Vol. 52, No. 4 DUKE MATHEMATICAL JOURNAL © December 1985

HURWITZ FAMILIES AND ARITHMETIC GALOIS GROUPS

KEVIN COOMBES AND DAVID HARBATER

Introduction. This paper is concerned with Galois branched covers of the Riemann sphere. In the first section we consider the moduli problem for such covers, including whether Hurwitz families exist and whether they are universal. In the second section we turn to arithmetic questions, involving finding fields of definition and of moduli for covers and for Hurwitz families. In the third section we discuss some techniques for constructing covers with given groups and field of definition, in special cases.

We wish to thank M. Artin, G. Glauberman, and J. Thompson for helpful discussions regarding material in this paper. We also wish to thank M. Fried, both for discussions regarding this material and for comments on the preliminary draft of this paper.

§1. Hurwitz families. In this section we will consider the moduli problem for Galois branched covers of the Riemann sphere $\mathbf{P}^1_{\mathbf{C}}$. We ask whether there is a coarse moduli space, whether this space has an associated family, and whether this family is universal. We do this by first studying the (easier) case of pointed covers, and then forgetting the base points.

We begin by fixing terminology. By a (branched) *cover* $X \xrightarrow{\pi} Y$ (of normal varieties or complex manifolds) we mean a surjective and generically étale map—e.g., any nonconstant map between Riemann surfaces. In the case of Riemann surfaces, the finite set $L \subset Y$ of points at which π is not étale is the *branch locus* of the cover, and generally we will consider such covers taken together with an ordering $(\xi_1, \ldots, \xi_r)$ of the branch points. A *Galois* covering is one which is connected and whose Galois group $\mathrm{Gal}_Y X$ of covering transformations acts transitively on the fibers. Related to this notion are two others: If G is an (abstract) finite group, a *G-cover* $X \to Y$ is a cover together with an inclusion $i : G \hookrightarrow \mathrm{Gal}_Y X$ whose image acts transitively on the fibers. If X is connected such a G-cover will be called *G-Galois*; any such cover is of course Galois in the above sense, and the inclusion i is an isomorphism. Observe that for a G-Galois cover, each $\gamma \in G$ acts on X in a way that conjugates the G-action by γ; thus the automorphisms of a G-Galois cover are in bijection with the center Z of G.

Received November 7, 1984. Research of first author supported in part by NSF. Research of second author supported in part by NSF and the Sloan Foundation.

Given $L = \{\xi_1, \ldots, \xi_r\} \subset \mathbf{P}^1$, we can choose a *standard homotopy basis* for $U = \mathbf{P}^1 - L$ at a base point $\xi_0 \notin L$; i.e., generators $\sigma_1, \ldots, \sigma_r \in \pi_1(U, \xi_0)$ such that $\prod \sigma_i = 1$, and such that σ_i is represented by a loop at ξ_0 which winds once around ξ_i counterclockwise, and winds around no other ξ_j. Of course this basis will generally not be unique. Relative to each such basis, each pointed G-Galois cover $X \xrightarrow{\pi} \mathbf{P}^1$ with ordered branch locus $(\xi_1, \ldots, \xi_r)$ corresponds to a quotient of $\pi_1(U, \xi_0)$ and hence to an r-tuple $g = (g_1, \ldots, g_r)$ of generators of G satisfying $\prod g_i = 1$. Call g the *description* of the G-Galois cover, relative to the given basis $\{\sigma_i\}$. (Also, a Galois cover $X \xrightarrow{\pi} \mathbf{P}^1$ will be said to have *description* (G, g) if there is an isomorphism $G \xrightarrow{\sim} \mathrm{Gal}_{\mathbf{P}^1} X$ such that the induced G-Galois cover has description g.)

By the Riemann Existence Theorem, the above correspondence between pointed G-Galois covers $X \to \mathbf{P}^1$ and r-tuples g is a bijection. Here, given a G-Galois cover $X \to \mathbf{P}^1$ together with two choices of base point $\zeta, \zeta' \in X$ over $\xi_0 \in \mathbf{P}^1$, the corresponding g, g' are related by $g_i' = \gamma g_i \gamma^{-1}$, where $\gamma \in G$ is the element satisfying $\zeta' = \gamma(\zeta)$. Meanwhile, by varying the homotopy bases, the bijection itself changes. Namely, if $\{\sigma_i\}, \{\bar{\sigma}_i\}$ are two standard homotopy bases at ξ_0 relative to the same ordered branch locus, then each $\sigma_i \sim \bar{\sigma}_i$ (i.e., σ_i is conjugate to $\bar{\sigma}_i$) in π_1. Hence if g, $\bar{g}$ are the descriptions of a single pointed G-Galois cover relative to the two bases, then $g_i \sim \bar{g}_i$ in G for all i. But the inner automorphism may vary with i. Since in the moduli problem the branch points will be allowed to move, it will be necessary to allow the homotopy basis to vary. Thus when we speak of coverings having variable branch locus and with fixed description g, we mean description relative to *some* standard homotopy basis (depending on the cover).

We now consider the moduli problem for Galois covers of $\mathbf{P}^1$ having a given description, and with variable branch locus. Actually, there are several different problems, depending on whether we consider pointed covers, and on whether we consider covers together with a given G-action. (To prevent a still further proliferation of problems, each cover will be assumed to be equipped with an ordering of its branch points.) In each case we can ask three questions:

(1) Is there a *Hurwitz space*, i.e., a coarse moduli space $\mathscr{P}$ for covers of the given type? In this case there is a covering map $\mathscr{P} \to (\mathbf{P}^1)^r - \Delta$, assigning to each cover its branch locus. (Here Δ is the "weak diagonal," consisting of r-tuples with two equal entries.)

(2) If so, then is there a *Hurwitz family*, i.e., a total space $\mathscr{H}$ and a covering map $\mathscr{H} \to \mathscr{P} \times \mathbf{P}^1$ such that the fiber over $\{\xi\} \times \mathbf{P}^1$ is the cover corresponding to ξ?

(3) If so, then is this family universal? Equivalently, is $\mathscr{P}$ a fine moduli space?

(Cf. also [Fu], [Fr1], [FB] for a discussion of these questions.) In our situation, things are of course trivial for $r = 1$ (i.e., only one branch point), since in that case there are no nontrivial covers. For $r = 2$ all covers are cyclic, and the answer to (1) is yes for any cyclic group G, with $\mathscr{P} = (\mathbf{P}^1)^2 - \Delta$. But the answer to (2) (and hence (3)) is no, unless G is cyclic of order 2. Namely, as observed in [Fr3], any such family $\mathscr{H} \to \mathscr{P} \times \mathbf{P}^1$ would determine an unbranched cover of $(\mathbf{P}^1)^3 - \Delta$. But $\pi_1((\mathbf{P}^1)^3 - \Delta) = \mathbf{Z}/2$, and so indeed $\# G = 2$. Henceforth, we restrict attention to $r \geqslant 3$. In this situation, we can use the following result of Mike Fried, which allows us to consider families of pointed covers with moving branch locus.

1.1. Lemma (Fried). *For $r \geqslant 3$, there is a continuous map (relative to the metric topology) $\beta : (\mathbf{P}^1)^r - \Delta \to \mathbf{P}^1$ such that $(\beta, 1)$ is a section of the projection $(\mathbf{P}^1)^{r+1} - \Delta \xrightarrow{p} (\mathbf{P}^1)^r - \Delta$ given by $p(\xi_0, \dots, \xi_r) = (\xi_1, \dots, \xi_r)$.*

Proof. We describe one possible choice for β. Identify $\mathbf{P}^1$ with the unit sphere S^2, and let d be the induced metric. Given $(\xi_1, \dots, \xi_r)$ let C be the unique circle through ξ_1, ξ_2, ξ_3, and let C_0 be the arc from ξ_1 to ξ_2 which does not contain ξ_3. Let ξ_0 be the unique point on C_0 whose distance to ξ_1 is equal to $\frac{1}{2}\mathrm{Min}\{d(\xi_1, \xi_i) \mid 2 \leqslant i \leqslant r\}$. It is then clear that ξ_0 is distinct from $\xi_1, \dots, \xi_r$, and that the assignment $(\xi_1, \dots, \xi_r) \mapsto \xi_0$ as above defines a continuous map β. $\square$

Remark. For $r = 3$ such a map β can be chosen to be algebraic, by using the cross ratio. But for $r \geqslant 4$, there is *no* algebraic choice of β. To see this, first observe that for a generic choice of $r - 1$ distinct points $S = \{\xi_1, \dots, \xi_{r-1}\} \subset \mathbf{P}^1$, there is no nontrivial algebraic automorphism of $\mathbf{P}^1$ (i.e., projective linear transformation) which fixes two of the ξ_i and permutes the others. So fix such a choice of points. Then, if a β as in the statement of 1.1 were algebraic, there would be an induced algebraic map $\alpha : \mathbf{P}^1 - S \to \mathbf{P}^1 - S$ without fixed points, defined by $\alpha(\lambda) = \beta(\xi_1, \dots, \xi_{r-1}, \lambda)$. This would extend to a surjective algebraic map $f : \mathbf{P}^1 \to \mathbf{P}^1$ such that $f^{-1}(S) = S$. The surjectivity of f would imply that f induces a permutation of S, and hence that the branched cover $f : \mathbf{P}^1 \to \mathbf{P}^1$ is totally ramified over S. Thus f is of degree 1, by the Hurwitz formula, and hence f is a projective linear transformation, corresponding to some $F \in \mathrm{SL}(2, \mathbf{C})$. Since $f^{(r-1)!}$ fixes each of the $r - 1$ points of S, and $r - 1 \geqslant 3$, it follows that $f^{(r-1)!}$ is the identity. Thus the image of F in $\mathrm{PSL}(2, \mathbf{C})$ has finite order, and so F itself has finite order. Hence F is diagonalizable, and so it has two linearly independent eigenvectors in $\mathbf{C}^2$. Thus f, which permutes S, fixes two points of S. By the construction of S, f is the identity. This contradicts the lack of fixed points of α.

