scheme to the source curve and the set of branch points, is birational onto its image.

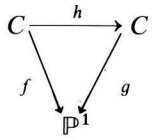
The second concerns the monodromy of the map from the Hurwitz scheme to the space of sets of points in $\mathbb{P}^1$ obtained by associating to each branched covering its branch points: the result 'explains' why for coverings of degrees 3 or 4 this monodromy group is smaller than the full symmetric group by giving a geometric structure to the fiber; in particular, we give a geometric interpretation of a result of Cohen [1974].

Introduction

Let C be a smooth irreducible curve. We say that a map $f: C \to \mathbb{P}^1$ of degree d has *simple branching* if the fiber over each point of $\mathbb{P}^1$ contains at least $d - 1$ points; equivalently, the ramification points of f are all simple and have distinct images (the *branch points*).

THEOREM 1. *Let $f, g: C \to \mathbb{P}^1$ be two coverings of $\mathbb{P}^1$ by a smooth irreducible curve C of genus $\geqslant 1$. Assume that both have simple branching and that the branching occurs over the same set $\Gamma \subset \mathbb{P}^1$. If Γ is sufficiently general, then f and g are the same in the sense that there is an automorphism h making the following*

diagram commutative:



Here is a more sophisticated statement of the Theorem:

COROLLARY 2. *Let $\mathscr{H}_{d,g}$ be the Hurwitz scheme of degree d branched covers of $\mathbb{P}^1$ by curves of genus $g \geqslant 1$, and let $\mathscr{P}_b$ be the moduli space of b-pointed rational curves with $b = 2d - 2 + 2g$. The natural map*

$$\mathscr{H}_{d,g} \to \mathscr{M}_g \times \mathscr{P}_b$$

sending each branched cover $C \to \mathbb{P}^1$ to the isomorphism type of C and the position of the branch points is birational onto its image. □

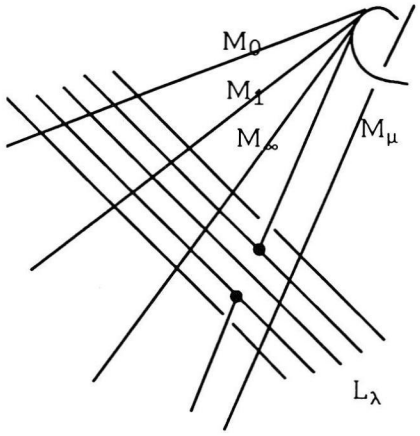
Note that since the assertion of the Corollary is birational, we do not need to worry about the part of $\mathscr{H}_{d,g}$ where the branching is not simple.

We were first led to investigate this subject because of work of Kleiman and Speiser on Tyrrell's conjecture that the 40 elliptic curves tangent to 6 general concurrent lines in the plane are pairwise nonisomorphic. It turns out that these 40 curves correspond to the 40 sheets of the map $\mathscr{H}_{3,1} \to \mathscr{P}_6$, so that the theorem implies this conjecture. The connection is made explicit in the third section, below.

In the last section of the paper we present some geometric results on the monodromy of the covering $\mathscr{H}_{d,g} \to \mathscr{P}_b$. Cohen [1974] has shown that in the case $d = 3$ this group is a symplectic group (see Kluitmann [1988] for a generalization.) We give a geometric interpretation of his result, showing that the bilinear form preserved is an avatar of the Weil pairing, and we extend these ideas to the case $d = 4$ as well. In the case $d = 4$, our result explains and makes more precise a remark of Maclachlan [1978, last paragraph].

Theorem 1 is the more surprising because it fails in case $C \cong \mathbb{P}^1$, even for coverings of degree 3: In this case there are 4 ramification points and 4 branch points, and the statement of the theorem with $C = \mathbb{P}^1$ would say that the cross ratio of the branch points (in some chosen order) determines the cross ratio of the ramification points in the corresponding order. We claim however that the association of ramification point cross ratios and branch point cross ratios is a correspondence of type 4,2 from $\mathbb{P}^1$ to $\mathbb{P}^1$, so that to almost every branch point cross ratio there correspond at least 2 distinct ramification point cross ratios.

To see this, regard maps from $\mathbb{P}^1$ to $\mathbb{P}^1$ of degree 3 as projections of a fixed twisted cubic in $\mathbb{P}^3$ from lines. If we fix 3 points on the twisted cubic, then the



projections with these 3 points as ramification points correspond to the lines meeting the three tangent lines M_0, M_1, M_∞ to the twisted cubic at the 3 given points. Let Q be the quadric containing the 3 given tangent lines as lines of one ruling $\{M_\mu \mid \mu \in \mathbb{P}^1\}$; the lines in $\mathbb{P}^3$ meeting all 3 tangent lines are precisely the lines $\{L_\lambda \mid \lambda \in \mathbb{P}^1\}$ in the other ruling of Q. Any 4th tangent line of the twisted cubic, corresponding to a value of the ramification point cross ratio, will intersect Q in 2 points which in general lie on distinct L_λ; thus there are in general two maps with given ramification point cross ratios. On the other hand, if we project from one of the L_λ then the points of the image $\mathbb{P}^1$ correspond to the lines M_μ. Thus μ is the cross ratio of the branch points of the map corresponding to L_λ iff the plane spanned by L_λ and M_μ is tangent to the twisted cubic. But there are exactly 4 planes containing M_μ which are tangent to the twisted cubic (they correspond to the ramification points of the twisted cubic under projection from M_μ), so there are 4 values of λ for which the branch point cross ratio is μ, as claimed.

We can make this example even more explicit: every triple branched cover is given by a rational function of the form

$$f_t(x) = x^2(x - t)/((2t + 3)x - t - 2)$$

for some number t. For every t, this function sends 0, 1, ∞ to 0, 1, ∞, and is ramified at these three points and at a fourth point

$$x = -(t^2 + 2t)/(2t + 3),$$

which is thus the cross ratio of the ramification points. The map

$$t \mapsto (\text{ramification point cross-ratio of } f_t,\ \text{branch point cross-ratio of } f_t)$$

is a map of type 2,4 as is shown above, and is actually birational onto its image in $\mathbb{P}^1 \times \mathbb{P}^1$; for example, the two values of t for which the map is ramified at -1 are $\pm 3^{1/2}$, and the corresponding ramification points are distinct. Thus the t-line is actually the moduli space for the space of triple covers. The image curve in $\mathbb{P}^1 \times \mathbb{P}^1$ has 3 ordinary nodes at $(0, 0)$, $(1, 1)$ and (∞, ∞) as one shows by checking that each of these points has two distinct preimages in the t-line. Since its arithmetic genus is 3, these are its only singularities.

The theorem also fails for higher genus if the position of the branch points is not assumed general; an example is given at the end of section 2.

REMARK. The Theorem was previously known in the case where $\dim \mathscr{H}_{d,g} < \dim \mathscr{M}_g$, that is, when $d < (g-1)/2$. In this case Arbarello and Cornalba [1981] have shown that the map $\mathscr{H}_{d,g} \to \mathscr{M}_g$ is generically one to one; that is, the generic curve possessing a map to $\mathbb{P}^1$ of degree $d < (g-1)/2$ has a unique such, and of course Theorem 1 follows.

Here are some appealing open problems in the area:

First, though Theorem 1 is stated in characteristic 0, and the proof is very tightly tied to characteristic 0 techniques, we know no reason to think that the result doesn't hold in arbitrary characteristic. In any case, it would be very nice to have an algebraic proof.

It seems reasonable to hope that Theorem 1 still holds if $\mathbb{P}^1$ is replaced by an arbitrary curve D, at least if a little caution is exercised (for example, in a map from one elliptic curve to another there are no branch points, so the 'general position of the branch points' doesn't help much.) There are so few maps between curves of higher genus that the Theorem ought in some sense to be easier in that setting.

