THE INVERSE GALOIS PROBLEM AND RATIONAL POINTS ON MODULI SPACES

Michael D. Fried[*], *UC Irvine*
Helmut Völklein[**], *U of Florida and Universität Erlangen*

Abstract: We reduce the regular version of the Inverse Galois Problem for any finite group G to finding one rational point on an infinite sequence of algebraic varieties. As a consequence, any finite group G is the Galois group of an extension $L/P(x)$ with L regular over any PAC field P of characteristic zero. A special case of this implies that G is a Galois group over $\mathcal{F}_p(x)$ for almost all primes p.

§0. INTRODUCTION

Many attempts have been made to realize finite groups as Galois groups of extensions of $\mathcal{Q}(x)$ that are regular over $\mathcal{Q}$ (see the end of this introduction for definitions). We call this the "regular inverse Galois problem." We show that to each finite group G with trivial center and integer $r \geq 3$ there is canonically associated an algebraic variety, $\mathcal{H}_r^{\text{in}}(G)$, defined over $\mathcal{Q}$ (usually reducible) satisfying the following.

Fundamental Property: *There exists a Galois extension of $\mathcal{Q}(x)$, regular over $\mathcal{Q}$, with Galois group isomorphic to G and with r branch points, if and only if $\mathcal{H}_r^{\text{in}}(G)$ has a $\mathcal{Q}$-rational point. (This holds if $\mathcal{Q}$ is replaced by any field of characteristic 0).*

This is contained in Corollary 1 (in §2.1). Theorem 1, our main result, gives a more general formulation that applies to any finite group. The Fundamental Property reduces the regular inverse Galois problem to finding $\mathcal{Q}$-points on certain (reducible) varieties. The first step towards this is to show that (under certain conditions) there exist absolutely irreducible components of $\mathcal{H}_r^{\text{in}}(G)$ that are defined over $\mathcal{Q}$. The components of $\mathcal{H}_r^{\text{in}}(G)$ are in one-one correspondence with the orbits of the *Hurwitz monodromy group* in its action on certain classes of generating systems of G (see §1.3).

[*]Supported by NSF grant DMS-8702150 and BSF grant #87-00038
[**]Supported by NSA grant MDA 904-89-H-2028

AMS Subject classification: 11G35, 12F10, 14D20, 14E20, 14G05, 20B25, 20C25

Keywords: Riemann's existence theorem; Galois groups; Nielsen classes; Braid and Hurwitz monodromy groups; PAC-fields.

Using a theorem of Conway and Parker [CP] on such group actions, we conclude that the space $\mathcal{H}_r^{\rm in}(G)$ has an (absolutely) irreducible component defined over $\mathcal{Q}$ if we allow r to be large and replace G by some group with quotient G (see §2.2). The $\mathcal{Q}$-components that we construct this way are generalizations of the classical *Hurwitz spaces*.

It is convenient to introduce the following terminology: A group G is called *regular over a field* k if G is isomorphic to the Galois group of an extension of $k(x)$ that is regular over k. The above has the following immediate corollary for P(seudo)A(lgebraically)C(losed) fields P of characteristic 0: Every finite group is regular over P (Theorem 2). Another corollary (which can be viewed as a special case of the previous one) is that every finite group is regular over the finite prime field $\mathcal{F}_p$ for almost all primes p (Corollary 2).

In §6 we derive an addendum to our main result that is crucial for the preprint [FrVo]. In that paper we prove a long-standing conjecture on Hilbertian PAC-fields P (in the case $\mathrm{char}(P) = 0$): Every finite embedding problem over P is solvable. For countable P this, combined with a result of Iwasawa, implies that the absolute Galois group of P is ω-free. That is, $G(\bar{P}/P)$ is a free profinite group of countably infinite rank, denoted $\hat{F}_\omega$. By a result of [FrJ, 2], every countable Hilbertian field k of characteristic 0 has a Galois extension P with the following properties: P is Hilbertian and PAC, and $G(P/k) \cong \prod_{n=2}^{\infty} S_n$ (where S_n is the symmetric group of degree n). From the above, $G(\bar{k}/P) = G(\bar{P}/P) \cong \hat{F}_\omega$, and we get the exact sequence

$$1 \to \hat{F}_\omega \to G(\bar{k}/k) \to \prod_{n=2}^{\infty} S_n \to 1.$$

Moduli spaces for branched covers of $\mathcal{P}^1$ were already considered by Hurwitz [Hur] in the special case of simple branching (where the Galois group is S_n). Fulton [Fu] showed — still in the case of simple branching — that the analytic moduli spaces studied by Hurwitz are the sets of complex points of certain schemes. Fried [Fr,1] studied more generally moduli spaces for covers of $\mathcal{P}^1$ with an arbitrary given monodromy group $G \subset S_n$ and with a fixed number of branch points. The new moduli spaces $\mathcal{H}_r^{\rm in}(G)$ studied in the present paper are coverings of those previous ones, parametrizing equivalence classes of pairs (χ, h) where χ is a Galois cover of $\mathcal{P}^1$ with r branch points and h is an isomorphism between G and the automorphism group of the cover χ. The extra data of the isomorphism h associated to the points of $\mathcal{H}_r^{\rm in}(G)$ ensures that a $\mathcal{Q}$-rational point corresponds to a cover of $\mathcal{P}^1$ that can be defined over $\mathcal{Q}$ such that also all its automorphisms are defined over $\mathcal{Q}$; the latter condition guarantees that the corresponding function field extension $L/\mathcal{Q}(x)$ is Galois with group G.

The proof of our main result relies on the construction of a family of certain covers of $\mathcal{P}^1$ with no (non-trivial) automorphisms (§4). Then we use the interplay between the spaces $\mathcal{H}_r^{\rm in}(G)$ and moduli spaces $\mathcal{H}_r^{\rm ab}(G, U)$ of equivalence classes of certain covers that are not Galois. Matzat [Ma, 2] has studied the function fields of the absolutely irreducible components of the spaces $\mathcal{H}_r^{\rm in}(G)$ and $\mathcal{H}_r^{\rm ab}(G, U)$ (for $U = 1$) from another point of view (using profinite algebraic fundamental groups).

Because of the essential use we make of the unpublished result [CP] (in the applications of our main result), we supply an appendix where we give a (slightly modified and corrected) proof of the version of [CP] that is needed here.

Acknowledgements: Moshe Jarden pointed out many of the potential consequences of the Main Theorem to the first author.

Notations: Throughout x will denote an indeterminate that is transcendental over any particular base field, usually denoted k. Thus $k(x)$ is the field of rational functions in x with coefficients in k. The algebraic closure of a field k is denoted by $\bar{k}$, and we let $G_k = G(\bar{k}/k)$ denote the absolute Galois group of k (in characteristic 0). A field L is said to be *regular* over a subfield k if L and $\bar{k}$ are linearly disjoint over k; in the case $\mathrm{char}(L) = 0$ this is equivalent to the condition that k is algebraically closed in L. We say that a finite group G is *regular* over a field k (with r branch points) if G is isomorphic to the Galois group of an extension $L/k(x)$ with L regular over k (and with r branch points). When we speak of the *branch points* of such an extension $L/k(x)$ (with $\mathrm{char}(k) = 0$), we mean branch points of the corresponding curve cover over $\bar{k}$.

The field of rationals (resp., complexes) is denoted by $\mathcal{Q}$ (resp., $\mathcal{C}$). We let $\mathcal{P}^1$ denote the Riemann sphere $\mathcal{C} \cup \{\infty\}$, viewed according to context as a Riemann surface or as an algebraic curve defined over $\mathcal{Q}$ (in the natural way). The fundamental group of a topological space Y, based at $y \in Y$, is denoted $\pi_1(Y, y)$. If U is a subgroup of G, then $[U]$ denotes the conjugacy class of subgroups of G containing U. A subgroup of G is called *self-normalizing* if it equals its own normalizer in G.

TABLE OF CONTENTS

1. MODULI SPACES FOR COVERS OF THE RIEMANN SPHERE

Let G be a finite group and $U \leq G$ a subgroup that does not contain a non-trivial normal subgroup of G. Let $\mathrm{Aut}(G,U)$ be the group of all automorphisms of G that preserve the conjugacy class of U, and let $\mathrm{Inn}(G)$ be the group of inner automorphisms.

§**1.1. Nielsen classes and the Hurwitz monodromy group:** In this subsection we fix some more terminology. Let r be an integer > 1, and consider the set

$$\mathcal{E}_r = \mathcal{E}_r(G) = \{(\sigma_1,\dots,\sigma_r) \mid \sigma_1,\dots,\sigma_r \in G \setminus \{1\}, < \sigma_1,\dots,\sigma_r >= G,\ \sigma_1\cdots\sigma_r = 1\}.$$

Let $\mathcal{E}_r^{\mathrm{ab}} = \mathcal{E}_r^{\mathrm{ab}}(G,U)$ (resp., $\mathcal{E}_r^{\mathrm{in}} = \mathcal{E}_r^{\mathrm{in}}(G)$) denote the quotient of $\mathcal{E}_r$ by the componentwise action of $\mathrm{Aut}(G,U)$ (resp., of $\mathrm{Inn}(G)$). For any conjugacy class C of G and for any integer m define C^m to be the conjugacy class of the g^m, $g \in C$. Let $\mathbf{C} = (\mathrm{C}_1,\dots,\mathrm{C}_r)$ be an r-tuple of conjugacy classes of G. We say $(\mathrm{C}_1,\dots,\mathrm{C}_r)$ is *rational* if for each integer m prime to the order of G we have $(\mathrm{C}_1^m,\dots,\mathrm{C}_r^m) = (\mathrm{C}_{\pi(1)},\dots,\mathrm{C}_{\pi(r)})$ for some $\pi \in S_r$. This generalizes the usual notion of a rational conjugacy class.

The *Nielsen class* $\mathrm{Ni}(\mathbf{C})$ of $\mathbf{C}$ is defined to be the set of all $(\sigma_1,\dots,\sigma_r) \in \mathcal{E}_r$ for which there exists a permutation $\pi \in S_r$ with $\sigma_i \in C_{\pi(i)}$ for $i = 1,...,r$. Define the set $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$ (resp., $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$) to be the image of $\mathrm{Ni}(\mathbf{C})$ in $\mathcal{E}_r^{\mathrm{ab}}$ (resp., $\mathcal{E}_r^{\mathrm{in}}$).

Embed affine space $\mathcal{A}^r$ in $\mathcal{P}^r$ by regarding $\mathcal{A}^r$ as the space of monic complex polynomials of degree r, and $\mathcal{P}^r$ as the space of all nonzero complex polynomials of degree at most r up to multiplication by a nonzero constant. Consider the classical discriminant locus in $\mathcal{A}^r$, corresponding to the polynomials with repeated roots, and denote its closure in $\mathcal{P}^r$ by D_r. We will work with the space $\mathcal{U}_r \stackrel{\mathrm{def}}{=} \mathcal{P}^r \setminus D_r$, which we view as the space of all subsets of cardinality r of the Riemann sphere $\mathcal{P}^1 = \mathcal{C} \cup \{\infty\}$. That is, we identify a point of $\mathcal{U}_r$ with the set of roots of a corresponding polynomial, where we count ∞ as a root if the degree of the polynomial is less than r (the degree is then necessarily $r-1$).