From now on, pointed covers of $\mathbf{P}^1$ with ordered branch locus $\xi = (\xi_1, \dots, \xi_r)$ will be assumed pointed over $\xi_0 = \beta(\xi)$.

1.2. Proposition. *Let G be a finite group, $r \geqslant 3$, and $\underset{\sim}{g} = (g_1, \dots, g_r)$ an r-tuple of generators with product 1. Then there is a fine moduli space $\tilde{\mathscr{P}}$ for pointed Galois covers with description $(G, \underset{\sim}{g})$, and also a fine moduli space $\mathscr{P}^*$ for pointed*

G-Galois covers with description g. The natural maps $\mathscr{P}^*, \tilde{\mathscr{P}} \to (\mathbf{P}^1)^r - \Delta$ *and* $\mathscr{P}^* \to \tilde{\mathscr{P}}$ *are covering maps, and the latter is an* $(\operatorname{Aut} G)$*-cover.*

Proof. Let $Q = \tilde{\mathscr{P}}$ or $\mathscr{P}^*$. As in [Fu] or [Fr1], we may topologize the set Q of (isomorphism classes of) such covers so that the map $Q \xrightarrow{\pi} (\mathbf{P}^1)^r - \Delta$, assigning to each cover its branch locus, becomes an unramified cover. In this topology, given a collection of disjoint discs $D_1, \ldots, D_r \subset \mathbf{P}^1$, the set $D = \prod D_i \subset (\mathbf{P}^1)^r$ is evenly covered, and there is a family $\mathscr{H}_D \to \pi^{-1}(D) \times \mathbf{P}^1$ such that the fibre over $\{\xi\} \times \mathbf{P}^1$ is the cover corresponding to ξ. This family is unique since D is simply connected. Given overlapping D and D', $\mathscr{H}_D$ and $\mathscr{H}_{D'}$ have isomorphic restriction over $D \cap D'$, since the intersection is simply connected as well. This isomorphism, moreover, is unique, since a *pointed* cover has no automorphisms. So these patch to give a global family. Again, by the lack of automorphisms, this family is universal. The final assertion now follows easily. $\square$

Remark. The coverings $\mathscr{P}^*, \tilde{\mathscr{P}} \to (\mathbf{P}^1)^r - \Delta$ need not be H-covers (for H some other group), as can be seen from the case that G is nonabelian, $r = 4$, $g_2 = g_1^{-1}$, $g_4 = g_3^{-1}$.

1.3. Proposition. *Given* (G, g) *as in Proposition* 1.2, *the fine moduli space* $\tilde{\mathscr{P}}$ *is also a Hurwitz space for Galois covers of* $\mathbf{P}^1$ *with description* (G, g), *over which there is a Hurwitz family.*

Proof. Observe first that the points of $\tilde{\mathscr{P}}$ are in bijection with the Galois covers of $\mathbf{P}^1$ with description (G, g) since each such cover can (up to isomorphism) be pointed in a unique way. Next, given any family of Galois covers $\mathscr{F} \to S \times \mathbf{P}^1$ with description (G, g), the map $S \to \tilde{\mathscr{P}}$ assigning to each $s \in S$ its isomorphism class is continuous, by definition of the topology on $\tilde{\mathscr{P}}$. So there is a morphism $\tilde{F} \xrightarrow{\phi} \tilde{\mathscr{P}}$, where $\tilde{F}$ is the functor of such covers. Here ϕ is a bijection on (complex) points. Now let $\mathscr{H} \to \tilde{\mathscr{P}} \times \mathbf{P}^1$ be the universal family given by Proposition 1.2 (regarded as a family of Galois covers). Then given a morphism $\tilde{F} \xrightarrow{\psi} N$, and evaluating at $\tilde{\mathscr{P}}$, the family $\mathscr{H}$ induces a map $\tilde{\mathscr{P}} \to N$. By definition of $\mathscr{H}$, the composition $\tilde{F} \to \tilde{\mathscr{P}} \to N$ is just ψ, as desired. So indeed $\tilde{\mathscr{P}}$ is a coarse moduli space, and $\mathscr{H} \to \tilde{\mathscr{P}} \times \mathbf{P}^1$ is a Hurwitz family. $\square$

Remarks. (i) There is no *universal* Hurwitz family for Galois covers, unless G is trivial. Namely, let $h \in G$ be an element of order $n > 1$, let $X \to \mathbf{P}^1$ be a Galois cover with description (G, g), and let $Y \to \mathbf{P}^1$ be the subcover of index n corresponding to the subgroup $\langle h \rangle \subset G$. The function fields of X and Y are related by $K_X = K_Y[w]/(w^n - f)$, for some $f \in K_Y$. Consider a family of covers $\mathscr{X} \to T \times \mathbf{P}^1$, where T is the complex t-line with $\{0, \infty\}$ deleted, corresponding to the function field $K_Y(t)[w]/(w^n - tf)$. This family is nontrivial, but is locally trivial in the metric topology. So it is not the pullback of any Hurwitz family.

(ii) The existence of a Hurwitz family for Galois covers may be regarded as somewhat surprising, since the analog is false for covers in general. In the non-Galois case, the proof of 1.3 breaks down, since the moduli space $\tilde{\mathscr{P}}$ for pointed covers is *not* a moduli space for unpointed covers, inasmuch as there are, up to isomorphism, several ways of choosing a base point.

(iii) The Hurwitz family above need not be Galois, since there may be no well-defined choice of G-action globally defined over $\tilde{\mathscr{P}}$. But this phenomenon cannot occur for Hurwitz families of G-Galois covers occurring in Proposition 1.4 below.

(iv) The assertion in Proposition 1.3 is purely algebraic, since every covering of Riemann surfaces is defined algebraically. But the remark after Lemma 1.1 shows that the proof is inherently nonalgebraic.

In the case of G-Galois covers (i.e., covers together with a group action), the situation is more complicated. But at least families can often be shown to exist:

1.4. PROPOSITION. (a) *Given (G, g) as in Prop. 1.2, there is a coarse moduli space $\mathscr{P}$ for G-Galois covers of $\mathbf{P}^1$ with description g, and the natural map $\mathscr{P}^* \to \mathscr{P}$ defines a (G/Z)-cover (where Z is the center of G, and so G/Z is the inner automorphism group* $\operatorname{Inn} G$). *The map $\mathscr{P} \to \tilde{\mathscr{P}}$ is an* $(\operatorname{Out} G)$-*cover (where* $\operatorname{Out} G = \operatorname{Aut} G/\operatorname{Inn} G$).

(b) *If Z is a direct summand of the centralizer of some g_i, then there is a Hurwitz family over $\mathscr{P}$. If Z is trivial, this family is universal, so $\mathscr{P}$ is a fine moduli space.*

(c) *If S is a* 1-*dimensional connected complex variety and $S \xrightarrow{f} \mathscr{P}$ is a map, then there is a family $\mathscr{F} \to S \times \mathbf{P}^1$ of G-Galois covers with description g such that the fibre over $s \in S$ is the cover corresponding to $f(s)$. So there is a Hurwitz family over $\mathscr{P}$ provided $r = 3$ or* 4.

Proof. (a) Let $\mathscr{P}$ be the set of (isomorphism classes of) G-Galois covers of $\mathbf{P}^1$ with description g. Then, as in the proof of Prop. 1.2, $\mathscr{P}$ may be topologized so that the branch locus map $\mathscr{P} \xrightarrow{\pi} (\mathbf{P}^1)^r - \Delta$ becomes a covering map. Observe that the covering map $\mathscr{P}^* \to (\mathbf{P}^1)^r - \Delta$ factors through $\mathscr{P}$, so that $\mathscr{P}^* \to \mathscr{P}$ is a covering map. Observe that G acts on $\mathscr{P}^*$ over $\mathscr{P}$, transitively on the fibres. Namely, given $g \in G$ and $\eta \in \mathscr{P}^*$, where η corresponds to a G-cover $X \to \mathbf{P}^1$ with base point ξ, let $g(\eta) \in \mathscr{P}^*$ be the point corresponding to $X \to \mathbf{P}^1$ with base point $g(\xi)$. Observe that $g \in G$ acts trivially on $\mathscr{P}^*$ if and only if $g \in Z$. So $\mathscr{P}^* \to \mathscr{P}$ is G/Z-Galois.