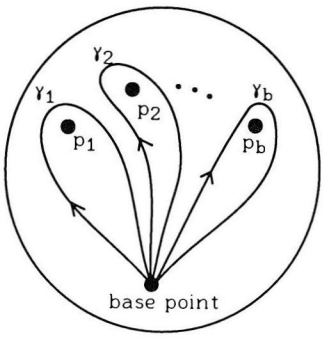
Perhaps most interesting is the problem raised in the last section of determining the monodromy groups of the Hurwitz scheme.

In the first section below we will review the (hoary) construction of curves as branched covers, and explain what happens to the stable model of the curve and branched cover as two branch points come together in the case of simple branching.

The second section is devoted to the proof of Theorem 1. In the third section of the paper we explain the connection of our work with Tyrrell's conjecture. The fourth section is devoted to the geometric structure of the fibers of the Hurwitz schemes of 3 and 4-sheeted coverings.

1. *Review of branched covers of* $\mathbb{P}^1$

The technique we will use is based on the Riemann existence Theorem, which we will now review. Suppose we are given a 'bouquet' of $b = 2d + 2g - 2$ oriented simple disjoint paths $\gamma_1, \ldots, \gamma_b$ on $\mathbb{P}^1$ starting at a given base point and encircling marked points $p_1, \ldots, p_b$:



If $\varphi_1, \ldots, \varphi_b$ are permutations of d letters such that:

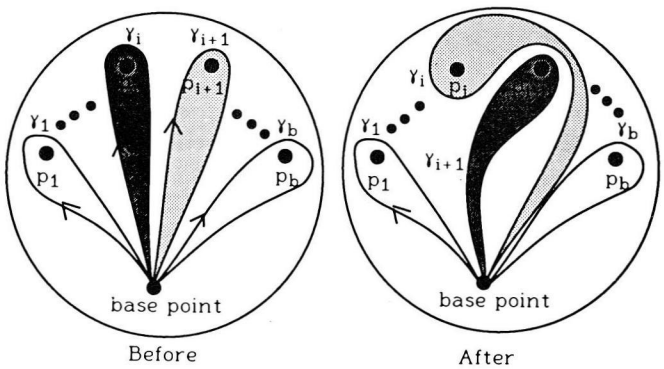
1. The product $\varphi_1 \cdots \varphi_b = 1$ in the symmetric group;

and

2. $\varphi_1, \ldots, \varphi_b$ generate a transitive subgroup of the symmetric group,

then there is a unique d-sheeted covering of $\mathbb{P}^1$, branched only over $p_1, \ldots, p_b$ with a labeling of the fiber over the base point, such that the monodromy around the path γ_i is the permutation φ_i of the sheets. We will call the data consisting of the p_i, γ_i and φ_i, together with the base point and the labeling of the sheets over it, a set of *branch data* for the covering. The covering itself may easily be reconstructed from the branch data as an analytic 1-manifold: one simply takes a disjoint union of d copies of the exterior of the region in the 2-sphere $\mathbb{P}^1$ bounded by the paths γ_i, and joins them with 'local plumbing fixtures' over the disks bounded by the γ_i; the local plumbing fixture for γ_i is obtained by decomposing φ_i into disjoint cycles, and taking the disjoint union of a disk for each cycle, where the map on the disk corresponding to an n-cycle is $z \mapsto z^n$.

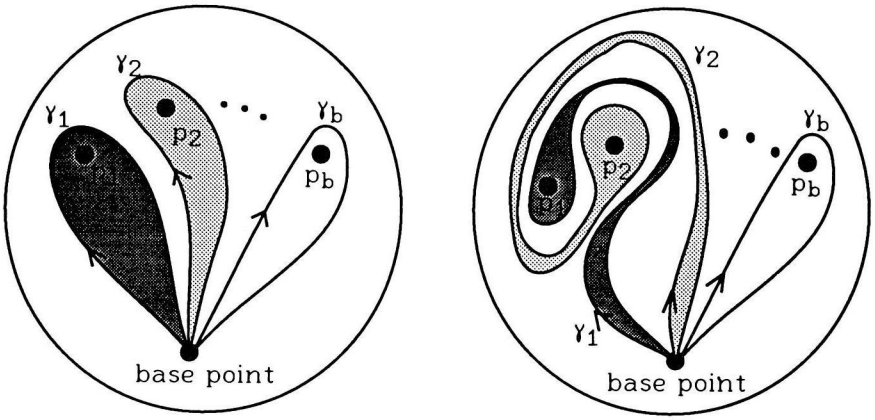
The permutations φ_i are not uniquely determined by the positions of the p_i, but depend on how the paths γ_i are chosen. Thus for example if we change the ith and $i+1$st paths as in the following pictures



it is easy to see that all the permutations but the ith are unaffected, while the ith changes to $\varphi_{i+1}^{-1}\varphi_i\varphi_{i+1}$, the conjugation of the old ith permutation by the $i+1$st. Such changes define an action of the braid group on n letters on the set of branch data associated to the given covering. Clebsch [1872], pp. 224–225, proved that by applying a suitable element of this group one can arrange the covering data in the form

$$\varphi_1, \ldots, \varphi_b = (1, 2), (1, 2), \ldots, (1, 2), (1, 2), (2, 3), (2, 3), (3, 4), (3, 4), \ldots, (d-1, d), (d-1, d).$$

(or indeed in any of a wide range of related forms) where the first transposition (12) occurs $2g+2$ times at the beginning and the other $(i, i+1)$ each occur twice, in order. (Note that the group generated by the φ_i, the monodromy group of the cover, is an invariant; but a transitive subgroup generated by transpositions must be the full symmetric group, so this invariant does not provide any obstruction.) He further proved that the same form could be achieved after any given relabeling of the points b_i; this amounts to saying that the given form can be achieved by an element of the 'pure braid group', the subgroup of the braid group consisting of those elements that induce the identity permutation of the strands. (A typical element of the pure braid group can be pictured as producing the following transformation of the diagram:



the effect is to replace φ_1 and φ_2 by their conjugates under the product $\varphi_1\varphi_2$.) A stronger version of Clebsch's result may also be found in Kluitmann [1988], but Clebsch's beautiful exposition, and also the subsequent wider-ranging one of Hurwitz [1891] are still well worth reading today.

One may also interpret Clebsch's theorem as saying that any covering of $\mathbb{P}^1$, branched in a given set of points p_i, can be brought into any other by a suitable

motion of the points (here the braid action is clear!) Thus it implies that the *Hurwitz scheme* $\mathscr{H}_{d,g}$ of all degree d branched covers of $\mathbb{P}^1$ by a curve of genus g with simple branching is irreducible.

Of course, once we know that the Hurwitz scheme is irreducible, we see that any list of $d + g - 1$ pairs of copies of transpositions

$$(a_1, b_1), (a_1, b_1), (a_2, b_2), (a_2, b_2), \ldots,$$
$$(a_{d+g-1}, b_{d+g-1}), (a_{d+g-1}, b_{d+g-1})$$

such that (a_i, b_i) generate a transitive subgroup satisfies conditions 1 and 2, and thus can serve as a normal form.

All the information above is quite standard. A little less standard is the information about the stable limit of the coverings produced when two of the branch points p_1 and p_2 are brought together, which we now explain:

Let $\mathscr{P}_b$ be the space of b-tuples of distinct ordered points in $\mathbb{P}^1$. Let $\mathscr{H} = \mathscr{H}_{d,g}$ be the Hurwitz scheme over $\mathscr{P}_b$, and let

$$\begin{array}{ccc} \mathscr{C} & \subset & \mathscr{H} \times \mathbb{P}^1 \\ & \searrow \quad \swarrow & \\ & \mathscr{H} & \\ & \downarrow & \\ & \mathscr{P}_b & \end{array}$$

be the universal family of branched covers. The family $\mathscr{C} \to \mathscr{H}$ induces a map $r: \mathscr{H} \to \mathscr{M}_g$ sending each cover to the isomorphism class of the curve on which it is defined.