The space $\mathcal{U}_r$ has a natural structure as algebraic variety defined over $\mathcal{Q}$. We fix a base point $\boldsymbol{b} = \{b_1,\dots,b_r\}$ in $\mathcal{U}_r$ that is rational over $\mathcal{Q}$ (i.e., the b_i's are permuted by $G_{\mathcal{Q}}$); further we assume $b_i \neq \infty$ for all i. For the moment we consider $\mathcal{U}_r$ only as a complex manifold. The (topological) fundamental group $H_r = \pi_1(\mathcal{U}_r, \boldsymbol{b})$ is called the *Hurwitz monodromy group* (cf. [BF]). It is a quotient of $\pi_1(\mathcal{A}^r \setminus D_r, \boldsymbol{b})$ (via the map induced from the embedding of $\mathcal{A}^r$ in $\mathcal{P}^r$). The latter group is classically known to be isomorphic to the Artin braid group B_r. Thus the "elementary braids" that generate B_r yield generators $Q_1,\dots,Q_{r-1}$ of H_r. In §1.3 we will work with an explicit description of these generators.

§**1.2. Moduli Spaces for Covers of $\mathcal{P}^1$:** From now on $\varphi : X \to \mathcal{P}^1$ will always denote a (branched) cover of compact (connected) Riemann surfaces. Two such covers $\varphi : X \to \mathcal{P}^1$ and $\varphi' : X' \to \mathcal{P}^1$ are called equivalent if there exists an isomorphism $\delta : X \to X'$ with $\varphi' \circ \delta = \varphi$. We let $\mathrm{Aut}(X/\mathcal{P}^1)$ denote the group of automorphisms of the cover $\varphi : X \to \mathcal{P}^1$ (i.e., automorphisms δ of X with $\varphi \circ \delta = \varphi$). The cover φ is called a Galois cover if $\mathrm{Aut}(X/\mathcal{P}^1)$ is transitive on the fibers of φ.

Let $a_1,\dots,a_r \in \mathcal{P}^1$ be the branch points of the cover φ, and set $\boldsymbol{a} = \{a_1,\dots,a_r\}$. Then φ restricts to an (unramified) topological cover φ^0 of the punctured sphere $\mathcal{P}^1 \setminus \boldsymbol{a}$. Choose a base point a_0 on this punctured sphere. By the theory of covering spaces, the equivalence class of φ^0 corresponds to a conjugacy class $[U_\varphi]$ of subgroups U_φ of the fundamental group $\Gamma = \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0)$. In fact we have a 1-1 correspondence between the equivalence classes of covers $\varphi' : X' \to \mathcal{P}^1$ with branch points among $a_1,\dots,a_r$, and conjugacy classes of subgroups of Γ of finite index (see e.g. [Fu, 1.3]). Under this correspondence, the covers with *exactly* r branch points correspond to those subgroups of Γ that do not contain the kernel of the natural map from Γ to $\Gamma_i \stackrel{\mathrm{def}}{=} \pi_1((\mathcal{P}^1 \setminus \boldsymbol{a}) \cup \{a_i\}, a_0)$, for any i. Furthermore, under the above correspondence the group $\mathrm{Aut}(X/\mathcal{P}^1)$ is isomorphic to $N_\Gamma(U_\varphi)/U_\varphi$ where $N_\Gamma(U_\varphi)$ is the normalizer of U_φ in Γ.

Let $\mathcal{H}^{\mathrm{ab}} = \mathcal{H}_r^{\mathrm{ab}}(G,U)$ be the set of equivalence classes $|\varphi|$ of all covers $\varphi : X \to \mathcal{P}^1$ with r branch points for which — in the above notation — there is a surjection $f : \Gamma \to G$ with $f^{-1}(U)$ conjugate to U_φ. (This is clearly independent of the choice of base point a_0). The 1-1 correspondence between equivalence classes of the covers φ and of their restrictions φ^0 allows us to say that the point $|\varphi|$ of $\mathcal{H}^{\mathrm{ab}}$ is represented by φ^0 (as well as by φ). From the last paragraph:

(1) $\mathrm{Aut}(X/\mathcal{P}^1) = 1$ if the class of $\varphi : X \to \mathcal{P}^1$ belongs to $\mathcal{H}^{\mathrm{ab}} = \mathcal{H}_r^{\mathrm{ab}}(G, U)$ and U is self-normalizing in G.

Let $\mathcal{H}^{\mathrm{in}} = \mathcal{H}_r^{\mathrm{in}}(G)$ be the set of equivalence classes of pairs (χ, h) where $\chi : \hat{X} \to \mathcal{P}^1$ is a Galois cover with r branch points, and $h : \mathrm{Aut}(\hat{X}/\mathcal{P}^1) \to G$ is an isomorphism; two such pairs (χ, h) and $(\chi' : \hat{X}' \to \mathcal{P}^1,\ h')$ are called equivalent if there is an isomorphism $\delta : \hat{X} \to \hat{X}'$ over $\mathcal{P}^1$ such that $h' \circ c_\delta = h$, where $c_\delta : \mathrm{Aut}(\hat{X}/\mathcal{P}^1) \to \mathrm{Aut}(\hat{X}'/\mathcal{P}^1)$ is the isomorphism induced by δ. Let $|\chi, h|$ denote the equivalence class of the pair (χ, h).

Note that points of $\mathcal{H}^{\mathrm{in}}$ can equally well be thought of as equivalence classes of triples $(\boldsymbol{a}, a_0, f)$, where $\boldsymbol{a} = \{a_1, \dots, a_r\} \in \mathcal{U}_r$, $a_0 \in \mathcal{P}^1 \setminus \boldsymbol{a}$ and $f : \Gamma = \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0) \to G$ is a surjection that does not factor through the canonical map $\Gamma \to \Gamma_i$, for any i. Two such triples $(\boldsymbol{a}, a_0, f)$ and $(\tilde{\boldsymbol{a}}, \tilde{a}_0, \tilde{f})$ are called equivalent if $\boldsymbol{a} = \tilde{\boldsymbol{a}}$ and there is a path γ from a_0 to $\tilde{a}_0$ in $\mathcal{P}^1 \setminus \boldsymbol{a}$ such that the induced map $\gamma^* : \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0) \to \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, \tilde{a}_0)$ satisfies $\tilde{f} \circ \gamma^* = f$.

Here is the correspondence between the above pairs and triples. Let $\chi : \hat{X} \to \mathcal{P}^1$ be a Galois cover with r branch points $a_1, \dots, a_r$, let $\boldsymbol{a} = \{a_1, \dots, a_r\}$ and $a_0 \in \mathcal{P}^1 \setminus \boldsymbol{a}$. Set $\Gamma = \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0)$ as above. Depending on the choice of a base point $\hat{x} \in \chi^{-1}(a_0)$, we get a surjection $\iota : \Gamma \to \mathrm{Aut}(\hat{X}/\mathcal{P}^1)$ as follows: For each path γ representing an element of Γ, let $\hat{y}$ be the endpoint of the unique lift of γ to $\hat{X} \setminus \chi^{-1}(\boldsymbol{a})$ with initial point $\hat{x}$; then ι sends γ to the unique element ϵ of $\mathrm{Aut}(\hat{X}/\mathcal{P}^1)$ with $\epsilon(\hat{x}) = \hat{y}$. Now h and f are related by $f = h \circ \iota$, and $U_\chi = \ker(f)$ $(= \ker(\iota))$. Varying $\hat{x}$ over $\chi^{-1}(a_0)$ means composing ι with inner automorphisms of $\mathrm{Aut}(\hat{X}/\mathcal{P}^1)$. Therefore h and f determine each other up to inner automorphisms of G, which is compatible with the equivalence of pairs (resp., triples).

We have a natural map $\Lambda : \mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$ sending $|\chi, h|$ to the class of the cover $\varphi : \hat{X}/h^{-1}(U) \to \mathcal{P}^1$ induced by $\chi : \hat{X} \to \mathcal{P}^1$. Then, in the notation of the preceding paragraph, $f^{-1}(U)$ is one of the subgroups of Γ corresponding to φ. Since U does not contain a non-trivial normal subgroup of G, the intersection of all conjugates of $f^{-1}(U)$ equals the kernel of f. It follows that φ has exactly the same r branch points as does χ (namely, if $\ker(\Gamma \to \Gamma_i)$ would lie in $f^{-1}(U)$, then it would also be in $\ker(f)$, a contradiction). Thus $|\varphi|$ lies actually in $\mathcal{H}^{\mathrm{ab}} = \mathcal{H}_r^{\mathrm{ab}}(G, U)$, and Λ is well defined. Let $\Psi : \mathcal{H}^{\mathrm{ab}} \to \mathcal{U}_r$ and $\Psi' : \mathcal{H}^{\mathrm{in}} \to \mathcal{U}_r$ be the maps sending $|\varphi|$ and $|\chi, h|$ to the set of branch points of φ and χ, respectively. Then $\Psi' = \Lambda \circ \Psi$.

The sets $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ carry a natural topology such that Ψ, Ψ' and Λ become (unramified) coverings. For $\mathcal{H}^{\mathrm{ab}}$ this is classical, going back to Hurwitz (cf. [Fu, 1.3]): To specify a neighborhood $\mathcal{N} = \mathcal{N}(\boldsymbol{p}; D_1, \dots, D_r)$ of $\boldsymbol{p} = |\varphi|$ in $\mathcal{H}^{\mathrm{ab}}$, choose pairwise disjoint discs $D_1, \dots, D_r$ around the branch points $a_1, \dots, a_r$ of φ. Then $\mathcal{N}$ consists of all $|\tilde{\varphi}|$ such that $\tilde{\varphi}$ has exactly one branch point in each D_i, and the two covers of $\mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r)$ induced by φ and $\tilde{\varphi}$ are equivalent. These $\mathcal{N}$ form a basis for the neighborhoods of $\boldsymbol{p}$ in $\mathcal{H}^{\mathrm{ab}}$.

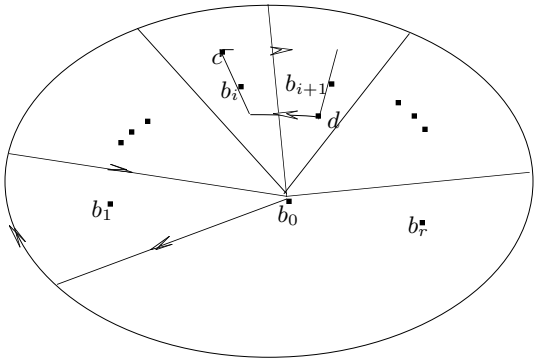
The analogous topology on $\mathcal{H}^{\mathrm{in}}$ is defined as follows: To specify a neighborhood $\mathcal{N}'$ of the point of $\mathcal{H}^{\mathrm{in}}$ represented by the triple $(\boldsymbol{a}, a_0, f)$, choose discs D_i around a_i as above, with $a_0 \notin D_1 \cup \cdots \cup D_r$. Then $\mathcal{N}'$ consists of all points represented by the triples $(\tilde{\boldsymbol{a}}, a_0, \tilde{f})$ such that $\tilde{\boldsymbol{a}}$ has exactly one point in each D_i, and $\tilde{f}$ is the composition of the canonical isomorphisms $\pi_1(\mathcal{P}^1 \setminus \tilde{\boldsymbol{a}}, a_0) \cong \pi_1(\mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r), a_0) \cong \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0)$ with f. Again these $\mathcal{N}'$ form a basis for the topology.