We have already seen that the points of $\mathscr{P}$ correspond to the covers in question, and that there is a morphism $F \xrightarrow{\Phi} \mathscr{P}$, where F is the functor of families of pointed covers as above. To complete the proof that $\mathscr{P}$ is a coarse moduli space, suppose $F \xrightarrow{\psi} N$ is a morphism. Apply ψ to the universal family $\mathscr{H} \to \mathscr{P}^* \times \mathbf{P}^1$ (regarded as a family of unpointed G-covers), to obtain a map $\mathscr{P}^* \xrightarrow{\alpha} N$. Since $\mathscr{H}$ remains invariant under the G/Z-action on $\mathscr{P}^*$ over $\mathscr{P}$, so does α. Thus α descends to a map $\mathscr{P} \to N$, and as desired the composition $F \to \mathscr{P} \to N$ is ψ. The final assertion follows easily, using Prop. 1.2.

(b) If Z is trivial, then any family of pointed G-Galois covers has only the identity automorphism, so as in the proof of 1.2 there is a universal family.

Next, say Z is a direct summand of the centralizer C of some g_i (say, g_1). Thus there is a homorphism $C/Z \to C$ which is a section of $C \to C/Z$. Observe that if we identify $\mathbf{P}^1$ with S^2 (as a metric space) as in the proof of 1.1, then for all $\xi = (\xi_1, \ldots, \xi_r) \in (\mathbf{P}^1)^r - \Delta$, the circle centered at ξ_1 and passing through $\xi_0 = \beta(\xi)$ contains no ξ_i in its interior other than ξ_1 itself. Thus this circle determines a loop $\sigma_1 \in \pi_1(P^1 - \{\xi_1, \ldots, \xi_r\}, \xi_0)$, which is part of a standard homotopy basis $\sigma_1, \ldots, \sigma_r$. So given a G-Galois cover $X \to \mathbf{P}^1$ with description g, and branched at ξ, there is a base point $\hat{\xi}$ in X over ξ_0 such that the loop σ_1 lifts to a path $\hat{\sigma}_1$ in X satisfying $\hat{\sigma}_1(1) = g_1(\hat{\sigma}_1(0))$. Let $\eta \in \mathscr{P}$ be the point corresponding to this G-Galois cover, and let $\mathscr{P}^0$ be the connected component of this point. It suffices to show that there is a family $\mathscr{F} \to \mathscr{P}^0 \times \mathbf{P}^1$ whose fibre over $\{\mu\} \times \mathbf{P}^1$ is the cover corresponding to μ, for all $\mu \in \mathscr{P}^0$. Such a family exists locally near η, and locally the base point on X extends to a section over the base point on $\mathbf{P}^1$. Given two such local families, defined on overlapping open sets $D, D' \in \mathscr{P}^0$ with connected intersection, there exists an isomorphism between them as (unpointed) G-Galois covers—in fact, such isomorphisms are in bijection with Z. Namely, for any such isomorphism, an element $\gamma \in G$ is determined, namely the covering transformation taking one section over the base point locus to the other. Hence γ is well defined up to multiplication by an element in Z. We thus obtain an element $\bar{\gamma} \in G/Z$. Actually, any such γ lies in C (and so $\bar{\gamma} \in C/Z$), since any cover corresponding to a point in the overlap has description $(g_1, \ldots)$ with respect to either section. Composing with the homomorphism $C/Z \to C$, we obtain a unique choice of $\gamma \in C$. Using this choice of patching then yields a family over $\mathscr{P}^0$.

(c) Given such a map $S \xrightarrow{f} \mathscr{P}$, we obtain such a family *locally* on S, but as in (b) the patching is not unique if $Z \neq 1$. But there is a pointed family over the universal covering space $\bar{S}$ of S, say $\mathscr{H} \to \bar{S} \times \mathbf{P}^1$.

Now given a $\sigma \in \pi_1(S) = \mathrm{Gal}_S \bar{S}$, the automorphism of $\bar{S}$ pulls back to $\mathscr{H}$, and induces a new pointed family $\mathscr{H}'$. Both $\mathscr{H}$ and $\mathscr{H}'$ induce maps $\phi, \phi' : \bar{S} \to \mathscr{P}^*$, and the two maps agree after composing with the G/Z-Galois cover $\mathscr{P}^* \to \mathscr{P}$. So ϕ is carried to ϕ' by some $h \in G/Z$ (acting on $\mathscr{P}^*$ over $\mathscr{P}$). The assignment $\sigma \mapsto h$ defines a homomorphism $\pi_1(S) \to G/Z$, i.e., an element $\xi \in H^1(S, G/Z)$. In order to descend $\mathscr{H}$ to a G-covering of S, it suffices to lift ξ to an element of $H^1(S, G)$. But the function field K of S is of cohomological dimension 1, since S is of transcendence degree 1 over $\mathbf{C}$ (Tsen's Theorem; cf. [Se]). Thus the image of ξ in $H^1(K, G/Z)$ is sent to $0 \in H^2(K, Z)$, and hence lifts to an element of $H^1(K, G)$. Thus the family descends "generically" on S. So the function field of $\hat{\mathscr{H}}$ (the profinite completion of $\mathscr{H}$) is Galois over K with group $\pi_1(S) \times G$. Thus the same is true for $\hat{\mathscr{H}}$ as a cover of S. So $\hat{\mathscr{H}}$ descends, i.e., there is a G-family over S.

In the case $r = 3$, the existence of a Hurwitz family follows from the triple transitivity of the group of automorphisms of $\mathbf{P}^1$. For $r = 4$, the triple transitivity reduces the problem to the one-dimensional case, with $S = \mathbf{P}^1 - \{\xi_1, \xi_2, \xi_3\}$. By the above there is a family. (Alternatively, since $\pi_1(\mathbf{P}^1 - \{\xi_1, \xi_2, \xi_3\})$ is free, the map $\pi_1 \to G/Z$ lifts to G, and so the cover $\mathscr{H} \to \bar{S} \times \mathbf{P}^1$ descends.) $\square$

Remark. Even if there is a Hurwitz family over $\mathscr{P}$ it need not induce the universal pointed family over $\mathscr{P}^*$ (much less be universal), if the hypothesis of Proposition 1.4(b) does not hold. For example, consider the quaternion group H of order 8, together with description $(-1, i, j, k)$. Then $\mathscr{P} = (\mathbf{P}^1)^4 - \Delta$, and $\mathscr{P}^* \to \mathscr{P}$ is noncyclic of order 4. By 1.4(c), there is a Hurwitz family over $\mathscr{P}$, but it is not hard to see that the pointed family over $\mathscr{P}^*$ cannot descend to a family over $\mathscr{P}$. (Compare with Example 2.6 below, where the arithmetic analog of this example is discussed in greater detail.)

Problem. Find (G, g) such that there is no Hurwitz family of G-Galois covers with description g.

Whether or not there is a Hurwitz family over $\mathscr{P}$, it is nevertheless the case that $\mathscr{P}$ is the maximal cover of $(\mathbf{P}^1)^r - \Delta$ which is dominated by all ramified covers of $(\mathbf{P}^1)^r - \Delta$ over which there is such a family. More precisely, we have

1.5. PROPOSITION. *Let $\mathscr{P}$ be the coarse moduli space of G-Galois covers with description g, let $Y_0 \to \mathbf{P}^1$ be such a cover, and let $\mathscr{P}^0$ be the connected component in $\mathscr{P}$ of this cover. Consider the set of connected covers $S \xrightarrow{\pi} \mathrm{U}$, where U is any open subset of $(\mathbf{P}^1)^r$, and for which there is a family $\mathscr{H} \to S \times \mathbf{P}^1$ of G-covers with description g, such that the fibre over $\{\pi(s)\} \times \mathbf{P}^1$ has (ordered) branch locus $\pi(s)$, and such that $Y_0 \to P^1$ is one of the fibres. Then the function field of $\mathscr{P}^0$ is the intersection of the function fields of all such parameter spaces S.*

Proof. Any such S induces a map $S \xrightarrow{\phi} \mathscr{P}^0$ whose composition with $\mathscr{P}^0 \to (\mathbf{P}^1)^r - \Delta$ is π. Thus ϕ is a ramified covering. The function field K_S is an extension of $K = K_{\mathscr{P}^0}$, and we may consider it as a subfield of a (fixed) algebraic closure Ω of K. The intersection of all such function fields K_S is the function field of some cover $X \xrightarrow{\alpha} \mathscr{P}^0$. We wish to show that α is an isomorphism.

Observe that α is unramified, since X is dominated by an unramified cover, viz. a connected component of the fine moduli space $\mathscr{P}^*$ of pointed G-Galois covers with description g. Also, for any $\xi \in \mathbf{P}^1$, X is dominated by a component $\mathscr{Q}^0$ of the moduli space $\mathscr{Q}$ of G-covers of $\mathbf{P}^1$ with description g which are unbranched at ξ and are pointed over ξ. By the same argument used in the proof of Prop. 1.2, $\mathscr{Q}$ is a fine moduli space, and the covering map $\mathscr{Q} \to \mathscr{P} - D'$ is G/Z-Galois. (Here $D' \subset \mathscr{P}$ is the inverse image of $\Delta' = \bigcup_{i=1}^r \Delta_i \subset (\mathbf{P}^1)^r$, where Δ_i is the locus at which the ith entry is ξ.) Now let $Y \to \mathbf{P}^1$ correspond to a point in $\mathscr{Q}$. Then Y has description g relative to some homotopy basis β of $\mathbf{P}^1 - \{\xi_1, \ldots, \xi_r\}$, where the ξ_i are the branch points of Y. By allowing the ith branch point to wind around ξ and return to ξ_i, the cover Y can be deformed into a new cover Y_i whose description as a pointed G-cover, relative to β, is g conjugated by g_i. Thus if the cover $\mathscr{Q}$ is extended to a branched cover $\overline{\mathscr{Q}} \to \mathscr{P} \to (\mathbf{P}^1)^r - \Delta$, then a component of the fibre of $\overline{\mathscr{Q}}$ over Δ_i is stabilized by the subgroup of G/Z generated by g_i. Since the elements g_i generate G/Z, the cover $\mathscr{Q}$ cannot dominate any nontrivial covering space over $\mathscr{P}$. The same is true for $\mathscr{Q}^0$ and $\mathscr{P}^0$. Thus X is trivial, and being connected it follows that $X \xrightarrow{\alpha} \mathscr{P}^0$ is an isomorphism.