What we need is some information on what happens to a curve simply branched in a given way over a set of points Γ as two of the points of Γ are brought together. The situation in general is rather complex, (see for example the paper of Harris and Morrison [1989] for general information about these limits) but the following will suffice for our purposes:

LEMMA 3. *Suppose that* $\{C_t \to \mathbb{P}^1\}_{t>0}$ *is a real analytic arc in the family of branched covers with simple branching over the b-tuple of distinct points* Γ_t. *If* $p_{1,t}$ *and* $p_{2,t}$ *in* Γ_t *approach each other as* $t \to 0$, *but the other points of* Γ_t *remain distinct, then*

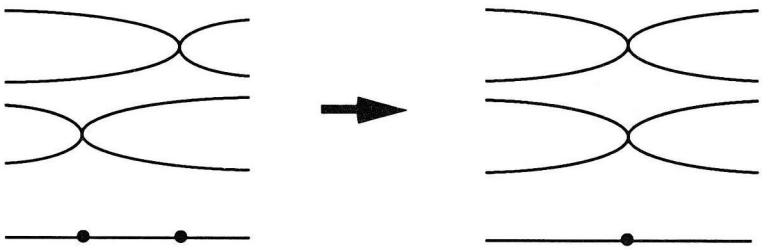
(a) *If the permutations associated to* $p_{1,t}$ *and* $p_{2,t}$ *in the branch data for* C_t *are not equal* (*this is independent of* t *so long as* $t \neq 0$), *then the stable limit of the family of curves* C_t *is a smooth curve.*

(b) *If the permutations associated to* $p_{1,t}$ *and* $p_{2,t}$ *are equal, then the stable limit of the family* C_t *is both irreducible and singular* (*necessarily an irreducible curve*

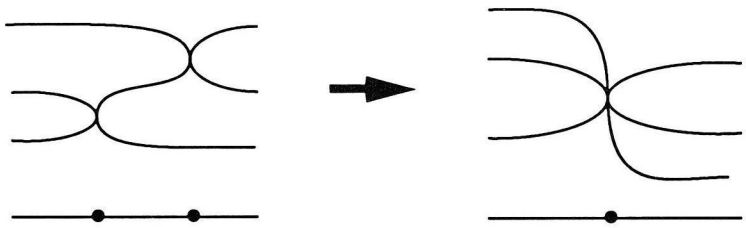
with one node) iff the permutations associated to the points other than p_1 and p_2 generate a transitive permutation group of the sheets.

REMARK. Let $\{\sigma_i\}$ be the transpositions in the branching data for C_t which are associated to the points other than $p_{1,t}$ and $p_{2,t}$. Consider the case not treated by Lemma 3, where the $\{\sigma_i\}$ generate a proper subgroup of the symmetric group on Γ. In this case the group generated by $\{\sigma_i\}$ has precisely two orbits (since adding a transposition makes it transitive), and in fact since all the σ_i are transpositions, it is the product of the full symmetric groups on the two orbits. Suppose that the orbits are of sizes a and b, so that the group is $S_a \times S_b$. Suppose that exactly $2a - 2 + \alpha$ of the transpositions σ_i belong to S_a. One can prove by the same method as that below that in this case C_t approaches a limit which is the union of a curve of genus α and a curve of genus $g - \alpha$, meeting transversely in a node; thus for example the stable limit is nonsingular iff $\alpha = 0$ or g.

Proof. The problem is local to the common limit point p of $p_{1,t}$ and $p_{2,t}$ on the base $\mathbb{P}^1$, and to the (at most 4) sheets affected by the transpositions τ_1 and τ_2 associated to $p_{1,t}$ and $p_{2,t}$ in some chosen branching data for C_t. If τ_1 and τ_2 are disjoint transpositions then the family has the form

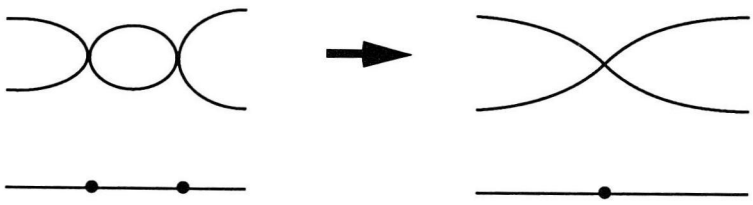


and it is clear that the limiting curve is nonsingular. If τ_1 and τ_2 have just one sheet in common, then we can find local analytic coordinates in the source and target so that the family is given by $z^3 - tz - x = 0$, projected to the x-axis. As t goes to 0, this looks like



As one sees from the local equation, the three sheets form a nonsingular disk in the limit.

Finally, if $\tau_1 = \tau_2$ then we may take the family $z^2 - (t - x^2) = 0$ as the local family; this is singular at $t = 0$:



In the limit, we see that there is no monodromy around p; thus if the remaining transpositions do not act transitively, then the curve splits into two components, necessarily joined at the node; since this curve will not be stable if one of the components is rational, we cannot immediately decide whether the stable limit is singular. However, if the remaining transpositions act transitively, then the curve remains irreducible, and therefore stable, so that it is its own stable model. This completes the proof. □

2. *Proof of Theorem* 1

We first explain how we use the assumption that Γ is general: the set of points $\Gamma \in \mathscr{P}_b$ such that 2 distinct points of the fiber of $\mathscr{H}$ over Γ go to the same point of $\bar{\mathscr{M}}_g$ is evidently closed; if the Theorem were false then it would contain a dense set, and thus be all of $\mathscr{P}_b$. By our description of $\mathscr{H}$ above in terms of branching data we see that $\mathscr{H}$ is unramified over $\mathscr{P}_b$. Thus if the theorem failed we could find a curve $C = C_0$ and two branched covers $f_0, g_0 : C_0 \to \mathbb{P}^1$ with simple branching over a general branch divisor Γ_0, as in Theorem 1, having the following property: For any path Γ_t starting from Γ_0 in $\mathscr{P}_b$ we can find a family $f_t, g_t : C_t \to \mathbb{P}^1$ of pairs of branched covers starting from the given pair. Because stable limits of curves are unique, this is still true if two points in the branch set come together at the terminal point of the path (in general we would have to blow up the family of $\mathbb{P}^1$'s that are the targets for the branched covers, but in the situations considered below this will never be necessary.) Thus *because* Γ *is chosen generally* it is possible to cover an arbitrary motion of Γ in an open subset of $\mathscr{P}_b$ by a motion of C together with the pair of maps from C to $\mathbb{P}^1$ branched over Γ. In particular, we can meaningfully speak of the 'limits of $f, g : C \to \mathbb{P}^1$ as p_1 and p_2 are brought together'; of course these limits will depend on the path along which p_1 and p_2 are brought together.

To prove the Theorem, we may assume by the remarks in section 1 that the branch data for the covering f are given by the sequence of permutations

$$\begin{aligned}&\varphi_1, \ldots, \varphi_b\\ &\quad = (12), (12), \ldots, (12), (12), (23), (23), (34), (34), \ldots, (d, 1), (d, 1)\\ &\quad = \sigma_1, \sigma_1, \ldots, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \ldots, \sigma_d, \sigma_d.\end{aligned}$$

The first 2 (genus C) of these permutations are equal to $\sigma_1 = (12)$, and each of the others is repeated exactly twice.

Let $\psi_1, \ldots, \psi_b$ be the branch data for g. We will prove that if the points of Γ are general, then the branch data of g are the same as the branch data of f up to relabeling the sheets of the covering.