Through the coverings Ψ and Ψ', the spaces $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ naturally inherit a structure of complex manifold.

§**1.3. Monodromy action on the fibers of $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$:** To determine the equivalence class of the covering $\Psi : \mathcal{H}^{\mathrm{ab}} \to \mathcal{U}_r$ one needs to identify the natural permutation representation of $H_r = \pi_1(\mathcal{U}_r, \boldsymbol{b})$ on the fiber $\Psi^{-1}(\boldsymbol{b})$. Recall that this action is defined as follows: The element of H_r represented by a closed path ω sends a point $\boldsymbol{p} \in \psi^{-1}(\boldsymbol{b})$ to the endpoint of the unique lift of ω with initial point $\boldsymbol{p}$. Similarly for Ψ'.

This depends on the choice of generators $\gamma_1, \ldots, \gamma_r$ for the fundamental group $\Gamma_0 = \pi_1(\mathcal{P}^1 \setminus \boldsymbol{b}, b_0)$, where b_0 is a base point in $\mathcal{P}^1 \setminus \boldsymbol{b}$ that we fix now once and for all; we choose $b_0 \neq \infty$ such that no line through b_0 contains more than one of $b_1, \ldots, b_r$. Choose a disc D centered at b_0 such that all the b_i's are contained in the interior of D. Partition D into sectors $S_1, \ldots, S_r$ such that b_i is in the interior of S_i for $i = 1, \ldots, r$. The numbering of the b_i's should be chosen so that the sectors $S_1, \ldots, S_r$ appear in this order in clockwise direction around the disc. Let γ_i be the path with initial and end-point b_0, travelling clockwise along the boundary of S_i. By abuse, we don't distinguish between the paths γ_i and their homotopy classes in Γ_0. Then Γ_0 is a free group on generators $\gamma_1, \ldots, \gamma_{r-1}$, and $\gamma_1 \cdots \gamma_r = 1$. (The latter relation can be seen especially clearly in the way we chose the γ_i's, since the product $\gamma_1 \cdots \gamma_r$ is equal in Γ_0 to a path going from b_0 on a straight line to the boundary of D, travelling once around this bounding circle, and then returning to b_0; this path is clearly trivial in Γ_0).

Generating Paths: *Paths made from sectors.*



Let N be the normal subgroup of Γ_0 generated by the conjugates of γ_r. Then Γ_0/N is generated by $\gamma_1 N, \ldots, \gamma_{r-2} N$, and the images of these elements under the natural map $\Gamma_0/N \to \pi_1(\mathcal{P}^1 \setminus \{b_1, \ldots, b_{r-1}\}, b_0)$ are free generators of the latter group. Hence this map is an isomorphism. With r replaced by any $i = 1, \ldots, r$, we conclude that the kernel of the natural map $\Gamma_0 \to \pi_1((\mathcal{P}^1 \setminus \boldsymbol{b}) \cup \{b_i\}, b_0)$ equals the normal subgroup of Γ_0 generated by the conjugates of γ_i. This implies the following: Assume $\varphi' : X' \to \mathcal{P}^1$ is a cover with branch points among $b_1, \ldots, b_r$, and one of the subgroups of Γ_0 corresponding to φ' is of the form $f^{-1}(U)$, where $f : \Gamma_0 \to G$ is a surjection. Then φ' has exactly r branch points if and only if $f(\gamma_i) \neq 1$ for all $i = 1, \ldots, r$ (cf. §1.2).

If now φ is a cover of $\mathcal{P}^1$ with $|\varphi| \in \psi^{-1}(\boldsymbol{b})$, then by definition there is a surjection $f : \Gamma_0 \to G$ with $f^{-1}(U)$ conjugate to U_φ. The kernel of f equals the intersection of all subgroups in the class $[U_\varphi]$, hence it depends only on $|\varphi|$. Thus f is determined by $|\varphi|$ up to composition with elements of $\mathrm{Aut}(G, U)$. Conversely, $|\varphi|$ is determined by f since $[U_\varphi] = f^{-1}([U])$. Also, each surjection $f : \Gamma_0 \to G$ with $f(\gamma_i) \neq 1$ for all $i = 1, \ldots, r$ gives rise to some $|\varphi| \in \Psi^{-1}(\boldsymbol{b})$ (by the preceding paragraph). Furthermore, f is determined by the r-tuple $(\sigma_1, \ldots, \sigma_r) = (f(\gamma_1), \ldots, f(\gamma_r)) \in \mathcal{E}_r(G)$ (see §1.1 for the definition of $\mathcal{E}_r(G)$). Since Γ_0 is free on $\gamma_1, \ldots, \gamma_{r-1}$, each $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r = \mathcal{E}_r(G)$ occurs in this way . Thus we get a bijection between the points $|\varphi|$ in the fiber $\Psi^{-1}(\boldsymbol{b})$ and the set $\mathcal{E}_r^{\mathrm{ab}}$ ($= \mathcal{E}_r$ modulo $\mathrm{Aut}(G, U)$) of $\mathrm{Aut}(G, U)$-classes of the r-tuples $(\sigma_1, \ldots, \sigma_r)$. Via this bijection, we get an action of $H_r = \pi_1(\mathcal{U}_r, \boldsymbol{b})$ on $\mathcal{E}_r^{\mathrm{ab}}$.

Similarly, we get a bijection between the points $|\chi, h|$ in the fiber $(\Psi')^{-1}(\boldsymbol{b})$ and the set $\mathcal{E}_r^{\mathrm{in}}$ ($= \mathcal{E}_r$ modulo $\mathrm{Inn}(G)$): Given (χ, h) define $f = h \circ \iota : \Gamma_0 \to G$ as in §1.2, and associate with it the class of $(\sigma_1, \ldots, \sigma_r) = (f(\gamma_1), \ldots, f(\gamma_r))$ in $\mathcal{E}_r^{\mathrm{in}}$. This yields the desired bijection, since f is determined by $|\chi, h|$ up to composition with inner automorphisms of G (see §1.2). This bijection induces an action of H_r on $\mathcal{E}_r^{\mathrm{in}}$.

We are going to describe explicitly the action of the generators $Q_1, \dots, Q_{r-1}$ of H_r (from §1.1) on the sets $\mathcal{E}_r^{\text{ab}}$ and $\mathcal{E}_r^{\text{in}}$. First we need an explicit description of Q_i for $i = 1, \dots, r-1$ (c.f. [BF], [Fu, 1.4]): Choose a point c on the line $\overline{b_0 b_i}$ strictly between b_i and the boundary of D, and closer to this boundary than b_{i+1}; further choose a point d on the line $\overline{b_{i+1} b_0}$ strictly between b_{i+1} and b_0, and closer to b_0 than b_i. We can represent Q_i by a path $\boldsymbol{a}(t) = \{a_1(t), \dots, a_r(t)\}$ in $\mathcal{U}_r$, $0 \le t \le 1$, where $a_j(t)$ is the constant path b_j for $j \ne i, i+1$; and $a_i(t)$ is a path going from b_i on a straight line to c, then travelling on a circular arc around b_0 in clockwise direction until it meets the line $\overline{b_0 b_{i+1}}$, from where it continues on this line to b_{i+1}; and $a_{i+1}(t)$ is a path going from b_{i+1} on a straight line to d, then travelling on a circular arc around b_0 in counter-clockwise direction until it meets the line $b_0 b_i$, from where it continues on this line to b_i.

Having fixed all the above data, the action of Q_i on $\mathcal{E}_r^{\text{ab}}$ and on $\mathcal{E}_r^{\text{in}}$ is now given by the following rule: Q_i sends the class of $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}_r$ to the class of

$$(\sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}, \sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_r). \tag{2}$$

For the case of $\mathcal{H}^{\text{ab}}$, this observation goes back to Hurwitz [Hur] (see also [Fr,1] and [Fu, 1.4]). We give a proof in §1.4.

By the theory of covering spaces (and the above identifications), the connected components of $\mathcal{H}^{\text{ab}}$ and $\mathcal{H}^{\text{in}}$ now correspond to the orbits of H_r on $\mathcal{E}_r^{\text{ab}}$ and $\mathcal{E}_r^{\text{in}}$, respectively. Note that for each r-tuple $\mathbf{C}$ of conjugacy classes of G, the subsets $\text{Ni}(\mathbf{C})^{\text{ab}}$ and $\text{Ni}(\mathbf{C})^{\text{in}}$ of $\mathcal{E}_r^{\text{ab}}$ and $\mathcal{E}_r^{\text{in}}$, respectively (see §1.1), are invariant under the action of H_r; hence these subsets are unions of H_r-orbits. Let $\mathcal{H}(\mathbf{C})^{\text{ab}}$ (resp., $\mathcal{H}(\mathbf{C})^{\text{in}}$) denote the union of the corresponding connected components of $\mathcal{H}^{\text{ab}}$ (resp. $\mathcal{H}^{\text{in}}$). We call these subspaces $\mathcal{H}(\mathbf{C})^{\text{ab}}$ and $\mathcal{H}(\mathbf{C})^{\text{in}}$ *Hurwitz spaces*. Each component of $\mathcal{H}^{\text{ab}}$ (resp., $\mathcal{H}^{\text{in}}$) belongs to such a Hurwitz space.

It is a basic problem to decide when the Hurwitz spaces themselves are connected. That is, when H_r acts transitively on $\text{Ni}(\mathbf{C})^{\text{ab}}$ or $\text{Ni}(\mathbf{C})^{\text{in}}$. For the case of simply branched covers (i.e., $\mathbf{C} = (\text{C}, \dots, \text{C})$ where C is the class of transpositions in $G = S_n$ ($n > 2$), and $U = S_{n-1}$) this was done by Clebsch [Cl]. In the Appendix we present a far more general result in this direction, due to Conway and Parker [CP].