Remark. The above result can also be proven using the fact (Tsen's Theorem) that a field of transcendence degree 1 over an algebraically closed field has c.d. $\leqslant 1$. Namely, let Ω be the algebraic closure of $F = \mathbf{C}(X_1, \ldots, X_r)$, and for each i let $\Omega_i \subset \Omega$ be the algebraic closure of $F_i = \mathbf{C}(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r)$. Also, let $K \subset \Omega$ be the function field of $\mathscr{P}^0$. Then as in the proof of 1.4(c), an element $\xi \in H^1(K, G/Z)$ is determined, and this induces elements $\xi_i \in H^1(\Omega_i K, G/Z)$ for each i. (Here $\Omega_i K$ denotes the compositum of Ω_i and K in Ω.) By Tsen's Theorem, $H^2(\Omega_i K, Z) = 0$, so ξ_i lifts to an element of $H^1(\Omega_i K, G)$. For some finite extension $F_i \subset L_i$ lying in Ω_i, this element is induced by an element of $H^1(L_i K, G)$, and so $L_i K$ is the function field of a parameter space S_i. It thus suffices to show that $K = \bigcap_i \Omega_i K$, or even that $K = \bigcap_i L_i K$. We may assume that L_i is Galois over F_i. Thus the field $K_i = L_i(X_i)$ is Galois over F. Also, $K_i \cap K = F$, since the closure of $\mathscr{P}^0$ is ramified only over Δ, whereas the cover of $(\mathbf{P}^1)^r$ with function field K_i is ramified only over a union of lines parallel to the X_i-axis. So $L_i K = K_i K = K_i \otimes_F K$. Thus $\bigcap_i L_i K = \bigcap_i (K_i \otimes_F K) = (\bigcap_i K_i) \otimes_F K = F \otimes_F K = K$, as desired.

§2. Fields of definition. In this section we consider the problem of finding fields of definition and fields of moduli for coverings and for Hurwitz families. In section 1, all covers were assumed defined over $\mathbf{C}$, and could be regarded either as covers of complex manifolds or of complex algebraic varieties. By the technique of specialization (cf. [Gr]) and the fact that étale covers are rigid, every branched cover $X \to \mathbf{P}^1_{\mathbf{C}}$ whose branch locus is defined over $\overline{\mathbf{Q}}$ will itself be defined over $\overline{\mathbf{Q}}$; i.e., X is induced by a cover $X_{\overline{\mathbf{Q}}} \to \mathbf{P}^1_{\overline{\mathbf{Q}}}$ of algebraic curves. A similar statement holds for Hurwitz spaces and families. The problem we wish to consider is finding *number fields* over which these structures are defined. To do this we need to study the action of $\mathrm{Gal}_K \overline{\mathbf{Q}}$, for K a number field.

2.1. LEMMA. *Let Y be a K-variety with K-point x, where K is a field. Then the natural sequence*

$$1 \to \pi_1(Y \times_K \overline{K}) \to \pi_1(Y) \to \mathrm{Gal}_K \overline{K} \to 1$$

is split exact.

Proof. Exactness is clear. To see the splitting, apply the functor π_1 to

$$\begin{tikzcd} \operatorname{Spec} K \arrow[r, "x"] \arrow[dr, "\text{identity}"'] & Y \arrow[d] \\ & \operatorname{Spec} K \end{tikzcd} \qquad \square$$

Apply this lemma to $Y = \mathbf{P}^1_K - \{n\ K\text{-points}\}$, for a number field K. The splitting then defines an action of the arithmetic fundamental group $\pi_1(K) = \mathrm{Gal}_K \overline{\mathbf{Q}}$ on the geometric fundamental group $\hat{F} = \pi_1(Y_{\overline{K}})$ (where $\hat{F}$ is the profinite completion of the group F on generators $x_1, \dots, x_n$ and the single relation $\prod x_i = 1$). The crux of the matter is to understand this action. One piece of information is:

2.2. COROLLARY (cf. [Fr1], [Bel]). *Let K be a number field, and $\hat{F}$ the profinite group on $x_1, \dots, x_n$ subject to $\prod x_i = 1$. Let $\omega \in \mathrm{Gal}_K \overline{\mathbf{Q}}$ and let χ be the cyclotomic character. Let $\Gamma = \mathrm{Gal}_K \overline{\mathbf{Q}}$ act on $\hat{F}$ as in Lemma 2.1, for $Y = \mathbf{P}^1_K - \{r\ K\text{-valued points}\}$. Then x_i^ω is conjugate to $x_i^{\chi(\omega)}$ in F.*

Proof. Since $\langle x_i \rangle$ is the decomposition group of some point over the L-rational branch point ξ_i, we see that $\langle x_i \rangle^\omega$ is some other decomposition group. In particular, $x_i^\omega \sim x_i^{a_i}$ for some (profinite) power $a_i \in \hat{\mathbf{Z}}^*$. By looking at the abelianization of $\hat{F}$ and using the relation $\prod x_i = 1$, we find that all the a_i are equal. It now suffices to look at the cyclic covers branched at ξ_i and ξ_r to see that ω acts on the generators through its action on roots of unity. $\square$

Remark. The above results can be reinterpreted as follows:

(a) 2.1: Given $\omega \in \Gamma = \mathrm{Gal}_K \overline{K}$, let ω^* be the induced K-morphism on Y. Then $\omega \mapsto (\omega^*)^{-1}$ is a homomorphism $\Gamma \to \mathrm{Aut}_K(Y_{\overline{K}})$. Pulling back the pro-universal cover $\mathscr{X} \to Y$ by $(\omega^*)^{-1}$ yields $\mathscr{X}^\omega$, given by

$$\begin{tikzcd} \mathscr{X}^\omega \arrow[r, "\omega'"] \arrow[d, "\pi^\omega"'] & \mathscr{X} \arrow[d, "\pi"] \\ Y \arrow[r, "(\omega^*)^{-1}"] & Y \end{tikzcd}.$$

Pick a $\overline{K}$-valued base point on $\mathscr{X}$; via inverse image we obtain a base point on $\mathscr{X}^\omega$. By universality, $\mathscr{X} \xrightarrow{\pi} Y_{\overline{K}}$ is K-isomorphic to $\mathscr{X}^\omega \xrightarrow{\pi^\omega} Y_{\overline{K}}$. There is a unique such isomorphism sending base point to base point. Identifying $\mathscr{X}^\omega$ with $\mathscr{X}$ via this $\overline{K}$-isomorphism, we may view ω' as a K-automorphism of $\mathscr{X}$, i.e. an element of $\pi_1(Y)$.

(b) 2.2: Given a G-cover $X \to \mathbf{P}^1_K$ with description g, branched at r K-valued points, there is an induced G-cover $X^\omega \to \mathbf{P}^1_K$, say with description h. Let $n = \# G$, and let $\omega(\zeta_n) = \zeta_n^a$ (where ζ_n is a primitive nth root of unity). Then $h_i \sim g_i^a$ for all i.

2.3. PROPOSITION. *Let G be a finite group generated by $g_1, \dots, g_r$. Let n be the least common multiple of the orders of the elements g_i. Identify $(\mathbf{Z}/n)^*$ with $\mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\zeta_n)$ by sending $a \in (\mathbf{Z}/n)^*$ to the map $\zeta_n \mapsto \zeta_n^a$. Let $\mathscr{P}$ (resp. $\tilde{\mathscr{P}}$) be the moduli space of G-Galois covers with description g (resp. of Galois covers with description (G, g)).*

(a) *The universal Hurwitz family over $\tilde{\mathscr{P}}$ (cf. Prop. 1.2) has a minimum field of definition $\tilde{K}$, viz. the fixed field in $\mathbf{Q}(\zeta_n)$ of*

$$\tilde{V} = \{ j \in (\mathbf{Z}/n)^* \mid (\exists \phi \in \mathrm{Aut}\, G)(\forall i) g_i^j \sim \phi(g_i) \}.$$

(b) *If Z is a direct summand of the centralizer of g_i (for some i), then a Hurwitz family over $\mathscr{P}$ exists and is defined over $\mathbf{Q}(\zeta_n)$. If, moreover, Z is a direct summand of the normalizer of g_i, then there is a minimum field of definition K for such Hurwitz families, viz. the fixed field in $\mathbf{Q}(\zeta_n)$ of*

$$V = \{ j \in (\mathbf{Z}/n)^* \mid (\forall i) g_i^j \sim g_i \}.$$

Proof. Part (a) follows as in Theorem 5.1 of [Fr1], using Proposition 2.2 above. Part (b) is similar, with descent being applied to the universal family over $\mathscr{P}^*$ (cf. Proposition 1.2), and proceeding as in the proof of Prop. 1.4(b). (Cf. also the proof of Proposition 2.8 below, which is similar.) $\square$

Remark. Unless $\mathscr{P}$ (resp. $\tilde{\mathscr{P}}$) is geometrically connected, the above proposition does not imply that any of its connected components (or families over them) are themselves defined over the field described above, or even over $\mathbf{Q}^{ab}$. The problem of determining these fields of definition seems to be a much deeper one. Cf. also the note after Theorem 5.1 of [Fr1].