Since $\varphi_{2i-1} = \varphi_{2i}$ and the other φ_j generate a transitive group, we must have $\psi_{2i-1} = \psi_{2i}$ and the other ψ_j generate a transitive group by Lemma 3; else the curve C would move in a family with two distinct stable limits as p_{2i-1} and p_{2i} are brought together. Similarly, we must have $\psi_1 = \psi_2 = \cdots = \psi_{2(\text{genus } C)}$, so that the branch data for g may be written as

$$\psi_1, \ldots, \psi_b = \tau_1, \tau_1, \ldots, \tau_1, \tau_1, \tau_2, \tau_2, \ldots, \tau_d, \tau_d.$$

Because the subset

$$\tau_1, \tau_2, \ldots, \hat{\tau}_i, \ldots, \tau_d$$

obtained by leaving out τ_i generates a transitive group of permutations, we see that the letters interchanged by τ_i must also be moved by other τ_j; thus each of the d letters occurs in at least two of the τ_i. Since there are only d permutations τ_i it follows that each letter occurs in precisely two.

We next use Lemma 3 in a more subtle way to show that τ_i does not commute with τ_{i+1} (interpreting i modulo $d + 1$, the argument also shows that τ_d does not commute with τ_1). Choose an $i \geqslant 2(\text{genus } C)$, and consider a path in $\mathscr{P}_b$ starting from $\Gamma = \{p_1, \ldots, p_b\}$ which begins by moving p_{2i+1} in a loop around p_{2i} (but no other p_j) and back to its starting point, and then brings p_{2i} and p_{2i-1} together. Considering the branch data of the cover f, we see that after the first part of the motion φ_{2i} is replaced by the permutation $(i, i + 2)$, while $\varphi_{2i-1} = (i - 1, i)$ is unchanged. Thus by Lemma 3a the limit of C at the end of the motion is a nonsingular curve. Now consider the limit from the point of view of the branch data of g. If τ_i and τ_{i+1} commute, then the inital part of the motion does not change g and its branch data at all, and thus the total motion would have as its limit a singular curve. This contradiction shows that τ_i and τ_{i+1} do not commute.

We can now show combinatorially that the τ_i and the σ_i differ only by a relabeling of the sheets. Suppose that after a relabeling we have arranged that, for some $j \geqslant 1$,

$$\tau_1, \ldots, \tau_j = (1, 2), \ldots, (j, j+1),$$

and consider τ_{j+1}. Since τ_{j+1} is a transposition and does not commute with τ_j, they must share exactly one letter. Since every letter occurs among the τ_i exactly twice, this shared letter must be $j+1$ (or, in case $j = 1$, may be taken to be so after relabeling.) The other letter involved in τ_{j+1} must be either 1 or some new letter which can be taken by relabeling to be $j+2$. In the latter case we may proceed with our induction. In the former case, $\tau_1, \ldots, \tau_{j+1}$ involves each of the letters $1, \ldots, j+1$ exactly twice, so these letters do not occur in any τ_i other than these. If $j+1 < d$ then the group generated by all the τ_i would not be transitive, contradicting the description of branch data. Thus $j+1 = d$ and $\tau_1, \ldots, \tau_j = (1,2), \ldots, (d-1, d), (d, 1)$ as required. This finishes the proof. □

We next sketch an alternative proof that works only in the case where the genus of C is >1, but contains a nice geometric idea:

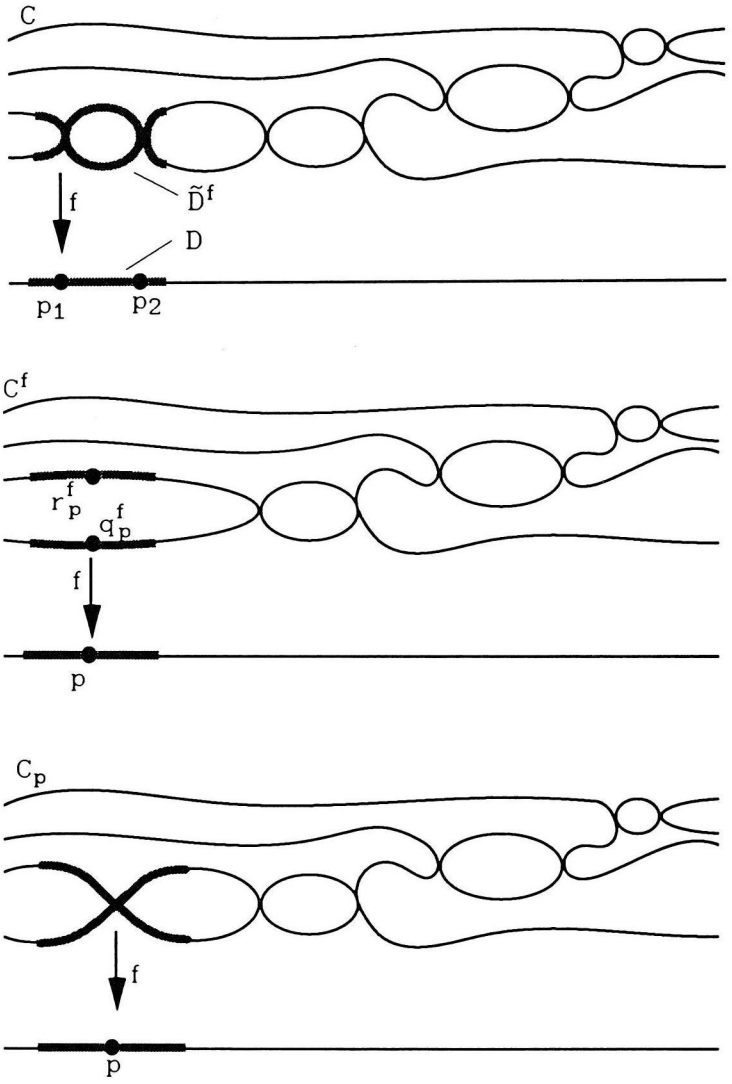
Suppose that genus $C > 1$, and that the branch data of f take the form

$$\varphi_1, \ldots, \varphi_b = (1,2), (1,2), \ldots, (1,2), (1,2), (2,3), (2,3), (3,4), (3,4), \ldots, (d-1, d), (d-1, d).$$

As before it follows from Lemma 3b that if $\psi_1, \ldots, \psi_b$ are the branch data of the covering g, then $\psi_1 = \psi_2$ and the rest of the ψ_j act transitively on the sheets.

Let D be a disk in $\mathbb{P}^1$ which contains p_1 and p_2 but no other p_i, and let Δ be the diagonal in $D \times D$. Because $\varphi_1 = \varphi_2$ and $\psi_1 = \psi_2$ there is no monodromy in the family of C, f, g obtained by moving p_1 and p_2 in D. Thus there is a family $\mathscr{C} \to D \times D$, whose fibers over Δ are singular curves with one node, and a family of ramified covers f, g defined on the fibers of $\mathscr{C}$ extending the given pair of ramified covers on C, such that on the fiber over $q_1 \times q_2 \in D \times D - \Delta$, the covers f, g are branched over $q_1, q_2, p_3, \ldots, p_b$. (This family may be described explicitly as the one obtained by gluing in the plumbing fixture defined, as a covering of the x-line branched over the points $t_1, t_2 \in D \times D$, by the local equation $z^2 - (x - t_1)(x - t_2)$.) To describe the fiber C_p of $\mathscr{C}$ over a point p of Δ, let C^f be the curve obtained from C by removing the preimage $\tilde{D}^f$ of D under f in sheets 1 and 2 and replacing it with two disjoint disks in such a way that the map f extends to C^f; this is possible because the monodromy transformations of f over p_1 and p_2 are both given by the permutation $(1, 2)$, so that around the boundary of D there is no monodromy. We abuse notation and write f for the maps on C^f and on the C_p which agree with f away from $\tilde{D}^f$, and similarly with g. The fiber

C_p is then the curve obtained from C^f by identifying the points q_p^f, r_p^f in sheets 1 and 2 over p, as in the following pictures:



Of course the corresponding construction can also be made using g. Since the isomorphism class of C_p is independent of which construction is used, we see that for each p there is an isomorphism $h_p: C^f \to C^g$ taking the unordered pair $\{q_p^f, r_p^f\}$ to the unordered pair $\{q_p^g, r_p^g\}$.