§1.4. The action of Q_i on $\mathcal{E}_r^{\text{ab}}$ and $\mathcal{E}_r^{\text{in}}$: Here we indicate how the action of Q_i gives formula (2). We represent Q_i by the path $\boldsymbol{a}(t)$ from §1.3. Choose another disc D' around b_0 that contains the point d in its interior, and b_i, b_{i+1} are not in D'. (This is possible by the choice of d). Let R_i be the interior of the sector of D' cut out by $S_i \cup S_{i+1}$, and let T_i be the interior of $(S_i \cup S_{i+1}) \setminus D'$. Let S_j^0 be the interior of S_j, and $P = \mathcal{P}^1 \setminus \mathbf{b}$. We may assume that the paths $a_i(t)$ and $a_{i+1}(t)$ reach the boundary between S_i and S_{i+1} at the same time $t = 1/2$, and that $a_{i+1}(t) \in R_i$ exactly for $1/4 < t < 3/4$. Note that the path $a_i(t)$ remains always in T_i. The inclusions between the respective spaces give canonical isomorphisms:

$$\pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}(t), b_0) \cong \pi_1(P \setminus (S_i^0 \cup S_{i+1}^0), b_0) \stackrel{\text{def}}{=} \Gamma^{(0)} \quad \text{for } \mathrm{t} < 1/2; \tag{3}$$

$$\pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}(t), b_0) \cong \pi_1(P \setminus (R_i \cup T_i), b_0) \stackrel{\text{def}}{=} \Gamma^{(1)} \quad \text{for } 1/4 < \mathrm{t} < 3/4; \text{and} \tag{4}$$

$$\pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}(t), b_0) \cong \pi_1(P \setminus (S_i^0 \cup S_{i+1}^0), b_0) = \Gamma^{(0)} \quad \text{for } \mathrm{t} > 1/2. \tag{5}$$

From (3) and (4) we get an isomorphism $\alpha_1 : \Gamma^{(0)} \to \Gamma^{(1)}$ for each choice of t with $1/4 < t < 1/2$, and this isomorphism is the same for all these t. Similarly, from (4) and (5) we get an isomorphism $\alpha_2 : \Gamma^{(1)} \to \Gamma^{(0)}$, independent of the choice of t with $1/2 < t < 3/4$. With paths and their respective homotopy classes identified, one checks easily that the automorphism $\alpha = \alpha_2 \circ \alpha_1$ of $\Gamma^{(0)}$ is given by

$$\alpha(\gamma_{i+1}) = \gamma_i, \quad \alpha(\gamma_i) = \gamma_i\gamma_{i+1}\gamma_i^{-1}, \qquad \alpha(\gamma_j) = \gamma_j \ \text{ for } j \ne i, i+1 \tag{6}$$

The groups $\Gamma^{(0)}$ and Γ_0 are canonically isomorphic, under an isomorphism which identifies the classes of $\gamma_1, \dots, \gamma_r$ in $\Gamma^{(0)}$ and Γ_0, respectively. We let α also denote the automorphism of Γ_0 given by (6).

Now let $\boldsymbol{p}(t)$ be a lift of the path $\boldsymbol{a}(t)$ to $\mathcal{H}^{\rm ab}$. Then for each t, the point $\boldsymbol{p}(t)$ is an equivalence class of covers of $\mathcal{P}^1$ with $\boldsymbol{a}(t)$ as its set of branch points. Thus $\boldsymbol{p}(t)$ corresponds to a conjugacy class Δ_t of subgroups of $\pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}(t), b_0)$; the image of Δ_t under the isomorphisms (3), (4) and (5) is independent of t (under the respective conditions on t), by the definition of the topology on $\mathcal{H}^{\rm ab}$. Thus the conjugacy classes Δ_0 and Δ_1 of subgroups of Γ_0 corresponding to the initial point $\boldsymbol{p}(0)$ and the endpoint $\boldsymbol{p}(1)$ of the path $\boldsymbol{p}(t)$, respectively, are related by $\Delta_1 = \alpha(\Delta_0)$.

Finally, if $f_0 : \Gamma_0 \to G$ is a surjection with $f_0^{-1}(U) \in \Delta_0$, then $f_1 \stackrel{\rm def}{=} f_0 \circ \alpha^{-1}$ is a surjection $\Gamma_0 \to G$ with

$$f_1^{-1}(U) = \alpha \circ f_0^{-1}(U) \in \alpha(\Delta_0) = \Delta_1.$$

Thus $(\sigma_1, \ldots, \sigma_r) = (f_0(\gamma_1), \ldots, f_0(\gamma_r))$ is an r-tuple representing the element of $\mathcal{E}_r^{\rm ab}$ corresponding to $\boldsymbol{p}(0)$, and $(\sigma_1, \ldots, \sigma_{i+1}, \sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}, \ldots, \sigma_r) = (f_1(\gamma_1), \ldots, f_1(\gamma_r))$ represents the element of $\mathcal{E}_r^{\rm ab}$ corresponding to $\boldsymbol{p}(1)$. This proves that the action of Q_i on $\mathcal{E}_r^{\rm ab}$ is given by formula (2).

Now let $\boldsymbol{p}'(t)$ be a lift of the path $\boldsymbol{a}(t)$ to $\mathcal{H}^{\rm in}$. For each t, the point $\boldsymbol{p}'(t)$ is represented by a triple $(\boldsymbol{a}(t), b_0, f_t)$ where $f_t : \pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}(t), b_0) \to G$ is a surjection. The surjections $\Gamma^{(0)} \to G$ (resp., $\Gamma^{(1)} \to G$) that are the composition of the isomorphisms (3) and (5) (resp., (4)) with f_t are independent of t (under the respective conditions on t), by the definition of the topology on $\mathcal{H}^{\rm in}$. It follows that the map f_0 corresponding to $\boldsymbol{p}'(0)$ and the map f_1 corresponding to $\boldsymbol{p}'(1)$ are related by $f_1 = f_0 \circ \alpha^{-1}$. From this we conclude—as in the preceding paragraph—that Q_i acts on $\mathcal{E}_r^{\rm in}$ via formula (2).

§**1.5. The field of definition of a cover :** For each cover $\varphi : X \to \mathcal{P}^1$ (of connected compact Riemann surfaces) the space X has a unique structure as algebraic variety defined over $\mathcal{C}$ (compatible with its analytic structure) such that φ becomes an algebraic morphism. This is Riemann's existence theorem. We say that φ can be defined over some subfield k of $\mathcal{C}$ if X can be given a structure of variety defined over k such that φ becomes a morphism defined over k.

Let $\boldsymbol{a} = \{a_1, \ldots, a_r\} \in \mathcal{U}_r$ be the set of branch points of φ, and $k_0 = \mathcal{Q}(\boldsymbol{a})$; thus k_0 is the field generated by the coefficients of the polynomial $\prod(x - a_i)$, where the product is over those $i = 1, \ldots, r$ with $a_i \neq \infty$. Now let k be any subfield of $\mathcal{C}$ over which φ can be defined. Then the branch points $a_1, \ldots, a_r$ are algebraic over k, and the absolute Galois group G_k permutes $a_1, \ldots, a_r$. Therefore k_0 is contained in k.

Conversely, φ can be defined over the algebraic closure F of k_0 in $\mathcal{C}$, in a unique way [Fr,1; Lemma 1.2]. Thus for each $\beta \in G_{k_0}$, we can form the cover $\varphi^\beta : X^\beta \to \mathcal{P}^1$ obtained from $\varphi : X \to \mathcal{P}^1$ through base change with β. Let k_1 be the fixed field in F of the group of those β for which φ^β is equivalent to φ. We show that k_1 is contained in each subfield k of $\mathcal{C}$ over which φ can be defined: By the above $k_0 \subset k$. If $c \in \mathcal{C}$ is algebraic over k_0 and not in k, then there exists $\beta' \in G_k$ with $\beta'(c) \neq c$. Since φ can be defined over k we have $\varphi^{\beta'}$ equivalent to φ. Therefore the restriction of β' to an element of G_{k_0} must fix k_1 elementwise, and thus $c \notin k_1$. This proves $k_1 \subset k$.

Conversely φ can actually be defined over k_1 if we have $\mathrm{Aut}(X/\mathcal{P}^1) = 1$ [Fr,1; Theorem 5.1]. For completeness we give the argument here. The condition that $\mathrm{Aut}(X/\mathcal{P}^1)$ is trivial implies that for each $\beta \in G_{k_1}$ the isomorphism $\delta_\beta : X^\beta \to X$ with $\varphi \circ \delta_\beta = \varphi^\beta$ is unique. This forces the maps δ_β to satisfy Weil's cocycle condition. By Weil's criterion [W], X can be defined over k_1 such that $\delta_\beta : X = X^\beta \to X$ is the identity for each $\beta \in G_{k_1}$. Then also $\varphi : X \to \mathcal{P}^1$ is defined over k_1.

Also if φ is a Galois cover then it can be defined over k_1 (but perhaps not together with its automorphisms); this was noted in [CHa]. (The proof is similar as above: Fix a point $z \in X$ lying over a k_1-point of $\mathcal{P}^1$ that is not a branch point, and normalize the δ_β such that $\delta_\beta(z^\beta) = z$). Thus if either φ is a Galois cover or $\mathrm{Aut}(X/\mathcal{P}^1) = 1$, then φ has a unique *minimal field of definition* $k_1 \subset \mathcal{C}$.

2. THE MAIN THEOREM AND SOME CONSEQUENCES

§**2.1. The Main Theorem:** Define a point $\boldsymbol{p} = |\varphi|$ of $\mathcal{H}^{\rm ab}$ to be a $\bar{\mathcal{Q}}$-point if the branch points of φ are algebraic over $\mathcal{Q}$. Then φ can be defined over $\bar{\mathcal{Q}}$ by §1.5. The notion of a $\bar{\mathcal{Q}}$-point of $\mathcal{H}^{\rm in}$ is defined similarly. There is a natural action of the absolute Galois group $G_{\mathcal{Q}}$ on the $\bar{\mathcal{Q}}$-points of $\mathcal{H}^{\rm ab}$: The element $\beta \in G_{\mathcal{Q}}$ sends $|\varphi|$ to $|\varphi^\beta|$, where $\varphi^\beta : X^\beta \to \mathcal{P}^1$ is the cover obtained from $\varphi : X \to \mathcal{P}^1$ through base change with β. Note that if $|\varphi| \in \mathcal{H}^{\rm ab} = \mathcal{H}_r^{\rm ab}(G,U)$ then also $|\varphi^\beta| \in \mathcal{H}_r^{\rm ab}(G,U)$, because the pair (G,U) can be recovered from φ as the pair $(\mathrm{Aut}(\hat{X}/\mathcal{P}^1), \mathrm{Aut}(\hat{X}/X))$, where $\hat{X} \to X \stackrel{\varphi}{\longrightarrow} \mathcal{P}^1$ is a Galois closure of φ (i.e., $\hat{X} \to \mathcal{P}^1$ is a minimal Galois cover factoring through φ).