Recall that given a structure (e.g., a variety, or a cover) defined over an algebraically closed field K, its *field of moduli* is the fixed field in K of those $\omega \in \operatorname{Aut} K$ which carry the structure to an isomorphic copy of itself.

Parallel to 1.4(a), it follows that the spectrum of the field of moduli of a G-Galois cover is a coarse moduli space for the appropriate functor.

2.4. *Example.* Let $X \xrightarrow{\pi} \mathbf{P}^1_{\mathbf{C}}$ be a (complex) G-cover branched at $\xi = (\xi_1, \ldots, \xi_r)$, with description $g = (g_1, \ldots, g_r)$, relative to a standard homotopy basis $\sigma = (\sigma_1, \ldots, \sigma_r)$ at a base point ξ_0. Acting on the cover by complex conjugation induces a new cover $\bar{X} \xrightarrow{\bar{\pi}} \mathbf{P}^1_{\mathbf{C}}$, with branch locus $\bar{\xi}$ and description g relative to the homotopy basis $\bar{\sigma}$ at $\bar{\xi}_0$. If the ξ_i are all real, we may compute the description of $\bar{X} \xrightarrow{\bar{\pi}} \mathbf{P}^1_{\mathbf{C}}$ relative to σ, and in particular see if the two covers are isomorphic—hence whether the field of moduli is real. For example, let $r = 3$. If all ξ_i are real, and $\xi_0 < \xi_1 < \xi_2 < \xi_3$, then the loops σ_1 and σ_3 may be chosen to have support which is invariant under complex conjugation. The cover $\bar{X} \xrightarrow{\bar{\pi}} \mathbf{P}^1$ is then seen to have description $(g_1^{-1}, g_1 g_3, g_3^{-1})$ relative to σ. In particular, if g_1 and g_3 are involutions, then the new cover is isomorphic to the old, and the field of moduli is real. $\square$

Unfortunately, since all other automorphisms of $\mathbf{C}$ (or, for that matter, of $\overline{\mathbf{Q}}$) are discontinuous, the method of the above example cannot be used to compute the field of moduli in terms of the description and the base points. Instead, according to Prop. 2.9 below, the field of moduli of a G-cover is not in general a function of the description and the field of definition of the branch point.

2.5. Proposition. *Let $X \to \mathbf{P}^1$ be a Galois branched cover with description (G, g), branched over algebraic points. Then the field of moduli of the cover is a field of definition of the cover, and hence is the minimum field of definition.*

Proof. Let K be the field of moduli, let ξ be a K-valued point of $\mathbf{P}^1$ over which X is unbranched, and let $\hat{\xi}$ be a $\overline{\mathbf{Q}}$-point of X lying over ξ. For each $\omega \in \mathrm{Gal}_K\overline{\mathbf{Q}}$, there is a unique isomorphism i_ω from the original cover to the pullback via ω, such that $i_\omega(\hat{\xi}) = \hat{\xi}$. These isomorphisms are compatible, and so (as in Theorem 5.1 of [Fr1]) the cover descends to K. □

The analog of 2.5 for G-Galois cover fails, as the following example shows. (Also cf. [Fr1], §6, Ex. 8.)

2.6. *Example.* There is an H-Galois cover of $\mathbf{P}^1$ (where H is the quaternion group of order 8) whose field of moduli is $\mathbf{Q}$, but which is not defined even over $\mathbf{R}$. Namely, let $X \to \mathbf{P}^1$ be the H-Galois cover branched at $x = 1,2,3$, with branch description $(i, j, -k)$ relative to a standard homotopy basis at base point $x = 0$. This H-cover is defined over $\overline{\mathbf{Q}}$, and any elements of $\mathrm{Gal}_{\mathbf{Q}}\overline{\mathbf{Q}}$ takes the cover to one branched at the same points, say with description (a,b,c). Here a,b,c are respectively conjugate to $i, j, -k$ and $abc = 1$. It follows that $a = \pm i$, $b = \pm j$, $c = \pm k$, and that there is in fact an element $\gamma \in H$ conjugating the original description to the new description. (In the terminology of Prop. 2.10 below, H together with this description is "inner rigid.") Thus the induced H-cover is isomorphic to the original one, and so the field of moduli is indeed $\mathbf{Q}$. But on the other hand, if the H-cover were defined over $\mathbf{R}$, then complex conjugation would induce an involution λ on the complex points of X, which would preserve the H-structure. In particular, if ξ is the (complex-valued) base point over $x = 0$, then $\lambda(\xi)$ lies over $x = 0$, and so $\lambda(\xi) = \ell(\xi)$ for some $\ell \in H$. But then for all $g \in H$, $\lambda(g(\xi)) = g(\lambda(\xi)) = g\ell(\xi)$. Setting $g = \ell$, we have $\xi = \lambda^2(\xi) = \ell^2(\xi)$, and so $\ell^2 = 1$. Thus $\ell = \pm 1$. But then ℓ is in the center, and so the description of X with respect to $\ell(\xi)$ is the same as that with respect to ξ. But according to Example 2.4, the description at $\ell(\xi)$ is $(-i, j, k)$. This is a contradiction, and so the H-cover is not in fact defined over $\mathbf{R}$. □

Still, G-covers do satisfy the following two propositions:

2.7. Proposition. *For G-Galois covers, the field of moduli is the intersection of the fields of definition.*

Proof. Let $X \to \mathbf{P}^1_{\overline{\mathbf{Q}}}$ be a G-Galois cover, and K its field of moduli. The proof proceeds analogously to the remark following 1.5, with K playing the role of the moduli space of G-Galois covers, and fields of definition of $X \to \mathbf{P}^1$ playing the role of parameter spaces for families of G-covers. Namely, choose an unramified base point p on X, lying over a $\mathbf{Q}$-point of $\mathbf{P}^1$. Each $\omega \in \mathrm{Gal}_K\overline{\mathbf{Q}}$ induces a G-Galois pullback $X^\omega \to \mathbf{P}^1_{\overline{\mathbf{Q}}}$, together with a base point p^ω. By definition of K, there is a $\overline{\mathbf{Q}}$-isomorphism of covers $i: X^\omega \to X$. Since X is Galois, there is an element $g \in G$ carrying p to $i(p^\omega)$. Here, i and hence g are uniquely determined up to composition with an element in the center Z of G. The assignment $\omega \mapsto g$ thus defines a map $\mathrm{Gal}_K\overline{\mathbf{Q}} \to G/Z$ which yields an element $\xi \in H^1(K, G/Z)$. Thus, as in the remark following 1.5, it suffices to show that the number field K is the intersection of fields of cohomological dimension 1.

For each $\omega \in \mathrm{Gal}_K\overline{\mathbf{Q}}$ let L_ω be the fixed field of ω. By the Artin–Schreier Theorem, if $\omega \neq 1$ has order 2 then $L_\omega \approx \mathbf{R} \cap \overline{\mathbf{Q}}$, and otherwise ω has infinite order. In the latter case $\mathrm{Gal}_{L_\omega}\overline{\mathbf{Q}}$ is a free profinite group, so c.d.$L_\omega = 1$. If K is not real (i.e., has no embedding into $\mathbf{R}$), it follows that each nontrivial $\omega \in \mathrm{Gal}_K\overline{\mathbf{Q}}$ has infinite order. Hence in this case, K is the intersection of a collection of fields of c.d. 1, namely the fields L_ω. In the general case, we may write $K = K_1 \cap K_2$, where K_1 and K_2 are number fields, neither of which is real. By the special case, each K_i is the intersection of c.d. 1 fields. Hence so is K. □

2.8. PROPOSITION. *Let* $X \xrightarrow{\pi} \mathbf{P}^1$ *be a* G*-Galois cover branched at* $\xi = (\xi_1, \ldots, \xi_r)$, *and with description* $g = (g_1, \ldots, g_r)$. *Let* K *be the field of moduli of* X *as a* G*-Galois cover.*

(a) *For some integer* n, $K(\zeta_n)$ *is a field of definition of* X *as a* G*-Galois cover.*

(b) *Suppose the center* $Z \subset G$ *is a direct summand of the centralizer of some* g_i, *and that* ξ_i *is a* K*-valued point. Then the integer* n *in part* (a) *may be chosen to be the order of* g_i.