Suppose that one of the h_p, say h, takes q_p^f to q_p^g or r_p^g for infinitely many values of p. It follows that $gh = f$ on an infinite subset of C^f, so they are equal

everywhere on C^f. But C^f agrees with C outside of a pair of disks, and these disks are identified with the corresponding disks of C^g by h. Since C can be reconstructed from either one of C^f and C^g by replacing these disks by isomorphic 'plumbing fixtures' $\tilde{D}^f$ and $\tilde{D}^g$, we may restrict the isomorphism h_0 to C^f minus these two disks, and extend it again to an automorphism h of C — it extends without difficulty because the map h respects the identifications of C^f and C^g with the base $\mathbb{P}^1$ near the boundaries of the disks. Since $gh = f$ on the open subset of C coming from C^f, we see that $gh = f$ everywhere on C, and the theorem is proved.

If the genus of C^f is at least 2, then the automorphism group of C^f is finite, so one of the h_p takes q_p^f to q_p^g or r_p^g for infinitely many values of p, as required. If the genus of C^f is only 1 (that is, the genus of C is 2), then a further argument is necessary, which we omit.

EXAMPLE. If the points of Γ are not in general position, then the Theorem fails. For example, consider the elliptic curve E defined as the 4-fold covering of $\mathbb{P}^1$ branched over the points $a, -a, b, c, -b, -c, d, -d \in \mathbb{A}^1$ with branching data

B_1: (12), (12), (23), (23), (34), (34), (41), (41).

Composing with the automorphism -1 on $\mathbb{A}^1$, we see that this is isomorphic to the curve with branching data

B_2: (12), (12), (34), (34), (23), (23), (41), (41);

however, it can be shown that B_1 and B_2 are not equivalent under relabeling of sheets, so that there is no commutative diagram as in Theorem 1.

Of course in this example the two coverings differ by an automorphism of $\mathbb{P}^1$, but this is not always the case. Indeed, the map $\mathscr{H}_{d,1} \to \mathscr{P}_b \times \mathscr{M}_1$ has image of codimension 1; as soon as the image is singular, as in the example above, it must be singular in codimension 2 in $\mathscr{P}_b \times \mathscr{M}_1$ and thus the preimage of the singular set is of codimension 1 in $\mathscr{H}_{d,1}$. If 2 branches meet at some points of the singular set in the image, then this will be so on a dense subset of a component of the singular set of the image, so there are pairs of codimension 1 loci in $\mathscr{H}_{d,1}$ which are identified to one another in the image. These loci are of course precisely maps not determined by their branch loci! On the other hand the locus in $\mathscr{P}_b$ consisting of b-tuples of points permuted by a nontrivial automorphism of $\mathbb{P}^1$ is of codimension >1 in $\mathscr{P}_b$ for $b \geqslant 7$. Thus for example there are elliptic curves that can be expressed as branched covers of $\mathbb{P}^1$ of degree 4 in two different ways having the same branch set, even if the branch set is not permuted by any nontrivial automorphism of $\mathbb{P}^1$.

3. *Tyrrell's conjecture*

Choose a point $x \in \mathbf{P}^2$ and choose 6 general lines, $L_1, \ldots, L_6$ through p. The family of plane cubics tangent to all the L_i is parametrized by a closed 3-fold, denoted T, in the $\mathbf{P}^9$ of plane cubics. Denote by E the open subscheme of $\mathbf{P}^9$ parametrizing the nonsingular plane cubics; we have a map

$$E \xrightarrow{j} \mathbf{A}^1,$$

which associates to each elliptic curve its j-invariant.

We now show that j is constant, where defined, on each irreducibile component of T. Indeed, as Tyrrell explains [1973], following Cayley [1868], we choose homogeneous coordinates so that $p = (0, 0, 1)$, and suppose that

$$F(x, y, z) = 0$$

is the equation of a smooth cubic off p, tangent to the L_i. Then, for constants α, β and γ, the equation

$$F(x, y, \alpha x + \beta y + \gamma z) = 0$$

also defines a smooth cubic tangent to the 6 lines. Varying α, β and γ, we obtain an irreducible 3-parameter family, that is, a component of T. The curves in this irreducible family are all isomorphic, so they all have the same value of j.

Having checked that j is constant on each component of T, Tyrrell showed that the number of components of T is the number of ways a binary sextic (the discriminant, on $\mathbf{P}^1$, of the projection from p of a smooth cubic off p, tangent to the 6 lines) can be written as the sum of a square and a cube. Tyrrell then observed that this number is 40, citing a result of Clebsch [1869] on the invariants of binary forms. Tyrrell then gave a new proof of Clebsch's result, using enumerative techniques.

Another proof that there are 40 components follows from the combinatorial description of branched covers, which we have sketched above. This description is also due to Clebsch [1872], although Tyrrell does not mention it. In our situation, the branch data of any triple cover, simply ramified over 6 given points of $\mathbf{P}^1$, can be brought into a unique normal form, beginning with the transposition (12), taken one or more times, followed by (13). This branch data consists of 6 transpositions, the last one uniquely determined by the requirement that the product of the 6 must be the identity. Distinguishing cases on the basis of how many times (12) appears, we immediately find $27 + 9 + 3 + 1 = 40$ possibilities.

Further, let

$$C \xrightarrow{f} \mathbf{P}^1$$

denote any one of these, and write $\mathscr{L}$ for $f^*\mathcal{O}_{\mathbf{P}^2}(1)$. The projection f corresponds to a 2-dimensional linear subspace

$$V \subset \Gamma(C, \mathscr{L}).$$

Choosing appropriate coordinates, C embeds in the plane $\mathbf{P}^2 = P(\Gamma(C, \mathscr{L}))$, such that the inclusion of V defines a projection from the center p to the line $\mathbf{P}^1 = P(V)$, with the given branch points. In other words, C is tangent to the 6 lines L_i from p to the branch points, and C is off p. This construction shows that a representative of each of the 40 classes of abstract covers branched at the 6 given points appears in the 3-parameter family parametrized by T. Conversely, any smooth cubic C, off p, tangent to the L_i, gives a branched cover, via the projection from p. It follows that there are 40 components.

Having checked that there are 40 components, Tyrrell conjectured the following statement.

THEOREM 4. (Tyrrell's Conjecture). *For general concurrent lines* $L_1, \ldots, L_6$, *the* 40 *components of* T *determine* 40 *distinct values of* j.

Proof. This follows immediately from Corollary 2, with $g = 1$ and $b = 6$, because the L_i, hence the given branch points on $\mathbf{P}^1$, are general.