Similarly, we get an action of $G_{\mathcal{Q}}$ on the $\bar{\mathcal{Q}}$-points of $\mathcal{H}^{\rm in}$: The element $\beta \in G_{\mathcal{Q}}$ sends the point $|\chi, h|$ to $|\chi^\beta, h \circ \beta^{-1}|$, where $h \circ \beta^{-1} : \mathrm{Aut}(\hat{X}^\beta/\mathcal{P}^1) \to G$ is the isomorphism sending A^β to $h(A)$ for every $A \in \mathrm{Aut}(\hat{X}/\mathcal{P}^1)$. So it is natural to expect that $\mathcal{H}^{\rm ab}$ and $\mathcal{H}^{\rm in}$ have a structure as varieties defined over $\mathcal{Q}$ such that the resulting action of $G_{\mathcal{Q}}$ on the $\bar{\mathcal{Q}}$-points is as above. Such a $\mathcal{Q}$- structure on $\mathcal{H}^{\rm ab}$ and $\mathcal{H}^{\rm in}$ is then necessarily unique. Its existence is our main theorem, which will be proved in §3–5:

Theorem 1: *Let G be a finite group, and $U \le G$ a proper subgroup that does not contain a non-trivial normal subgroup of G. Let $r \ge 3$ be an integer such that G can be generated by $r-1$ elements. Then the spaces $\mathcal{H}^{\rm ab} = \mathcal{H}_r^{\rm ab}(G,U)$ and $\mathcal{H}^{\rm in} = \mathcal{H}_r^{\rm in}(G)$ have a unique structure as (reducible) algebraic varieties defined over $\mathcal{Q}$ (compatible with their analytic structure) so that the maps*

$$\mathcal{H}^{\rm in} \stackrel{\Lambda}{\longrightarrow} \mathcal{H}^{\rm ab} \stackrel{\Psi}{\longrightarrow} \mathcal{U}_r$$

are algebraic morphisms defined over $\mathcal{Q}$, and the following hold:

(a) *If $\boldsymbol{p} = |\varphi|$ is a point of $\mathcal{H}^{\rm ab}$ such that the branch points of φ are algebraic over some subfield k of $\mathcal{C}$, then $\boldsymbol{p}$ is algebraic over k, and each automorphism β of $\bar{k}$ sends $\boldsymbol{p} = |\varphi|$ to $|\varphi^\beta|$.*

(b) *If $\boldsymbol{p}' = |\chi, h|$ is a point of $\mathcal{H}^{\rm in}$ such that the branch points of χ are algebraic over some subfield k of $\mathcal{C}$, then $\boldsymbol{p}'$ is algebraic over k, and each automorphism β of $\bar{k}$ sends $\boldsymbol{p}' = |\chi, h|$ to $|\chi^\beta, h \circ \beta^{-1}|$ (where $h \circ \beta^{-1}$ is to be understood as in the preceding paragraph).*

Furthermore, the absolutely irreducible components of $\mathcal{H}^{\rm ab}$ and $\mathcal{H}^{\rm in}$ (defined over $\bar{\mathcal{Q}}$) coincide with the connected components (in the topology from §1.2). Let $\mathbf{C}$ be an r-tuple of conjugacy classes of G such that $\mathrm{Ni}(\mathbf{C})^{\rm in}$ is non-empty. Then $\mathbf{C}$ is rational (as defined in §1.1) if and only if the subspace $\mathcal{H}(\mathbf{C})^{\rm in}$ of $\mathcal{H}^{\rm in}$ is defined over $\mathcal{Q}$. In addition, $\mathcal{H}(\mathbf{C})^{\rm in}$ is absolutely irreducible if and only if the Hurwitz monodromy group H_r acts transitively on $\mathrm{Ni}(\mathbf{C})^{\rm in}$.

We remark that the subspace $\mathcal{H}(\mathbf{C})^{\rm ab}$ of $\mathcal{H}^{\rm ab}$ may be defined over $\mathcal{Q}$ even for non-rational $\mathbf{C}$. But if $\mathbf{C}$ is rational then $\mathcal{H}(\mathbf{C})^{\rm ab}$ is certainly defined over $\mathcal{Q}$. Also, $\mathcal{H}(\mathbf{C})^{\rm ab}$ is absolutely irreducible if and only if H_r is transitive on $\mathrm{Ni}(\mathbf{C})^{\rm ab}$. Here is the significance of Theorem 1 for the Inverse Galois Problem:

Corollary 1: *Keep the hypotheses of Theorem 1, and let K be any field of characteristic 0. Assume additionally that the group G has trivial center. Then G is regular over K with r branch points if and only if $\mathcal{H}^{\rm in} = \mathcal{H}_r^{\rm in}(G)$ has a K-rational point. More precisely:*

(a) *For each point $\boldsymbol{p} = |\varphi|$ of $\mathcal{H}^{\rm ab}$ the field $\mathcal{Q}(\boldsymbol{p})$ is the minimal field of definition of the cover φ, if either $U = 1$ or U is self-normalizing in G (cf. §1.5).*

(b) *For each point $\boldsymbol{p}' = |\chi, h|$ of $\mathcal{H}^{\rm in}$ the field $\mathcal{Q}(\boldsymbol{p}')$ is the minimal subfield k' of $\mathcal{C}$ such that the cover $\chi : \hat{X} \to \mathcal{P}^1$ together with all its automorphisms can be defined over k'. The resulting function field extension $L/k'(x)$, where $L = k'(\hat{X})$, is Galois with Galois group isomorphic to G, and L is regular over k'.*

Proof of Corollary 1: (a) Set $k_0 = \mathcal{Q}(\Psi(\boldsymbol{p}))$ as in §1.5. Then $\boldsymbol{p}$ is algebraic over k_0, and clearly $k = \mathcal{Q}(\boldsymbol{p})$ is the fixed field of the group of all $\beta \in G_{k_0}$ with $\boldsymbol{p}^\beta = \boldsymbol{p}$. By Theorem 1, k is the fixed field of the group of all $\beta \in G_{k_0}$ with φ^β equivalent to φ. From §1.5, this proves (a) (in view of (1)).

(b) Set $k_0 = \mathcal{Q}(\Psi'(\boldsymbol{p}'))$. If k' is a field such that χ together with all its automorphisms is defined over k', then $(\chi^\beta, h \circ \beta^{-1}) = (\chi, h)$ for all $\beta \in G_{k'}$, and $k_0 \subset k'$. By Theorem 1, $G_{k'}$ fixes $\boldsymbol{p}'$ and so $\mathcal{Q}(\boldsymbol{p}') \subset k'$.

It remains to show that χ together with all its automorphisms can actually be defined over $K' = \mathcal{Q}(\boldsymbol{p}')$. As in §1.5, the cover χ can be defined over $\bar{k}_0 = \bar{K}'$. For all $\beta \in G_{K'}$, we have $(\chi^\beta, h \circ \beta^{-1})$ equivalent to (χ, h) by Theorem 1. Thus there exist isomorphisms $\delta_\beta : \hat{X}^\beta \to \hat{X}$ over $\mathcal{P}^1$ with $h \circ \beta^{-1}(\delta_\beta^{-1} A \delta_\beta) = h(A)$ for each $A \in \mathrm{Aut}(\hat{X}/\mathcal{P}^1)$. The latter implies that $A^\beta = \delta_\beta^{-1} A \delta_\beta$. In particular, since G has trivial center, δ_β is uniquely determined by β. This uniqueness again forces the δ_β to satisfy Weil's cocycle condition, and by Weil's criterion it follows that the cover $\chi : \hat{X} \to \mathcal{P}^1$ can be defined over K' so that $\delta_\beta : \hat{X} = \hat{X}^\beta \to \hat{X}$ becomes the identity. Then $A^\beta = \delta_\beta^{-1} A \delta_\beta = A$ for all $A \in \mathrm{Aut}(\hat{X}/\mathcal{P}^1)$. That is, all automorphisms of χ are defined over K'. This proves the first claim in (b). The second follows immediately.

For the first assertion in Corollary 1, note that if $\mathcal{H}^{\rm in}$ has a point $\boldsymbol{p}'$ over the field K then we may assume that $\boldsymbol{p}'$ is a complex point (because $k' = \mathcal{Q}(\boldsymbol{p}')$ is finitely generated over $\mathcal{Q}$). Then (b) yields a regular Galois extension $L/k'(x)$ with group G and with r branch points. Tensoring with K shows that G is regular over K with r branch points. Conversely, suppose the latter holds. Then there is a finitely generated subfield K' of K such that G is regular over K' with r branch points; we may assume that K' is a subfield of $\mathcal{C}$. Hence there is a Galois cover $\chi : \hat{X} \to \mathcal{P}^1$ with r branch points and an isomorphism $h : \mathrm{Aut}(\hat{X}/\mathcal{P}^1) \to G$ such that χ together with all its automorphisms is defined over K'. By (b) it follows that $\mathcal{Q}(\boldsymbol{p}') \subset K'$, where $\boldsymbol{p}' = |\chi, h| \in \mathcal{H}^{\rm in}$. Thus $\boldsymbol{p}'$ is a point of $\mathcal{H}^{\rm in}$ that is rational over K. □

Corollary 1 shows that the $\mathcal{Q}$-structure on $\mathcal{H}^{\rm in}$ (and on its Hurwitz subspaces) is crucial for the Inverse Galois Problem. See [Fr,3] for a discussion in the case $r \le 4$, including a relation between Hurwitz spaces and modular curves for $r = 4$. In the following example we determine the $\mathcal{Q}$-structure of Hurwitz spaces $\mathcal{H}(\mathbf{C})^{\rm in}$ for which $\mathbf{C}$ satisfies the rigidity condition of Thompson [Th].

Example: *Hurwitz spaces and rigidity.* Assume G has trivial center. The r-tuple $\mathbf{C} = (C_1, \dots, C_r)$ of conjugacy classes of G is called *rigid* if the tuples $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}_r(G)$ with $\sigma_i \in C_i$ form a single (non-empty) orbit under $\mathrm{Inn}(G)$. Assume this holds. For simplicity we consider only the case that the C_i's are all distinct. (The transition to the general case is immediate). Then the elements of $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ correspond to the permutations of $C_1, ..., C_r$, and Q_i acts (via formula (2)) as the transposition $(i, i+1)$ on these permutations (for $i = 1, \dots, r-1$). Thus the Hurwitz group H_r acts through its natural S_r-quotient on $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$, more precisely, through the regular permutation representation of S_r. This determines the permutation representation of H_r that defines the equivalence class of the cover $\mathcal{H}(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}_r$ (cf. §1.3). It follows that this cover is equivalent over $\bar{\mathcal{Q}}$ to the cover

$$\mathcal{U}^{(r)} \stackrel{\mathrm{def}}{=} \{(x_1, \dots, x_r) \in (\mathcal{P}^1)^r : \ x_i \neq x_j \text{ for } i \neq j\} \to \mathcal{U}_r$$

where the (ordered) tuple $(x_1, \dots, x_r)$ is mapped to the set $\{x_1, \dots, x_r\} \in \mathcal{U}_r$.

Fix a $\bar{\mathcal{Q}}$-isomorphism $\theta : \mathcal{H}(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}^{(r)}$ over $\mathcal{U}_r$. Now assume additionally that the r-tuple $\mathbf{C}$ is rational. Then $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$ is an absolutely irreducible variety defined over $\mathcal{Q}$ (by Theorem 1). For $\beta \in G_{\mathcal{Q}}$, consider the map $\theta^\beta : \mathcal{H}(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}^{(r)}$ obtained by base change with β (where $\mathcal{U}^{(r)}$ is viewed as $\mathcal{Q}$-variety in the natural way). Set $c(\beta) = \theta^{-1}\theta^\beta$, an element of $\mathrm{Aut}(\mathcal{H}(\mathbf{C})^{\mathrm{in}}/\mathcal{U}_r)$.