(c) *Suppose that either*

(i) Z *is a direct summand of* G*—e.g.,* G *is centerless or abelian, or*

(ii) Z *is a direct summand of the normalizer of some* $\langle g_i \rangle$, *where* ξ_i *is* K*-valued.*

Then K *is itself a field of definition of* X *as a* G*-Galois cover.*

Proof. (a) It suffices to show that $L = K\mathbf{Q}^{ab}$ is a field of definition. This follows as in [Be1], Thm. 1, from the fact that L has c.d. 1 (cf. [Se], II 3.3, Prop. 9).

(b) We may assume $i = 1$. Let $K' = K(\zeta_n)$, where n is the order of g_1. Let C be a circle centered at ξ_1 of radius sufficiently small that for all $j \neq 1$, no conjugate (over K) of any ξ_j lies on or inside C. We may choose C so as to contain a K-valued point ξ_0. Choose a standard homotopy basis $\sigma = (\sigma_1, \ldots, \sigma_r)$ for $\mathbf{P}^1 - \{\xi_1, \ldots, \xi_r\}$ at ξ_0, such that C is the support of σ_1, and choose a point $\hat{\xi}_0 \in X$ over ξ_0. Let $h = (h_1, \ldots, h_r)$ be the description of the cover relative to σ at base point $\hat{\xi}_0$, and for $\omega \in \mathrm{Gal}_{K'}\overline{\mathbf{Q}}$ let $h^\omega = (h_1^\omega, \ldots, h_r^\omega)$ be the description of the induced cover X^ω (cf. the remark after 2.2) relative to a standard basis which includes σ_1. Then each h_j^ω is conjugate to g_j, and $h_1^\omega = h_1$, by 2.2 and the definition of K'. Since $K' \supset K$, there is a $\gamma \in G$ such that $h_j^\omega = h_j^\gamma$ for all j. Thus γ lies in the centralizer of h_1. This induces a homomorphism $\Gamma' = \mathrm{Gal}_{K'}\overline{\mathbf{Q}} \to C(h_1)/Z$, since γ is unique up to multiplication by Z. But Z is a direct summand of $C(g_1)$, and applying the inner automorphism taking g_1 to h_1 we observe that Z is also a direct sumand of $C(h_1)$. Thus we obtain a homomorphism $\Gamma' = \mathrm{Gal}_{K'}\overline{\mathbf{Q}} \xrightarrow{\mu} C(h_1) \subset G$, such that $(X^\omega, \hat{\xi}_0) \approx (X, \mu(\omega)(\hat{\xi}_0))$ as G-covers, for all $\omega \in \Gamma'$. So as in [Be1], Thm. 1, the cover descends to K'.

(c) Arguing as in (b) above, and considering $\omega \in \Gamma = \mathrm{Gal}_K\overline{\mathbf{Q}}$, we obtain a homomorphism $\Gamma \to G/Z$. In case (i), we compose with $G/Z \to G$ to complete the proof. In case (ii) (which actually subsumes (i)), we observe that $h_1^\omega = h_1^m$, where $\omega(\zeta_n) = \zeta_n^m$ (cf. 2.2). Thus γ lies in the normalizer of $\langle h_1 \rangle$. This induces a homomorphism $\Gamma \to N(\langle h_1 \rangle)/Z$. Hypothesis (ii) implies (as in (b)) that Z is a direct summand of $N(\langle h_1 \rangle)$, and so we obtain a lifting $\Gamma \to N(\langle h_1 \rangle)$. The proof is then completed as before. $\square$

2.9. PROPOSITION. *Let $\mathcal{P}$ be the moduli space of Galois G-covers with description g, and let $\mathcal{P}^0$ be a connected component of $\mathcal{P}$. Let $\mathcal{P}^0 \xrightarrow{\pi} (\mathbf{P}^1)^r - \Delta$ be the canonical map. Then there is a number field L such that every G-cover in $\mathcal{P}^0$ with $\mathbf{Q}$-valued branch points has field of moduli contained in L, if and only if π is an isomorphism.*

Proof. First assume that π is an isomorphism. Let $\mathcal{H}^* \to \mathcal{P}^*$ be the universal family of pointed G-covers with description g, and let $\mathcal{P}^{*0}$ be a component of $\mathcal{P}^*$ lying over $\mathcal{P}^0$. Let $\mathcal{P}' \to (\mathbf{P}^1)^r - \Delta$ be the Galois closure of $\mathcal{P}^{*0} \to (\mathbf{P}^1)^r - \Delta$ and let $\mathcal{H}' \to \mathcal{P}' \times \mathbf{P}^1$ be the pullback of $\mathcal{H}^*$ to $\mathcal{P}'$. For any σ in the Galois group of $\mathcal{P}'$, the pullback of $\mathcal{H}' \to \mathcal{P}' \times \mathbf{P}^1$ by σ is isomorphic to $\mathcal{H}' \to \mathcal{P}' \times \mathbf{P}^1$ as a G-cover, since π is an isomorphism. We may regard the G-cover $\mathcal{H}' \to \mathcal{P}' \times \mathbf{P}^1$ and the map $\mathcal{P}' \to (\mathbf{P}^1)^r - \Delta$ as defined over a number field L. Over any L-valued point ξ of $(\mathbf{P}^1)^r - \Delta$, the fibre $\mathcal{P}'_\xi$ is a disjoint union of spectra of finite field extensions of L. Let L' be one of these field extensions, and let $X \to \mathbf{P}^1_{L'}$ be the corresponding G-cover. Since any $\omega \in \mathrm{Gal}_L L'$ lifts to an element of $\mathrm{Gal}_{(\mathbf{P}^1)^r - \Delta} \mathcal{P}'$, the pullback of $X \to \mathbf{P}^1$ by ω is again isomorphic to $X \to \mathbf{P}^1$. Thus L contains the field of moduli.

Conversely, assume there is such an L. With $\mathcal{H}' \to \mathcal{P}' \times \mathbf{P}^1$ as above, we may assume (possibly after enlarging L) that the various spaces and maps are defined over L. By Hilbert's Irreducibility Theorem ([Hi], [La]) applied to the extension $\mathcal{P}' \to (\mathbf{P}^1_{\mathbf{Q}})^r - \Delta$, we see that for some $\mathbf{Q}$-valued point ξ of $(\mathbf{P}^1)^r - \Delta$, the fibre of $\mathcal{P}'$ is irreducible, i.e., is the spectrum of some field L' containing L. Now each element of $\mathrm{Gal}_L L'$ is induced by an element of $\mathrm{Gal}_{(\mathbf{P}^1)^r - \Delta} \mathcal{P}'$ and yet the latter acts transitively on the fibre of $\mathcal{P}' \to (\mathbf{P}^1)^r - \Delta$. Since the cover corresponding to ξ has field of definition contained in L, it follows that any two points of $\mathcal{P}'$ in the same fibre over $(\mathbf{P}^1)^r - \Delta$ correspond to the same point of $\mathcal{P}^0$, i.e., that π is an isomorphism. $\square$

Question. If π is an isomorphism, is there a common field of *definition* for the G-covers in $\mathcal{P}^0$ with $\mathbf{Q}$-valued branch points?

Remarks. (i) In the statement of the above proposition, we may replace $\mathbf{Q}$ by L, as is clear from the proof.

(ii) In general, given (G, g), π will *not* be an isomorphism and so *no* number field (or even Hilbertian field, such as $\mathbf{Q}^{ab}$) will suffice to contain all the fields of moduli, much less the fields of definition. For example, if $g_1, \ldots, g_r$ generate G, and g_1 is not central, then $(g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_r, g_r^{-1})$ yields a π which is not an isomorphism. On the other hand, in the 3 point case, π is *always* an isomorphism (by the triple transitivity of automorphisms), yet the covering will not always be defined over $\mathbf{Q}^{ab}$. Cf. Prop. 2.11 below.

(iii) By 2.9, $\pi_1(\mathbf{P}^1_L - (r \text{ points}))$ depends on the position of the r points, for any number field L and $r > 3$. This also is the case for $L = \mathbf{Q}^{ab}$, by (ii) above. This relates to the corresponding fact for $L = \overline{\mathbf{F}}_p$, by specialization (i.e. by passing to the integral closure of $\mathbf{Z}$ in $\mathbf{Q}^{ab}$, and then passing to a residue field). $\square$

Define a pair (G, g) to be *inner* (resp. *outer*) *rigid* if the corresponding map on moduli $\mathscr{P} \to (\mathbf{P}^1)^r - \Delta$ (resp. $\tilde{\mathscr{P}} \to (\mathbf{P}^1)^r - \Delta$) are isomorphisms. Equivalently, (G, g) is inner rigid if every g' whose entries generate G and which satisfies $\prod g_i' = 1$ is a (uniform) conjugate of g by an element of G. Similarly, (G, g) is outer rigid if for every such g' there is a $\phi \in \operatorname{Aut} G$ taking g to g'. Compare with Thompson's notion of "rigidity" [Th1] and Belyi's notions of Γ and Γ' [Be1]. Special cases and parts of the following result appeared in [Th1], [Be1], and [Fr2].

2.10. PROPOSITION. (a) *If (G, g) is outer rigid, then each Galois cover with description (G, g) and with $\mathbf{Q}$-valued branch points is defined over the field $\tilde{K}$ of* 2.3 (a), *as a cover of $\mathbf{P}^1$.*

(b) *If (G, g) is inner rigid, then each G-Galois cover with description g and with $\mathbf{Q}$-valued branch points is defined (as a G-cover) over $\mathbf{Q}^{ab}$. If Z is a direct summand of the centralizer (resp. normalizer) of some g_i, then it is defined over $\mathbf{Q}(\zeta_n)$, where $n =$ l.c.m. (order g_j) (resp. over the field K of* 2.3 (*b*)).