Theorem 4 has an interesting further interpretation, which motivated Tyrrell to make his conjecture. The sextics in the dual plane $\check{\mathbf{P}}^2$ are parametrized by a $\mathbf{P}^{27}$. We denote by Γ the closure, in $\mathbf{P}^9 \times \mathbf{P}^{27}$, of the correspondence which associates to each smooth plane cubic its dual sextic. As Tyrrell observed, the components of T correspond canonically to the branches of Γ through the pullback of the Veronese surface $V \subset \mathbf{P}^9$ parametrizing the triple lines in $\mathbf{P}^2$. Indeed, it was known classically that when a smooth cubic degenerates to a triple line, the dual sextic degenerates to a union of 6 lines through the point in $\check{\mathbf{P}}^2$ dual to the tripled line. We can view the corresponding point of Γ as a triple line equipped with 6 unordered points, called *vertices.*

Given a triple line with 6 general vertices, it is in fact easy to construct a degeneration which realizes it as a point of Γ. Indeed, choose a point p off the triple line, and join it to the vertices with lines $L_1, \ldots, L_6$. Choose a smooth cubic C, tangent to the 6 lines, and move it toward the triple line through a family of linear transformations which hold p fixed and fix the tripled line pointwise. The dual sextic then degenerates to the union of the lines dual to the vertices. (For more details, consult Kleiman-Speiser [1990].)

It was also known classically (by Maillard [1871] for example, see Kleiman-Speiser [1990]) that Γ has 40 branches over the pullback of the Veronese. Because the normalization $n(\Gamma)$ can be viewed as a compactification of E, we can define j as a rational map on $n(\Gamma)$. By normality, j is defined except perhaps on a subvariety of codimension $\geqslant 2$ on $n(\Gamma)$. The pullback of V, however, has codimension 1, so each branch of Γ, over a general point of V, has a well-defined limiting value of j. The explicit degenerations above, together with Theorem 4, give the following result.

COROLLARY 5. *The j-invariant separates the branches of* Γ *over a general point of V.*

The parameter space E is a very simple kind of Severi variety, in the sense of Diaz-Harris [1989]. Compactifying it by associating the dual curve and the moduli point, we obtain a variety which is nonsingular in codimension 1, and is thus suitable for enumerative geometry. In Kleiman-Speiser [1990], the characteristic numbers for smooth plane cubics were found using a natural open subscheme, denoted by **E**, of $n(\Gamma)$ to parametrize the smooth plane cubics, their duals, and their most general degenerations. The choice of **E**, by what we have shown, reflects the basic principle that to understand families of plane curves, we should study them not only in the plane, but also in moduli.

4. *Some remarks on monodromy of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$

In this section we study the monodromy of the map $\mathscr{H}_{d,g} \to \mathscr{P}_b$. Recall that we have defined $\mathscr{P}_b$ to be the set of ordered b-tuples of distinct points of $\mathbb{P}^1$, so that the fundamental group of the base is the pure braid group; it is a classical, largely unsolved problem to know its image G_0, the monodromy group, in the group of permutations of the fiber. By taking the branch points unordered, we also get a monodromy map of the full braid group to the group of permutations of a fiber; we write G for its image.

It is easy to see that G_0 is always contained in the alternating group, since its action is generated by elements of order 3, as one can check from the description given in the first section above. But aside from this we do not know any general restrictions.

However, the numbers of sheets of the map $\mathscr{H}_{d,g} \to \mathscr{P}_b$ are already interesting for small d. They were computed for $d \leqslant 6$ by Hurwitz [1891, p. 18] as being (with $b = 2g + 2d - 2$, the number of branch points):

d	*number of sheets of the cover* $\mathscr{H}_{d,g} \to \mathscr{P}_b$
2	1
3	$(3^{2(g+1)} - 1)/2$
4	$(2^{2(g+1)} - 1)(3^{2(g+2)} - 1)/2$

5	$10^b/7200 - 6^b/288 + 5^b/450 - 4^b/72 + 3^b/18 + 2^b/12 - 5/9$
6	$15^b/(2)(360)^2 - 10^b/7200 + 9^b/(2)(72)^2 - 7^b/(2)(24)^2$ $+ 6^b(7)/(2)(36)^2 - 5^b/360 + 4^b/36 - 3^b(19)/324 - 2^b(19)/144$ $+ 727/1152$

Now $(3^n - 1)/2$ is the number of points in the projective space of dimension $n - 1$ over the field of 3 elements, while $2^n - 1$ is the number of points in a projective space over a field of 2 elements. Thus if d is 3 or 4 one might hope that the fibers of the Hurwitz scheme could be given some corresponding geometric structure, which would lead to a restriction on the transformations in the monodromy group. Indeed, in the case $d = 3$ Cohen [1974, p. 502] (see also Kluitmann [1988 Theorem 6. iv case $\Phi = 1$]) has shown by combinatorial methods that G is isomorphic to the projective symplectic group over the field F_3 of 3 elements, $\mathrm{PSp}(2(g + 1), F_3)$, reinforcing this idea. For $d = 4$, Maclachlan [1978, last paragraph] remarks that the monodromy group should at least be a wreath product with quotient group a similar symplectic group. On the other hand, for $d > 4$ no such structure is apparent.

In the next result we 'explain' the numbers of triple and 4-fold covers: we give the set of triple covers a geometrically natural structure of a projective space on a vector space over the field of 3 elements, and we show that the set of 4-fold covers naturally maps to such a projective space, the fiber acquiring the structure of a projective space on a vector space over the field with 2 elements. Furthermore, these vector spaces support natural skew-symmetric forms (coming from the Weil pairings), which further limit the monodromy:

THEOREM 6. *Fix a point* $\Gamma \in \mathscr{P}_b$, $(b = 2g + 2d - 2)$ *and let* C_0 *be the* (*unique*) *double cover of* $\mathbb{P}^1$ *branched over the points of* Γ.

(1) *If* $d = 3$ *then the fiber of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$ *over* Γ *is in one-to-one correspondence with the projective space associated to the* F_3*-vector space of* 3*-torsion elements of the Picard group of* C_0. *The monodromy group* G *of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$ *preserves the Weil pairing on this vector space, and thus is a subgroup of* $\mathrm{PSp}(2g_0, F_3)$. (*By Cohen's result, it is actually all of* $\mathrm{PSp}(2g_0, F_3)$.)

(2) *If* $d = 4$ *then the fiber of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$ *over* Γ *maps surjectively to the projective space associated to the* F_3*-vector space* W_0 *of* 3*-torsion elements of the Picard group of* C_0. *The points of this projective space correspond naturally to the curves* C_1 *which are unramified triple covers of* C_0. *Given such a curve* C_1, *the points of the fiber of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$ *which correspond to* C_1 *are in one to one correspondence with the elements of the projective space associated to a certain* $2g + 2$*-dimensional* F_2*-vector space* W_1 *of* 2*-torsion elements of the Picard group of* C_1. *The monodromy group* G *of* $\mathscr{H}_{d,g} \to \mathscr{P}_b$ *preserves the Weil pairing on* W_0, *and the elements fixing a given point* C_1 *preserve the Weil pairing on* W_1. *Thus* G *is naturally a subgroup of the wreath product of* $\mathrm{PSp}(2g_0, F_3)$ *and a projective orthogonal group.*

It seems natural to hope that the monodromy group in case (2) is all of the wreath product.

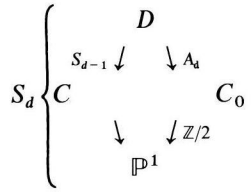
The theorem shows that the subgroup of the monodromy group fixing a given sheet of $\mathscr{H}_{d,g} \to \mathscr{P}_b$ must preserve the set of sheets corresponding to lines orthogonal to the given sheet with respect to the Weil pairing. We immediately obtain:

COROLLARY 7. *If $d = 3$ or 4 then the monodromy of $\mathscr{H}_{d,g} \to \mathscr{P}_b$ is not doubly transitive.* □

For example, if $d = 3$, $g = 1$, $b = 6$, then the cover $\mathscr{H}_{d,g} \to \mathscr{P}_b$ has 40 sheets, corresponding to the points of the projective 3-space $\mathbb{P}^3(F_3)$. If we denote the alternating form on $(F_3)^4$ stabilized by $\mathrm{PSp}(4, F_3)$ by $\langle -, - \rangle$, then the stabilizer of a sheet s has two orbits besides $\{s\}$: One of order 12 consisting of the hyperplane in $\mathbb{P}^3(F_3)$ of points t with $\langle s, t \rangle = 0$, and the other its complement, of order 27.