Consider a point $\boldsymbol{p} \in \mathcal{H}(\mathbf{C})^{\mathrm{in}}$ that lies over the base point $\boldsymbol{b} = \{b_1, \dots, b_r\} \in \mathcal{U}_r$ (from §1.3). We assume here that all $b_i \in \mathcal{Q}$. Then β fixes all points of $\mathcal{U}^{(r)}$ that lie over $\boldsymbol{b}$, hence $c(\beta)(\boldsymbol{p}) = \theta^{-1}(\theta(\boldsymbol{p}^{\beta^{-1}}))^\beta = \boldsymbol{p}^{\beta^{-1}}$. The point $\boldsymbol{p}$ corresponds to the $\mathrm{Inn}(G)$-class of some tuple $(\sigma_1, \dots, \sigma_r) \in \mathrm{Ni}(\mathbf{C})$ under the identification from §1.3. Further, $\boldsymbol{p}^{\beta^{-1}}$ corresponds to the class of a tuple $(\rho_1, \dots, \rho_r)$ with ρ_i conjugate σ_i^m for all i, where m is given by the condition that β acts on the $|G|$-th roots of unity as $\zeta \mapsto \zeta^m$ (see §3.2 below).

Part 1: *The case that* $\mathbf{C}$ *is rationally rigid.* This means that the C_i are rational conjugacy classes (i.e., $C_i^m = C_i$ for all integers m prime to $|G|$). By the rigidity assumption, it follows that $(\sigma_1, \dots, \sigma_r)$ and $(\rho_1, \dots, \rho_r)$ are conjugate under $\mathrm{Inn}(G)$. That is, $\boldsymbol{p}^{\beta^{-1}} = \boldsymbol{p}$. Then also $c(\beta)(\boldsymbol{p}) = \boldsymbol{p}$, hence $c(\beta)$ is the identity (being an automorphism of an unramified cover). Thus θ is defined over $\mathcal{Q}$. Therefore the covers $\mathcal{H}(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}_r$ and $\mathcal{U}^{(r)} \to \mathcal{U}_r$ are equivalent over $\mathcal{Q}$.

Let $|\chi, h|$ be any point of $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$. It follows from the above and Corollary 1 that the cover χ together with all its automorphisms can be defined over some field k if and only if the branch points $x_1, \dots, x_r$ of χ are rational over k. As usual, then we have a Galois extension of $k(x)$ with group isomorphic to G, regular over k and with branch points $x_1, \dots, x_r$. This is also the conclusion of Thompson's rigidity criterion [Th].

Part 2: *An example with* $\mathbf{C}$ *rigid, but not rationally rigid.* Let $G = \mathrm{PSL}_2(p)$ for a prime $p > 3$ for which 3 is not a quadratic residue modulo p. Let C_1 be the conjugacy class of elements of order 3, and let C_2 and C_3 be the two conjugacy classes of G of elements of order p. Let $r = 3$ and $\mathbf{C} = (\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3)$. This triple is rational and rigid [Ma, 1; p. 180], but the single classes C_2 and C_3 are not rational: An element $\sigma \in G$ of order p is conjugate to σ^m if and only if m is a quadratic residue mod p. It follows that $c(\beta) = 1$ if and only if β acts on the p-th roots of unity as $\zeta \to \zeta^m$ with m a quadratic residue mod p. These β form a subgroup Γ of $G_{\mathcal{Q}}$ of index 2. ($\Gamma = G_K$ with $K = \mathcal{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Thus c takes only two values, the non-trivial value being an involution. Since all involutions in $\mathrm{Aut}(\mathcal{U}^{(3)}/\mathcal{U}_3) \cong S_3$ are conjugate, it follows that the space $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$ is $\mathcal{Q}$-isomorphic to that $\mathcal{Q}$-form of $\mathcal{U}^{(3)}$ given by the following action of $G_{\mathcal{Q}}$ on the $\bar{\mathcal{Q}}$-points: Each $\beta \in \Gamma$ sends (x_1, x_2, x_3) to $(x_1^\beta, x_2^\beta, x_3^\beta)$, and each $\beta \in G_{\mathcal{Q}} \backslash \Gamma$ sends (x_1, x_2, x_3) to $(x_1^\beta, x_3^\beta, x_2^\beta)$. □

§2.2. Irreducibility of Hurwitz spaces, and full high branching:

Corollary 1 shows that to go further with the inverse Galois problem we need to find $\mathcal{Q}$-points on $\mathcal{H}^{\mathrm{in}}$. These $\mathcal{Q}$-points lie on absolutely irreducible components of $\mathcal{H}^{\mathrm{in}}$ that are defined over $\mathcal{Q}$. The first step, therefore, is to find such components of $\mathcal{H}^{\mathrm{in}}$. Theorem 1 gives a criterion to decide when a Hurwitz subspace $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$ of $\mathcal{H}^{\mathrm{in}}$ is such a component. To apply this criterion, the following group-theoretic condition is crucial:

(*) The Schur multiplier of G is generated by commutators (cf. §2.4).

An (unpublished) theorem of Conway and Parker [CP] shows that the Hurwitz group H_r acts transitively on $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ if (*) holds and the r-tuple $\mathbf{C}$ contains each non-trivial conjugacy class of G a suitably large number of times. For the convenience of the reader, we supply a proof of this in the Appendix, adapted from [CP]. It follows from Theorem 1 that the Hurwitz space $\mathcal{H} = \mathcal{H}(\mathbf{C})^{\mathrm{in}}$ is absolutely irreducible under the above conditions. If, in addition, $\mathbf{C}$ is rational and $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ is non-empty (this holds, for example, if each non-trivial conjugacy class of G occurs the *same* — suitably large — number of times in $\mathbf{C}$), then the corresponding Hurwitz space is the desired absolutely irreducible $\mathcal{Q}$-component of $\mathcal{H}^{\mathrm{in}}$. Summarizing:

Proposition 1: *Assume that G satisfies (*). Then for infinitely many r, there exists an r-tuple $\mathbf{C}$ of conjugacy classes of G with the following property: The Hurwitz space $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$ is an absolutely irreducible component of $\mathcal{H}_r^{\mathrm{in}}(G)$ that is defined over $\mathcal{Q}$. In particular, the latter is true if $\mathbf{C}$ is rational, $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ is non-empty and $\mathbf{C}$ contains each non-trivial conjugacy class of G a suitably large number of times.*

In Lemma 2 below we show that each finite group H is the quotient of a finite group G that satisfies (*) and has trivial center. Thus, in order to demonstrate that H is regular over $\mathcal{Q}$, by Corollary 1 it suffices to show the following: One of the absolutely irreducible Hurwitz spaces $\mathcal{H}$ defined over $\mathcal{Q}$ that are associated to G has a $\mathcal{Q}$- rational point. At this time we don't know how to get a rational point on $\mathcal{H}$. But, as far as we know, it is even possible that for suitably large r, $\mathcal{H}$ is a unirational variety. In this case, it has a dense set of rational points.

It seems natural to conjecture that if a group G can be realized as $G(L/\mathcal{Q}(x))$ with L regular over $\mathcal{Q}$, then in fact there are such realizations with an arbitrarily large number of branch points (i.e., $\mathcal{H}_r^{\mathrm{in}}(G)$ has $\mathcal{Q}$-points for infinitely many r). Let $\chi : X \to \mathcal{P}^1$ be a cover with r branch points corresponding to the function field extension $L/\mathcal{Q}(x)$, let $h : G(L/\mathcal{Q}(x)) \to G$ be an isomorphism, and let $\boldsymbol{p}' \in \mathcal{H}_r^{\mathrm{in}}(G)$ be the point corresponding to the pair (χ, h). To each branch point of the cover χ there is associated a conjugacy class of G (via the isomorphism h), represented by the corresponding *branch cycle*. The conjugacy classes of G arising that way are exactly those occurring in the r-tuple $\mathbf{C}$ with $\boldsymbol{p}' \in \mathcal{H}(\mathbf{C})^{\mathrm{in}}$. We say that G is regular over $\mathcal{Q}$ with *full high branching* if for each integer t the group G can be realized as $G(L/\mathcal{Q}(x))$ (with L regular over $\mathcal{Q}$) in such a way that each non-trivial conjugacy class of G is associated to at least t branch points.

For an r-tuple $\mathbf{C}$ of conjugacy classes of G, let $\tau(\mathbf{C}) \geq 0$ be the minimal number of times that any non-trivial conjugacy class of G occurs in $\mathbf{C}$. We can arrange all the rational tuples $\mathbf{C}$ of non-trivial conjugacy classes of G in a doubly indexed collection $\{\mathbf{C}_{t\,i}\}_{t\in\mathcal{N}, i\in I_t}$ with $\tau(\mathbf{C}_{t\,i}) = t$. From Corollary 1 and Proposition 1 we get the following result:

Proposition 2: *Suppose G satisfies (*) and has trivial center. Then for suitably large t, the Hurwitz spaces $\mathcal{H}(\mathbf{C}_{t\,i})^{\mathrm{in}}$ are absolutely irreducible varieties defined over $\mathcal{Q}$. And G is regular over $\mathcal{Q}$ with full high branching (as defined above) if and only if for infinitely many values of t there exist such Hurwitz spaces $\mathcal{H}(\mathbf{C}_{t\,i})^{\mathrm{in}}$ that have $\mathcal{Q}$-points.*

§**2.3. The application to PAC-fields:** A field P is called P(seudo)A(lgebraically)C(losed) if every absolutely irreducible variety defined over P has a P-rational point. Consider a PAC-field P of characteristic 0. It follows from Corollary 1 and Proposition 1 that every finite group G satisfying (*) and having trivial center is regular over P. But by Lemma 2 below the quotients of these groups G yield all finite groups. Thus we get the following result.

Theorem 2: *If P is a PAC-field of characteristic 0, then every finite group is regular over P. In particular, if P is also Hilbertian, then every finite group is a Galois group over P.*

PAC-fields first appeared in [Ax] and have been studied since then by various authors (cf. [FrJ]). PAC fields have projective absolute Galois group—a result of Ax [FrJ; Theorem 10.17]. Conversely, if H is a projective profinite group, then there exists a PAC field P such that H is the absolute Galois group of P—an observation of Lubotzky and van den Dries ([LD], [FrJ; Corollary 20.16]).

There are many examples of Hilbertian PAC fields inside of $\bar{\mathcal{Q}}$. For example, F. Pop [P] has recently announced that one obtains a PAC-field by adjoining $\sqrt{-1}$ to the field of all totally real algebraic numbers. This PAC-field is Hilbertian by Weissauer's theorem [Ws] (which says that any *proper* finite extension of a Galois extension of a Hilbertian field is Hilbertian). Thus Theorem 2 applies to it. Furthermore, there are PAC-fields P with the property that they are Galois over $\mathcal{Q}$, and $G(P/\mathcal{Q}) \cong \prod_{n=2}^{\infty} S_n$ [FrJ; p. 224, Theorem 16.46]. Again these are also Hilbertian by Weissauer's theorem.