Proof. (a) By 2.3 (a) and specialization of the branch locus.

(b) By 2.2, the field of moduli is contained in $\mathbf{Q}^{ab}$, hence so is the field of definition (by 2.8 (a)). In the cases that Z is a direct summand, apply 2.3 (b) and then specialize the branch locus. $\square$

Remarks. (i) Part (b) can be used to obtain groups as Galois groups over abelian extensions of $\mathbf{Q}$—as was done in the papers listed above, and in [Be2], [Ma], [Th2], [Th3].

(ii) The second part of (b) does not always hold if the assumption of Z is dropped. Cf. Example 2.6 above.

(iii) If (G, g) is (inner or outer) rigid, then the proposition applies to $(G/N, \bar{g})$, even if that is not rigid (as indeed it may not be).

(iv) By a theorem of Magnus, the free group F_2 on two generators a, b is inner rigid, relative to the generating set (a, b, c), where $c = b^{-1}a^{-1}$. But this group is not finite, and so Prop. 2.10 cannot be applied in order to deduce that the universal cover (and hence every G-cover) of $\mathbf{P}^1 - \{0, 1, \infty\}$ is defined over $\mathbf{Q}^{ab}$. This approach would work if instead the pro-universal cover could be used, for example if the profinite completion $\hat{F}_2$ were inner rigid. But in fact

2.11. PROPOSITION. *Not every G-cover of $\mathbf{P}^1 - \{0, 1, \infty\}$ is defined over $\mathbf{Q}^{ab}$. In fact for* any *K strictly contained in $\overline{\mathbf{Q}}$, there is a group G and a G-cover of $\mathbf{P}^1 - \{0, 1, \infty\}$ which is not defined over K.*

Proof. This follows from the corollary to Thm. 4 in [Be1]. $\square$

2.12. COROLLARY. *$\hat{F}_2$ is not inner rigid, relative to (a, b, c).*

Proof. By 2.11 and the remark (iv) prior to that result. $\square$

§3. Groups as Galois groups. In this section we address more directly the problem of building Galois covers of the line with a given description and defined over a given field. In its most general form, this question asks for a description of $\pi_1(U)$, where U is a Zariski open subset of $\mathbf{P}^1_K$, for K a number field. In this form the problem is, at present, totally inaccessible. After all, as discussed in section 2, it is difficult to make any general statements about the field of moduli of covers of $\mathbf{P}^1$. In certain situations, however, such statements can be made—e.g., if the description is "inner rigid" (cf. Proposition 2.10). Below we show how under related situations as well, covers can be constructed over a given field (e.g., $\mathbf{Q}$) by using branch points defined over a larger field. The covers $X \to \mathbf{P}^1_K$ that we wish to construct will generally be *regular*, in the sense that K is algebraically closed in the function field of X. (Of course *every* cover $X \to \mathbf{P}^1_K$ can be factored as $X \to \mathbf{P}^1_L \to \mathbf{P}^1_K$, where $X \to \mathbf{P}^1_L$ is regular and $\mathbf{P}^1_L \to \mathbf{P}^1_K$ is induced by extension of constants.) Thus by applying Hilbert's Irreducibility Theorem, we can obtain infinitely many linearly disjoint Galois extensions of K with the given group.

The techniques in this section are concerned with the construction of special types of covers and towers of covers, and involve analyzing the internal structure of the groups involved. This is quite different from the approach in [Ha1] and [Ha2] (which studied Galois covers of the arithmetic disc, rather than the arithmetic line).

3.1. *Example.* Cyclic groups: To illustrate some of the general ideas, we begin with the most naive groups and ask how to build regular cyclic covers of $\mathbf{P}^1_{\mathbf{Q}}$. If $X \to \mathbf{P}^1_{\mathbf{C}}$ is any $\mathbf{Z}/n$-Galois cover with branching over $\mathbf{Q}$-points, then it is inner rigid, with field of definition $\mathbf{Q}(\zeta_n)$. Thus for $n > 2$, no $\mathbf{Z}/n$-cover branched at $\mathbf{Q}$-points is defined (as a Galois cover) over $\mathbf{Q}$. But regular cyclic covers of $\mathbf{P}^1_{\mathbf{Q}}$ can be constructed by using a variant of rigidity, and using nonrational branch points which are conjugate over $\mathbf{Q}$. To do this, let $K = \mathbf{Q}(\zeta_n)$ and let $\mathbf{P}^1_K \xrightarrow{[n]} \mathbf{P}^1_K$ be the $\mathbf{Z}/n$-cover branched at the two points ∞ and ζ, where ζ is a primitive nth root of unity. Then the composition $\mathbf{P}^1_K \xrightarrow{[n]} \mathbf{P}^1_K \to \mathbf{P}^1_{\mathbf{Q}}$ is not Galois; let $Y \to \mathbf{P}^1_{\mathbf{Q}}$ be the Galois closure. Thus Y is the fibre product over $\mathbf{P}^1_K$ of all the $\mathbf{Z}/n$-covers of $\mathbf{P}^1_K$ each of which is branched at the two points ζ^i, ∞, with $i \in (\mathbf{Z}/n)^*$.

Now $\mathrm{Gal}_{\mathbf{P}^1_{\mathbf{Q}}} Y$ is the wreath product of $(\mathbf{Z}/n)^*$ with $\mathbf{Z}/n$:

$$1 \to (\mathbf{Z}/n)^{\phi(n)} \to W \to (\mathbf{Z}/n)^* \to 1.$$

The addition map $(\mathbf{Z}/n)^{\phi(n)} \to \mathbf{Z}/n$ extends to a surjection $W \to \mathbf{Z}/n$ which kills the lifted subgroup isomorphic to $(\mathbf{Z}/n)^*$. By Galois theory, this corresponds to an intermediate extension $X_n \to \mathbf{P}^1_{\mathbf{Q}}$ which is Galois with group $\mathbf{Z}/n$. Since the only arithmetic part of the extension was $K/\mathbf{Q}$ with group $(\mathbf{Z}/n)^*$, it is clear that X_n is regular. $\square$

Remark. In the above example, the cover $X_n \to \mathbf{P}^1_{\mathbf{Q}}$ is branched at ∞ and at all the primitive nth roots of unity. If g is a chosen generator of $\mathbf{Z}/n$, then the branching data (written multiplicatively) is $(g^{-\phi(n)}, g, \ldots, g)$. If L is any number field, let $d=[L(\zeta_n):L]$, and let α be an $L(\zeta_n)$-point of $\mathbf{P}^1$ having d distinct conjugates over L. Then the above construction yields $\mathbf{Z}/n$-covers of $\mathbf{P}^1_L$ branched at ∞ and at all the conjugates of α, and with branching data $(g^{-d}, g, \ldots, g)$. In particular, X_n has genus 0 only if $n=2$.

3.2. *Example.* Abelian groups: Every abelian group G occurs regularly over $\mathbf{Q}$. Namely, decompose G into a product of cyclic groups, build each factor branched over a different set of points (e.g., as in 3.1), and take the fibre product over $\mathbf{P}^1_{\mathbf{Q}}$. $\square$

3.3. *Example.* Dihedral groups D_n: Let $Y\to\mathbf{P}^1_{\mathbf{Q}}$ be a regular double cover with genus $(Y)=0$. As in Example 3.1, there is a regular $\mathbf{Z}/n$-cover of Y branched at ∞ and at any chosen set of $\mathbf{Q}(\zeta_n)$-points which forms a maximal complete orbit under $\mathrm{Gal}_{\mathbf{Q}}\mathbf{Q}(\zeta_n)$. In particular, these points can be chosen so that the composite extension is not Galois over $\mathbf{P}^1_{\mathbf{Q}}$. The Galois closure then has Galois group isomorphic to the wreath product W of $\mathbf{Z}/2$ with $\mathbf{Z}/n$. But W has a D_n-quotient: If $x\in D_n$ has order n and if x_1, x_2 are generators of the copies of $\mathbf{Z}/n$ in W which are interchanged by the $\mathbf{Z}/2$-action, then $x_1\mapsto x$, $x_2\mapsto x^{-1}$ defines $W\twoheadrightarrow D_n$. Since the quadratic quotient remains the same, we obtain a regular dihedral cover of $\mathbf{P}^1_{\mathbf{Q}}$ which dominates Y. (Observe that if Y were not regular, but instead had $L=$ algebraic closure of $\mathbf{Q}$ in K_Y, then by using $L(\zeta_n)$-points the above construction again yields a D_n-cover of $\mathbf{P}^1_{\mathbf{Q}}$ extending Y—though, of course, this cover will no longer be regular.) $\square$

If, in the above example, we were not interested in controlling the branch locus, we could simply invoke [Sa; Thm. 3.12(f)] (cf. also [Th5]), which showed that given a split exact sequence

$$1\to N\to E\to G\to 1$$

with N abelian, every regular G cover of $\mathbf{P}^1_{\mathbf{Q}}$ is dominated by a regular E-cover of $\mathbf{P}^1_{\mathbf{Q}}$. (On the level of extensions of number fields (e.g., after specializing), the corresponding result appeared in [Ne] and [Fr2; Thm. 2.5].) Thus many groups occur regularly over $\mathbf{P}^1_{\mathbf{Q}}$—e.g., every group of order pq.