The situation for $d > 4$ is not so clear, but from Hurwitz' computation of the number of sheets one can see that in general the fiber of $\mathscr{H}_{d,g} \to \mathscr{P}_b$ can no longer be identified with a projective space over a field. Thus no result of the type above can hold, and it seems natural to expect that the monodromy group will be doubly transitive, perhaps even the full alternating group, in general.

To prove Theorem 6 we begin by considering the case of general d. Let π: $C \to \mathbb{P}^1$ be a covering of degree d with only simple branching. Since the monodromy group of π is transitive and generated by simple transpositions, it is the full symmetric group on d letters, S_d. This monodromy group is equal to the Galois group of the normal closure $L/\mathbb{C}(t)$ of the field extension $K(C)/\mathbb{C}(t)$ corresponding to π (see for example the proof of Proposition 8, below, or Harris [1979].) We may write L as $K(D)$, the field of rational functions on a smooth curve D covering C, so that C is the quotient of D by S_{d-1}, the stabilizer of a point of D.



Let C_0 be the quotient of D by the alternating group A_d, so that C_0 is a double cover of the projective line.

We claim that C_0 is the (unique) double cover of $\mathbb{P}^1$ ramified over the same points as C, and that the covering $D \to C_0$ is unramified. To see this, we use the following well-known result relating Galois Theory and monodromy:

Let $C \to A$ be a map of smooth curves, and let $D \to C \to A$ be the maps of curves corresponding to the Galois closure of the function field extension

$K(C)/K(A)$. Let H be a subgroup of the Galois group $G = \mathrm{Gal}(D/A)$, and let $C_0 = D/H$ be the corresponding curve. Let $p_0 \in A$ be a base point (not a branch point of D), and $\gamma \subset A$ a loop based at p_0. If we identify G with the monodromy group of D/A, then γ induces an element g of G. If we identify G with the fiber of D over p_0, then the fiber of C_0 over p_0 can be identified with the coset space G/H.

PROPOSITION 8. *With these conventions, the monodromy transformation corresponding to γ on the fiber of $C_0 \to A$ over p_0 is left multiplication by g, and the monodromy group of $C_0 \to A$ is thus G modulo the intersection of the conjugates of H.*

Proof. The statement about γ follows at once from the special case $H = \langle 1 \rangle$, $C_0 = D$. To establish this case, let Γ be the branch locus of $C \to A$, and let $K \subset \pi_1(A - \Gamma)$ be the subgroup of the fundamental group corresponding to the covering C, so that the fiber of C over p_0 corresponds to the coset space $\pi_1(A - \Gamma)/K$. The group $\pi_1(A - \Gamma)$ acts on the coset space by left multiplication, and this is the monodromy action. The kernel of the action is the intersection N of all the conjugates of K in $\pi_1(A - \Gamma)$, and thus the monodromy group is $G_1 = \pi_1(A - \Gamma)/N$.

The main point is that the Galois closure D is the covering D_1 corresponding to N. Since the monodromy action of $\pi_1(A - \Gamma)$ on D_1 is by left multiplication on $\pi_1(A - \Gamma)/N$, this will suffice to prove the proposition.

First, G_1 acts naturally on D_1 preserving the map to A (on which G_1 acts trivially, so that G_1 acts on $K(D_1)$ fixing $K(A)$.) Since the order of G_1 is the degree of D_1 over A, which is in turn the degree of the field extension $K(D_1)/K(A)$, we see that $K(D_1)^{G_1} = K(A)$, that $K(D_1)/K(A)$ is Galois, and that G_1 is its Galois group, all by the fundamental theorem of Galois theory. Again comparing orders and degrees, we see that the subfield fixed by $K/N \subset G_1$ is precisely $K(C)$. If now $K(D_1)$ were not the Galois closure of $K(C)/K(A)$, there would be a nontrivial subgroup of K/N, corresponding to the Galois closure, which was normal in G_1. Since N is the intersection of the conjugates of K, this is ridiculous, and we are done. □

COROLLARY 9. *In the situation in the diagram above, C and C_0 have the same branch divisor in $\mathbb{P}^1$; in particular, C_0 depends only on the branch locus of π and not on the isomorphism type of C. On the other hand, D is unramified over C_0.*

Proof. Proposition 8 shows immediately that C_0 cannot be ramified over any point where C is not. Conversely, if p is a point over which C is ramified, then the monodromy transformation of the fiber in C corresponding to a small loop γ around p is a simple transposition; since this transformation is not in the alternating group, the proposition shows that γ induces a nontrivial monodromy transformation of the fiber of C_0. Thus C_0 is also ramified over p. This proves the first statement.

To show that D is unramified over C_0, note that by the same argument as above, D can be ramified over $\mathbb{P}^1$, and thus a fortiori over C_0, only over branch

points of C. On the other hand, the monodromy transformation of D over one of these branch points is of order 2 by Proposition 8 (in fact the proposition shows that it is the product of $d!/2$ disjoint 2-cycles.) Thus the ramification points of D over $\mathbb{P}^1$ are all simple. From this we see that if the map $D \to C_0$ were ramified at $q \in D$, the image of q in C_0 could not be a ramification point of C_0 over $\mathbb{P}^1$, though of course q would be a ramification point of $D \to \mathbb{P}^1$. On the other hand, since the degree of $C_0 \to \mathbb{P}^1$ is 2, and C_0 is branched over the same points as C, we see that C_0 is totally ramified over each branch point; thus the image in C_0 of every ramification point of $D \to \mathbb{P}^1$ must be a ramification point of $C_0 \to \mathbb{P}^1$, and we see that $D \to C_0$ is unramified as claimed. □

We now return to the proof of Theorem 6. The covering $C \to \mathbb{P}^1$ is determined by $D \to \mathbb{P}^1$ since C is the quotient of D by the subgroup of the Galois group fixing one sheet, and the different subgroups of this form are conjugate. Thus the points in the fiber of $\mathscr{H}_{d,g} \to \mathscr{P}_b$ over Γ correspond to unramified covers D of C_0 which are Galois over $\mathbb{P}^1$ with Galois group S_d.

In the case $d = 3$ we have $A_3 = \mathbb{Z}/3$, so that D is an unramified cyclic extension of C_0. Any such extension has the form

$$D = \operatorname{Spec} \mathscr{O}_{C_0} \oplus \mathscr{L} \oplus \mathscr{L}^2$$

for some line bundle $\mathscr{L}$ on C_0 with $\mathscr{L}^3 = \mathscr{O}_{C_0}$, the sheaf $\mathscr{O}_{C_0} \oplus \mathscr{L} \oplus \mathscr{L}^2$ being regarded as a sheaf of $\mathscr{O}_{C_0}$-algebras by means of this identification. The line bundles $\mathscr{O}_{C_0}$, $\mathscr{L}$, $\mathscr{L}^2$, viewed as points of the F_3-vector space of 3-torsion elements in the Picard group of C_0, form a line through the origin; that is, a point of $\mathbb{P}^{2g'-1}(F_3)$, where $g' = g + 1$ is the genus of C_0. Since the construction is reversible, we see that the fiber of $\mathscr{H}_{3,g} \to \mathscr{P}_b$ is in natural correspondence with $\mathbb{P}^{2g'-1}(F_3)$. Since the Weil pairing is constant in families (it may be regarded as the intersection form on the singular cohomology group $H^1(C_0, \mathbb{Z}/3)$) we see that it is preserved by the monodromy action, and the result is proved. (Since the family of 3-torsion points in $\operatorname{Pic} C_0$ is unramified over $\mathscr{P}_b$, we can follow $\mathscr{L}$ and $\mathscr{L}^2$ individually around a loop, so that the monodromy preserves the Weil pairing exactly – not just up to scalars – and we get PSp rather than the group of transformations preserving the Weil pairing up to scalars.)