On the other hand, the abelian closure of any number field has projective absolute Galois group and it is Hilbertian [FrJ; Theorem 15.6]. But Frey noted that such a field isn't PAC ([Fy] or [FrJ; Corollary 10.15]). Shafarevich conjectured that the abelian closure of the rationals has an ω-free absolute Galois group. Our methods yield an analogue of this (to appear in a sequel to the present paper): Every countable Hilbertian PAC-field of characteristic 0 has an ω-free absolute Galois group (cf. the Introduction). Now let $\mathcal{F}_p$ denote the finite field with p elements.

Corollary 2: *Let G be any finite group. Then G is regular over $\mathcal{F}_p$ for all but finitely many primes p.*

Corollary 2 can be derived from Theorem 2 as follows: Assume the claim is wrong for infinitely many primes p. Then there exists a non-principal ultraproduct P of the fields $\mathcal{F}_p$ for these primes p. The field P is a PAC-field by a result of Ax [FrJ; Cor. 10.6] (this was the original motivation for the introduction of PAC-fields). Also, $\mathrm{char}(P) = 0$. Thus G is regular over P by Theorem 2. It is easy to give first order quantified statements equivalent to the statement that G is regular over a given field; it is an *elementary* statement. Thus it follows that G is regular over some (in fact, infinitely many) of the fields $\mathcal{F}_p$ occurring in the above ultraproduct—a contradiction. We omit the details, and rather give the following more direct proof. The underlying idea is the same as for the proof that the above ultraproduct is PAC; it uses the existence of $\mathcal{F}_p$-rational points on absolutely irreducible varieties defined over $\mathcal{F}_p$, for sufficiently large p (the Lang-Weil observation). First we need a basic lemma:

Lemma 0: *Suppose R is an integral domain, and k is its field of fractions. Let $L/k(x)$ be a finite Galois extension, regular over k. Then there is some $u \neq 0$ in R with the following property: For any field k' such that R admits a homomorphism $\lambda : R \to k'$ with $\lambda(u) \neq 0$, there is a Galois extension $L'/k'(x')$ with x' transcendental over k' and L' regular over k' and $G(L'/k'(x')) \cong G(L/k(x))$.*

Proof: Choose $y_1 \in L$ with $L = k(x, y_1)$. Then there is a polynomial $f \in R[x, y]$ of degree $n = [L : k(x)]$ in y, such that $f(x, y_1) = 0$. By multiplying y_1 by the y^n-coefficient of f we may assume that f is monic in y. Then f is absolutely irreducible (as a polynomial in two variables over k) since L is regular over k.

By the Bertini-Noether theorem (e.g., [FrJ, Prop. 8.8]) there is some $u_0 \neq 0$ in R with this property: If λ is a homomorphism from R to a field k' with $\lambda(u_0) \neq 0$, then the image $f' \in k'[x, y]$ of f under λ is again absolutely irreducible. From now on we assume that this condition $\lambda(u_0) \neq 0$ holds.

The map λ extends canonically to a map $R[x] \to k'[x']$, sending x to some element x' that is transcendental over k'. This map can further be extended to a place of L: a homomorphism $\bar{\lambda}$ from some valuation ring P of L (containing $R[x]$) into the algebraic closure of $k'(x')$. Since P is integrally closed and $f(x, y)$ is monic in y, the elements $y_1, \ldots, y_n \in L$ with $f(x, y_i) = 0$ lie in P. Set $L' = k'(x', y_1', \ldots, y_n')$, where $y_i' = \bar{\lambda}(y_i)$.

Since $f'(x', y_i') = 0$ and f' is absolutely irreducible, the element y_i' has degree n over $k'(x')$. Hence for any $b \in R[x, y_i]$ we have: $\bar{\lambda}(b) = 0$ if and only if λ annihilates all coefficients in the unique expression of b as an R-linear combination of the $x^\nu y_i^\mu$ with $\nu \geq 0, 0 \leq \mu \leq n-1$. We will refer to this fact as the criterion (C).

Since L is the field of fractions of $S_1 \stackrel{\mathrm{def}}{=} R[x, y_1]$, there is $c \neq 0$ in S_1 such that $cy_i \in S_1$ for all $i = 1, \ldots, n$. Then $b = c \prod_{i \neq j}(cy_i - cy_j)$ is a non-zero element of S_1, and $by_i \in S_1$ for all i. By criterion (C), we can multiply u_0 by certain elements of R to obtain some $u \neq 0$ in R with the following property: If $\lambda(u) \neq 0$ then $\bar{\lambda}(\sigma(b)) \neq 0$ for all $\sigma \in G(L/k(x))$.

We will show that u is as desired. So assume $\lambda(u) \neq 0$. Then $y_i' = \bar{\lambda}(b)^{-1} \bar{\lambda}(by_i) \in k'(x', y_1')$ for all i. Therefore $L' = k'(x', y_1', \ldots, y_n') = k'(x', y_1')$. Thus $[L' : k'(x')] = n$, and L' is regular over k' (since f' is absolutely irreducible). Furthermore, since $\bar{\lambda}(b) \neq 0$, the $y_1', \ldots, y_n'$ are pairwise distinct.

It remains to show that L' is Galois over $k'(x')$ with Galois group isomorphic to $G \stackrel{\text{def}}{=} G(L/k(x))$. The ring $S = R[x, y_1, \ldots, y_n]$ is clearly invariant under G. We claim that also $S \cap \ker(\bar{\lambda})$ is G-invariant: Namely, for each $s \in S$ the element $s_1 = b^m s$ lies in S_1 for some positive integer m. If $\bar{\lambda}(s) = 0$ then $\bar{\lambda}(s_1) = 0$. By criterion (C) it follows that $\bar{\lambda}(\sigma(s_1)) = 0$ for each $\sigma \in G$. Thus $\bar{\lambda}(\sigma(b))^m \bar{\lambda}(\sigma(s)) = 0$, which implies $\bar{\lambda}(\sigma(s)) = 0$.

It follows that G acts naturally on $\bar{\lambda}(S)$. This yields a homomorphism $G \to \mathrm{Aut}(L'/k'(x'))$, which is injective since G acts transitively on $y'_1, \ldots, y'_n$ (and $|G| = n$). Thus $|\mathrm{Aut}(L'/k'(x'))| \geq n = [L' : k'(x')]$, which shows that L' is Galois over $k'(x')$ with group isomorphic to G. □

Proof of Corollary 2: By Lemma 2 we may assume that G satisfies (*) and has trivial center.

Part 1: Here we show that there exists a finite extension $k'/\mathcal{Q}(t)$, with t transcendental over $\mathcal{Q}$ and k' regular over $\mathcal{Q}$, and a Galois extension $L'/k'(x)$, regular over k' and with Galois group isomorphic to G.

By Proposition 1 there exists $r \geq 3$ such that the space $\mathcal{H}_r^{\text{in}}(G)$ has an absolutely irreducible component $\mathcal{H}$ defined over $\mathcal{Q}$. Let $\boldsymbol{p}$ be a generic point of $\mathcal{H}$ over $\mathcal{Q}$, and consider $k \stackrel{\text{def}}{=} \mathcal{Q}(\boldsymbol{p}) = \mathcal{Q}(\mathcal{H})$. Corollary 1 gives a Galois extension $L/k(x)$, regular over k, with Galois group isomorphic to G. Let $R \subset k$ be the coordinate ring of an affine open subset $\mathcal{H}_0$ of $\mathcal{H}$ defined over $\mathcal{Q}$. Let u be a non-zero element of R with the properties from Lemma 0, and let $\mathcal{H}_1$ be the complement of the vanishing set of u in $\mathcal{H}_0$. By [FrJ, Cor. 9.32] there exists an absolutely irreducible curve C on $\mathcal{H}_1$ defined over $\mathcal{Q}$. The restriction homomorphism $\lambda : R \to k'$, where $k' = \mathcal{Q}(C)$, satisfies $\lambda(u) \neq 0$. Therefore, by Lemma 0 there exists a Galois extension $L'/k'(x)$ with the desired properties. (Indeed, k' is regular over $\mathcal{Q}$ because C is absolutely irreducible).

Part 2: *Reduction mod p.* As in the proof of Lemma 0 we have $k' = \mathcal{Q}(t, z)$ with $f(t, z) = 0$, where $f \in \mathcal{Z}[T, Z]$ is an absolutely irreducible polynomial, monic and of degree $m = [k' : \mathcal{Q}(t)]$ in Z. By Bertini-Noether, f remains absolutely irreducible modulo p for all but finitely many primes p. Thus it follows from the Lang-Weil estimate for the number of rational points on a curve over a finite field (e.g., [FrJ, Th. 3.14]) that the number of pairs $(a, b) \in (\mathcal{F}_p)^2$ with $f(a, b) = 0$ goes to infinity as $p \to \infty$.

Now let u be an element of $R = \mathcal{Z}[t, z] \subset k'$ with the properties from Lemma 0 (with respect to the extension $L'/k'(x)$ constructed in Part 1). We have $u = g(t, z)$ for a unique polynomial $g \in \mathcal{Z}[T, Z]$ of degree $< m$ in Z. By Bezout's theorem, the number of common solutions of $f(a, b) = 0$ and $g(a, b) = 0$ over $\mathcal{F}_p$ is bounded independent of p (since f is absolutely irreducible and $g \not\equiv 0 \pmod{p}$ for all but finitely many p). Hence for all but finitely many primes p there exists $(a_0, b_0) \in (\mathcal{F}_p)^2$ with $f(a_0, b_0) = 0$ and $g(a_0, b_0) \neq 0$. Such a point (a_0, b_0) yields a homomorphism $\lambda : R \to \mathcal{F}_p$ (sending t to a_0 and z to b_0) with $\lambda(u) \neq 0$. Now the claim follows from Lemma 0. □

§**2.4. Two group-theoretic Lemmas:** The goal of this section is to prove Lemma 2 below: Every finite group is the quotient of a finite group G with trivial center satisfying (*). These conditions were needed above to guarantee the existence of absolutely irreducible $\mathcal{Q}$-components of the parameter space $\mathcal{H}^{\text{in}}$.

For any finite group G let G' denote its commutator subgroup and $Z(G)$ its center. Recall that a *representation group* R of G is a group of maximal order with the property that R has a subgroup $M \subseteq R' \cap Z(R)$ satisfying $R/M \cong G$. Such an R always exists (but it is not necessarily unique). The group M is isomorphic to the Schur multiplier $M(G) = H^2(G, \mathcal{C}^*)$ of G [Hu; p. 631]. We say that $M(G)$ is *generated by commutators* (condition (*)) if $M \cap \{g^{-1}h^{-1}gh \mid g, h \in R\}$ generates M. This is independent of the choice of R. Our first lemma shows that representation groups satisfy this condition.