Another example of such an extension theorem appears at Theorem 2.2 of [Fr2]. We turn to yet another example of such a result. Let M be a nonabelian simple group such that

(i) $$1\to M\to \mathrm{Aut}\, M\to \mathrm{Out}\, M\to 1 \text{ splits.}$$

This condition is often satisfied. For example, as G. Glauberman pointed out to us, it holds for every sporadic simple group and for every alternating group A_n, $n\geqslant 5$, $n\neq 6$. (To see this, examine Table 1, p. 441, of [AS], in order to see that for each sporadic group, $\#\mathrm{Out}\, M=1$ or 2, and that in the latter case there is a class of involutions outside M. The assertion for A_n is similar, using $\mathrm{Aut}\, A_n=S_n$ for $n\neq 6$.) Next, we assume in addition a generalized rigidity hypothesis: Let $Y\to\mathbf{P}^1_L$ be a Galois cover with description (M, m) (where $m=(m_1,\ldots,m_r)$)

such that the connected component $\mathscr{P}^0 \subset \mathscr{P}$ of Y in the corresponding Hurwitz space (cf. section 1) satisfies

(ii) $\pi : \mathscr{P}^0 \to (\mathbf{P}^1)^r - \Delta$ is an isomorphism, and m is stable under Out M (up to order).

In this case say that (M, m) is an *automorphic description* of the cover Y.

3.4. THEOREM. *Let (M, m) be an automorphic description of a cover of $\mathbf{P}^1_L$, and let $N = M^k$. Let*

$$1 \to N \to E \to G \to 1, \tag{$*$}$$

where $G = \mathrm{Gal}_L F$ for some number field F. Then there is a Galois cover $Y \to \mathbf{P}^1_L$ with group E, dominating the (purely arithmetic) map $\mathbf{P}^1_F \to \mathbf{P}^1_L$.

Of course by Hilbert's Irreducibility Theorem, this shows that E occurs as the Galois group of a field extension of L.

Proof. By assumption on M, there is a split exact sequence

$$1 \to M^k \to \mathrm{Aut}(M^k) \to (\mathrm{Out}\, M)^k \rtimes S_k \to 1,$$

where S_k is the symmetric group, and the semidirect product is Out$N$. Since $(*)$ is a pullback of this sequence along some homomorphism $\rho : G \to (\mathrm{Out}\, M)^k \rtimes S_k$, there is also a splitting homomorphism $\sigma : G \to E$ for $(*)$. Now consider the description $(M^k, (m_1^{(1)}, \ldots, m_r^{(1)}, \ldots, m_1^{(k)}, \ldots, m_r^{(k)}))$, where $m^{(j)}$ denotes the image of $m \in M$ under the jth injection $M \hookrightarrow M^k$. This description has the property that the composition

$$\mathscr{P}^0(N) \to \mathscr{P}(N) \xrightarrow{\ \pi\ } (\mathbf{P}^1)^{rk} - \Delta$$

is an isomorphism, where $\mathscr{P}(N)$ is the associated Hurwitz space and $\mathscr{P}^0(N)$ is the connected component of the cover which is a fibre product of covers in $\mathscr{P}^0 = \mathscr{P}^0(M)$. So we can build an N-cover $Y \to \mathbf{P}^1_F$ at any choice of F-branch points $B_i^{(j)}$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant k$. But ρ describes an action of G on the branch points. Choose the points $B_i^{(j)}$ so that the action of G defined by ρ (or equivalently, by σ followed by conjugation) agrees with the action of G defined by its identification with $\mathrm{Gal}_L F$. Then the composition $Y \to \mathbf{P}^1_F \to \mathbf{P}^1_L$ is Galois with group E. $\square$

3.5. COROLLARY. *Any extension E of a Galois group $G = \mathrm{Gal}_{\mathbf{Q}} F$ by a product of A_n's with $n \geqslant 5$, $n \neq 6$, itself occurs as a Galois group over $\mathbf{Q}$.*

Proof. We have already noted that A_n satisfies condition (i) prior to 3.4. In order to satisfy (ii), we use a classical construction of an A_n-Galois cover $Y \to \mathbf{P}^1_{\mathbf{Q}}$, due to Hilbert [Hi]. (Cf. also [Sh] and [Fr1].) First let $Y_{\mathbf{C}} \to \mathbf{P}^1_{\mathbf{C}}$ be the S_n-cover branched at three rational points a, b, c with description $((12), (12 \ldots n),$

($n \ldots 431$)). This description is inner rigid, with field of definition $\mathbf{Q}$. Now let X be the intermediate cover corresponding to the normal subgroup A_n. By the Hurwitz formula, X has genus 0. Since X has a $\mathbf{Q}$-point (viz. the ramification point lying over $a \in \mathbf{P}^1_{\mathbf{Q}}$), there is an isomorphism $X \approx \mathbf{P}^1$ defined over $\mathbf{Q}$. The map $Y \to X = \mathbf{P}^1_{\mathbf{Q}}$ is then a (regular) A_n-Galois cover. Since this cover is branched only at three points (viz. the two points on X over b, and the point over c), the map π of condition (ii) is an isomorphism. Since the nontrivial outer automorphism merely interchanges the points on X over b, the description is stable up to order, and so (ii) holds. $\square$

3.6. COROLLARY (Thompson [Th4], Fried [Fr2]). *Suppose that G occurs as a Galois group over a number field L. Then any extension of G by a product of $G_2(p)$'s with $p > 5$, also occurs as a Galois group over L.*

Proof. Thompson has shown [Th2] that $G_2(p)$ is inner rigid with field of definition $\mathbf{Q}$. Also, every automorphism of $G_2(p)$ is inner, so the exact sequence splits. $\square$

3.7. COROLLARY. *Let G be any group each of whose composition factors admits an automorphic description over a number field L. Then G occurs as a Galois group over L.*

Proof. Induct along a principal series. $\square$

REFERENCES

[AS] M. ASCHBACHER AND G. SEITZ, *On groups with a standard component of known type*, Osaka J. of Math. **13** (1976), 439–482.

[Be1] G. V. BELYI, *On Galois extensions of a maximal cyclotomic field*, Math USSR Izvestija **14** (1980), 247–256.

[Be2] ———, *On extensions of the maximal cyclotomic field having a given classical Galois group*, Crelle's J. **341** (1983), 147–156.

[Fr1] M. FRIED, *Fields of definition of function fields and Hurwitz families—Groups as Galois groups*, Comm. Alg. **5** (1977), 17–82.

[Fr2] ———, *On reduction of the inverse Galois problem to simple groups*, Proceedings of the Rutgers Group Theory Year, 1983–1984, 289–301.

[Fr3] ———, *Degeneracy in the branch locus of Hurwitz schemes*, Proc. of 1972 Number Theory Conf. (Univ. Colo.), 87–94.

[FB] M. FRIED AND R. BIGGERS, *Moduli spaces of covers and the Hurwitz monodromy group*, Crelle's J. **335** (1983), 87–121.

[Fu] W. FULTON, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. Math., series 2, **90** (1969), 543–573.

[Gr] A. GROTHENDIECK, *Revêtements étales et groupe fondamental* (SGA1), LNM 224, Springer, NY, 1970.

[Ha1] D. HARBATER, *Mock covers and Galois extensions*, Journal of Algebra **91** (1984), 281–293.

[Ha2] ———, *Algebraic rings of arithmetic power series*, Journal of Algebra **91** (1984), 294–319.

[Hi] D. HILBERT, *Über die Irreduzibilitat ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Crelle's J. **110** (1892), 264–286.

[La] S. LANG, *Fundamentals of Diophanine Geometry*, Springer, NY, 1983.

[Ma] B. MATZAT, *Zur Konstruction von Zahl- und Funktionkorpern mit Vorgegebenen Galoisgruppe*, Karlsruhe, 1980.

[Ne] J. NEUKIRCH, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Inv. Math. **21** (1973), 59–116.

[Sa] D. SALTMAN, *Generic Galois extensions and problems in field theory*, Advances in Math. **43** (1982), 250–283.

[Se] J.-P. SERRE, *Cohomologie Galoisienne*, LNM 5, Springer, NY, 1964.

[Sh] K.-Y. SHIH, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.

[Th1] J. THOMPSON, *Some finite groups which appear as* $\mathrm{Gal}\, L/K$, *where* $K \subset \mathbf{Q}(\mu_n)$, J. Alg. **89** (1984), 437–499.

[Th2] ———, *Some finite groups of type* G_2 *which appear as Galois groups over* $\mathbf{Q}$, Preprint, 1983.

[Th3] ———, PSL_3 *and Galois groups over* $\mathbf{Q}$, Preprint, 1983.

[Th4] ———, *Some finite groups which appear as Galois groups over* $\mathbf{Q}$, Preprint, 1983.

[Th5] ———, *Regular Galois extensions of* $\mathbf{Q}(x)$, Preprint, 1984.

COOMBES: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OKLAHOMA, NORMAN, OKLAHOMA 73019

CURRENT ADDRESS: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN 48109

HARBATER: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PENNSYLVANIA 19104-3859