Turning to the case $d = 4$, we note that A_4 has a normal subgroup N of order 4 (consisting of the products of pairs of disjoint transpositions), with quotient $\mathbb{Z}/3$, so that D determines an unramified $\mathbb{Z}/3$ covering C_1 of C_0, and we get as before a point of $\mathbb{P}^{2g'-1}(F_3)$, where $g' = g + 2$ is the genus of C_0 in this case. Every unramified irreducible $\mathbb{Z}/3$ covering occurs in this way, as follows from the construction below. As before, we see that the monodromy group of $\mathscr{H}_{4,g} \to \mathscr{P}_b$ maps to $\mathrm{PSp}(2g', F_3)$.

Let H be the fiber of $\mathscr{H}_{4,g} \to \mathscr{P}_b$ over $\Gamma \in \mathscr{P}_b$, and let W be the F_3 projective space of the lines in the 3-torsion subgroup of $\operatorname{Pic} C_0$. We may identify a line w in

W with an unramified cyclic triple cover C_1 of C_0, which has genus $3g + 4$ by Hurwitz' formula. To identify the fiber of $H \to W$ over w, note that the points of the fiber correspond to (certain) Galois covers with group $N = \mathbb{Z}/2 \times \mathbb{Z}/2$. Such a cover is the composite of 2 unramified cyclic covers of degree 2, so to each point of the fiber we may associate a 2-dimensional subgroup V of the 2-torsion subgroup of $\operatorname{Pic} C_1$, which we regard as a vector space over the field of 2 elements F_2. The subgroup V is isomorphic as an $F_2[S_3]$-module to the module V_0 defined by the property:

(*) $S_3 = S_4/N$ acts on the 3 nonzero elements of $V_0 \mapsto F_2^2$ via the natural permutation action of S_3.

This is because the action on the nonzero elements of V_0 is the same as the action on the intermediate subfields of $K(D)/K(C_1)$.

Conversely, every subgroup of $\operatorname{Pic} C_1$ which is isomorphic to V_0 as an $F_2[S_3]$-module corresponds to a point in the fiber over w because it determines a covering of $\mathbb{P}^1$ with Galois group S_4.

To complete the proof, we must identify the set of subgroups $V \subset \operatorname{Pic} C_1$ such that $V \cong V_0$ as $F_2[S_3]$-modules with a projective space over F_2. In fact, if we choose a transposition $\sigma \in S_3$, then each such subgroup V contains a unique nonzero σ-invariant element, which we may take as a 'representative' of V; the fiber over w is thus identified with the projective space on the vector space W_1 spanned by these representative elements. The Weil pairing on W_1 is preserved by the subgroup of the monodromy group fixing w, and thus this subgroup acts as a subgroup of a projective orthogonal group on W_1 as claimed.

We could now complete the proof by deducing the dimension $2g + 1$ of the projective space of representative elements from Hurwitz' formula for the number of points in the fiber in the 4-sheeted case, but this number follows easily from representation theory, so we derive it directly; at the same time, our considerations will 'locate' the copies of V_0 in $\operatorname{Pic} C_1$:

First consider the action of the Sylow 3-subgroup $\mathbb{Z}/3 = \langle \tau \rangle \subset S_3$. The group algebra $F_2[\mathbb{Z}/3]$ is semisimple, and decomposes into two irreducible submodules: the trivial representation and the two-dimensional representation V (regarded as an $F_2[\mathbb{Z}/3]$-module) whose 3 nonzero elements are cyclically permuted by τ. Thus the 2-torsion subgroup $(\mathbb{Z}/2)^{6g+8}$ of $\operatorname{Pic} C_1$ decomposes under the action of $\mathbb{Z}/3$ into two pieces: the set of τ-invariant elements, which is isomorphic to the 2-torsion subgroup $(\mathbb{Z}/2)^{2g+4}$ of $\operatorname{Pic} C_0$, and its complement $H' \cong (\mathbb{Z}/2)^{4g+4}$, which, at least as an $F_2[\mathbb{Z}/3]$-module, is a direct sum of copies of V_0.

It now follows that H' is a direct sum of copies of V_0 as an $F_2[S_3]$-module. To see this, note that $1 + \tau + \tau^2$ is a central idempotent in $F_2[S_3]$ which splits

$F_2[S_3]$ into the two blocks

$$A := (1 + \tau + \tau^2)F_2[S_3] \cong F_2[\varepsilon]/\varepsilon^3$$

and

$$B := (\tau + \tau^2)F_2[S_3] \cong 2 \times 2 \text{ matrices over } F_2.$$

(All we really need of this is that $B = F_2[S_3]/(1 + \tau + \tau^2)$ is semi-simple, which follows at once because $B = B(\sigma + \tau) \oplus B(\sigma + \tau^2)$, and the summands are irreducible B-modules.) Thus there is a unique irreducible $F_2[S_3]$-module annihilated by $1 + \tau + \tau^2$, which is V_0; and every $F_2[S_3]$-module annihilated by $1 + \tau + \tau^2$ is a direct sum of copies of V_0. In particular, this applies to H', proving our assertion.

Since V_0 is 2-dimensional, we must have $H' \cong V_0^{2g+2}$, so the subspace W_1 of σ-invariant elements is of dimension $2g + 2$. It follows that the fiber over w is $\mathbb{P}^{2g+1}(F_2)$, which has $2^{2g+2} - 1$ points, as Hurwitz found. □

Acknowledgment

The authors are grateful to the NSF for partial support during the preparation of this work.

References

E. Arbarello and M. Cornalba: Footnotes to a paper of Beniamino Segre. *Math. Ann.* 256 (1981) 341–362.

A. Cayley, On the cubic curves inscribed in a given pencil of six lines. *Quart J. of Pure and Appl. Math.* 9 (1868) 210–221.

A. Clebsch, Zur Theorie der binären Formen sechster Ordnung und zur Dreitheilung der hyperelliptischen Funktionen. *Abh. der k. Ges. Wiss. zu Göttingen* 14 (1869) 1–59.

A. Clebsch: Zur Theorie der algebraischen Funktionen, *Math. Ann.* 29 (1887) 171–186.

D. B. Cohen: The Hurwitz monodromy group. *J. Alg.* 32 (1974) 501–517.

S. Diaz and J. Harris: Geometry of the Severi Variety I, *Trans. Am. Math. Soc.* (1989).

J. Harris, Galois groups of enumerative problems. *Duke J. Math.* 46 (1979) 685–724.

J. Harris and I. Morrison: Slopes of effective divisors on the moduli space of stable curves. *Invent. Math.* (to appear 1989).

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

S. Kleiman and R. Speiser: Enumerative geometry of nonsingular plane cubics, submitted to the Proc. 1988 Sundance Conference. Contemporary Math. (to appear 1990.)

P. Kluitmann: Hurwitz action and finite quotients of braid groups. In *Braids*, (Ed. J. S. Birman and A. Libgober), *Contemporary Math.* 78, (1988) 299–325.

J. Lüroth, Note über Verzweigungsschnitte und Querschnitte in einer Riemann'schen Fläche. *Math. Ann.* 4 (1871) 181–184.

C. Maclachlan, On representations of Artin's Braid group. *Mich. Math. J.* 25 (1978) 235–244.

S. Maillard, *Recherche des charactéristiques des systèmes élémentaires de courbes planes du trosième ordre.* Thèse, Paris, (1871), published by Cusset.

J. A. Tyrrell, Degenerate plane cubics and a theorem of Clebsch. *Bull. London Math. Soc.* 5 (1973) 203–208.