Lemma 1: *If H is a finite group and G is a representation group of H, then the Schur multiplier $M(G)$ is generated by commutators.*

Proof: We have a surjection $G \to H$ with kernel $M_H \cong M(H)$ satisfying
$M_H \leq G' \cap Z(G)$. Let R be a representation group of G. Then we have a surjection $R \to G$ with kernel $M \cong M(G)$ satisfying $M \leq R' \cap Z(R)$. Let C be the subgroup of M generated by commutators (from R), and consider $\bar{R} \stackrel{\text{def}}{=} R/C$. Then $\bar{M} \stackrel{\text{def}}{=} M/C$ contains no non-trivial commutators (from $\bar{R}$), and $\bar{M} \leq \bar{R}' \cap Z(\bar{R})$.

The map $R \to G$ induces a map $\varphi : \bar{R} \to G$ with kernel $\bar{M}$. From $M_H \leq G'$ we get $L \stackrel{\text{def}}{=} \varphi^{-1}(M_H) \leq \bar{R}'\bar{M} = \bar{R}'$. Clearly, $\bar{R}/L \cong H$. Furthermore, $[\bar{R}, L] \subset \bar{M}$. Since $\bar{M}$ contains no non-trivial commutators, $[\bar{R}, L] = 1$. Therefore, $\bar{R}$ is a central extension of H with kernel $L \leq \bar{R}'$. It follows that $|L| \leq |M(H)|$. That is, $\bar{M} = 1$ and $M = C$. This proves the lemma. □

Lemma 2: *Every finite group H is the quotient of a finite group G with trivial center such that the Schur multiplier of G is generated by commutators (Condition (*)).*

Proof: By Lemma 1 we may assume that H already has property (*) (Replacing H by a representation group of H). Let $m = |H|$, let S be a non-abelian finite simple group with trivial Schur multiplier (e.g., $S = \mathrm{SL}_2(8)$, see [Hu, Satz 25.7]) and set $A = S^m$, the direct product of m copies of S. The (regular) *wreath-product* G of S and H is defined to be the semi-direct product $G = A \times^s H$ where H acts on A by permuting the factors of A sharply transitively (i.e., in its regular permutation representation). Clearly G has trivial center.

Any central extension of S splits because $M(S) = 1$. By a simple induction argument, it follows that also every central extension of $A = S^m$ splits. This implies that every representation group of G has a normal subgroup isomorphic to A such that the quotient by this subgroup is a representation group of H. Therefore, $M(G) \cong M(H)$ is generated by commutators. □

3. PROOF OF THEOREM 1 UNDER A CONTINUITY ASSUMPTION

Assume the hypotheses of Theorem 1. The unramified coverings $\Psi : \mathcal{H}^{\mathrm{ab}} \to \mathcal{U}_r$ and $\Psi' : \mathcal{H}^{\mathrm{in}} \to \mathcal{U}_r$ equip the spaces $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ with a unique structure as (non-singular, usually reducible) algebraic varieties defined over $\mathcal{C}$ (compatible with their analytic structure) such that the maps Ψ and Ψ' are algebraic morphisms defined over $\mathcal{C}$. This follows from the generalized Riemann existence theorem (see [SGA1, exp. XII, Th. 5.1]). By [Se, Thm. 6.7], the field $\mathcal{C}$ can be replaced by $\bar{\mathcal{Q}}$ in the above statement.

From now on we view the spaces $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ as equipped with this natural structure of a variety defined over $\bar{\mathcal{Q}}$. The resulting notion of $\bar{\mathcal{Q}}$-points of $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ is clearly compatible with the definition in §2.1. Furthermore, $\Lambda : \mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$ becomes a morphism defined over $\bar{\mathcal{Q}}$. For each automorphism β of $\mathcal{C}$ let $\epsilon_\beta : (\mathcal{H}^{\mathrm{ab}})^\beta \to \mathcal{H}^{\mathrm{ab}}$ be the map sending $|\varphi|^\beta$ to $|\varphi^\beta|$ (where $|\varphi| \in \mathcal{H}^{\mathrm{ab}}$). Then ϵ_β is well-defined (cf. §2.1) and bijective, and we have $\Psi \circ \epsilon_\beta = \Psi^\beta$.

Similarly, let $\epsilon'_\beta : (\mathcal{H}^{\mathrm{in}})^\beta \to \mathcal{H}^{\mathrm{in}}$ be the map sending $|\chi, h|^\beta$ to $|\chi^\beta, h \circ \beta^{-1}|$ (where $|\chi, h| \in \mathcal{H}^{\mathrm{in}}$). Also ϵ'_β is bijective, and $\Psi' \circ \epsilon'_\beta = (\Psi')^\beta$. In the remainder of §3 we show that Theorem 1 holds under the assumption that the maps ϵ_β and ϵ'_β are continuous (in the complex topology). In §4 this assumption is verified in the special case that U is self-normalizing in G. In §5 we reduce the problem to this special case.

§3.1. The $\mathcal{Q}$-structure on $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$: Assume that the map $\epsilon_\beta : (\mathcal{H}^{\mathrm{ab}})^\beta \to \mathcal{H}^{\mathrm{ab}}$ is continuous (in the complex topology) for each $\beta \in \mathrm{Aut}(\mathcal{C})$. Since ϵ_β is bijective and $\Psi \circ \epsilon_\beta = \Psi^\beta$, it follows that ϵ_β is a complex analytic isomorphism, inducing an equivalence between the coverings Ψ and Ψ^β. By the uniqueness of the algebraic structure of $\mathcal{H}^{\mathrm{ab}}$, the map ϵ_β is even an algebraic isomorphism defined over $\bar{\mathcal{Q}}$. Further, ϵ_β depends only on the restriction of β to $\bar{\mathcal{Q}}$ (since the $\bar{\mathcal{Q}}$-points are dense on $\mathcal{H}^{\mathrm{ab}}$, and the corresponding covers φ can be defined over $\bar{\mathcal{Q}}$, see §2.1). Thus we use the notation ϵ_β also for $\beta \in G_{\mathcal{Q}}$. (Because our maps act from the left, we use the convention $\varphi^{\alpha\beta} = (\varphi^\beta)^\alpha$.) It is straightforward to check that the ϵ_β ($\beta \in G_{\mathcal{Q}}$) satisfy Weil's cocycle condition:

$$\epsilon_\alpha \circ \epsilon_\beta^\alpha\ (|\varphi|^{\alpha\beta}) = \epsilon_\alpha((\epsilon_\beta(|\varphi|^\beta))^\alpha) = \epsilon_\alpha(|\varphi^\beta|^\alpha) = |\varphi^{\alpha\beta}| = \epsilon_{\alpha\beta}(|\varphi|^{\alpha\beta}) \qquad (\alpha, \beta \in G_{\mathcal{Q}})$$

Hence $\mathcal{H}^{\mathrm{ab}}$ can be defined over $\mathcal{Q}$ such that $\epsilon_\beta : \mathcal{H}^{\mathrm{ab}} = (\mathcal{H}^{\mathrm{ab}})^\beta \to \mathcal{H}^{\mathrm{ab}}$ is the identity. Since $\Psi \circ \epsilon_\beta = \Psi^\beta$ it follows that also $\Psi : \mathcal{H}^{\mathrm{ab}} \to \mathcal{U}_r$ is defined over $\mathcal{Q}$. Further it is clear that condition (a) of Theorem 1 holds.

Assuming that $\epsilon'_\beta : (\mathcal{H}^{\mathrm{in}})^\beta \to \mathcal{H}^{\mathrm{in}}$ is continuous (in the complex topology) for each $\beta \in \mathrm{Aut}(\mathcal{C})$, we conclude similarly that $\Psi' : \mathcal{H}^{\mathrm{in}} \to \mathcal{U}_r$ can be defined over $\mathcal{Q}$ such that condition (b) of Theorem 1 holds.

§3.2. The remaining part of Theorem 1: We have shown that the spaces $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ are equipped with a $\mathcal{Q}$-variety structure such that (a) and (b) of Theorem 1 hold. Then also $\Lambda : \mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$ is defined over $\mathcal{Q}$ (c.f. §5.1).

Further, the connected components (in the complex topology) of $\mathcal{H}^{\mathrm{ab}}$ and $\mathcal{H}^{\mathrm{in}}$ are irreducible, since they are complex (nonsingular) manifolds. In §1.3 we have set up a 1-1 correspondence between the components of $\mathcal{H}^{\mathrm{in}} = \mathcal{H}_r^{\mathrm{in}}(G)$ and the orbits of the Hurwitz monodromy group H_r on the set $\mathcal{E}_r^{\mathrm{in}} = \mathcal{E}_r^{\mathrm{in}}(G)$. The last assertion in Theorem 1 is a special case of this.

It remains to show that the Hurwitz space $\mathcal{H}(\mathbf{C})^{\text{in}}$ is defined over $\mathcal{Q}$ if and only if the r-tuple $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ of conjugacy classes of G is rational. Consider the group $\Gamma_0 = \pi_1(\mathcal{P}^1 \setminus \boldsymbol{b}, b_0) = \langle \gamma_1, \dots, \gamma_r \rangle$ as in §1.3, and let $\boldsymbol{p} = |\chi, h|$ be a point in $(\Psi')^{-1}(\boldsymbol{b})$. As usual, we write $\chi : \hat{X} \to \mathcal{P}^1$. Let $\iota : \Gamma_0 \to \mathrm{Aut}(\hat{X}/\mathcal{P}^1)$ be the surjection from §1.2 (canonical up to inner automorphisms), and set $f = h \circ \iota$, $\tau_i = \iota(\gamma_i)$ for $i = 1, \dots, r$. Then under the bijection from §1.3, the point $\boldsymbol{p}$ corresponds to the class of $(\sigma_1, \dots, \sigma_r)$ in $\mathcal{E}_r^{\text{in}}$, where $\sigma_i = f(\gamma_i) = h(\tau_i)$. By definition, $\boldsymbol{p} \in H(\mathbf{C})^{\text{in}}$ if and only if $(\sigma_1, \dots, \sigma_r) \in \mathrm{Ni}(\mathbf{C})$; the latter means that there exists $\pi \in S_r$ such that $\sigma_i \in \mathrm{C}_{\pi(i)}$ for $i = 1, \dots, r$.

The *branch cycle argument* from [Fr,1; p. 63] (see also [Ma,1; p. 47]) yields the following: For a fixed $\beta \in \mathrm{Aut}(\mathcal{C})$, let $\iota' : \Gamma_0 \to \mathrm{Aut}(\hat{X}^\beta/\mathcal{P}^1)$ be defined analogously as ι, and set $\tau_j' = \iota'(\gamma_j)$ for $j = 1, \dots, r$. Then the element $\tau_i^\beta \in \mathrm{Aut}(\hat{X}^\beta/\mathcal{P}^1)$ is conjugate to $(\tau_j')^m$, where the integer m is given by the condition that β acts on the $|G|$-th roots of unity as $\zeta \mapsto \zeta^m$, and the index j is given by $\beta(b_i) = b_j$. (Recall that by our choice of $\boldsymbol{b} = \{b_1, \dots, b_r\}$ from §1.1, β permutes $b_1, \dots, b_r$.) Choose an integer n with $mn \equiv 1 \pmod{|G|}$. Since $\boldsymbol{p}^\beta = |\chi^\beta, h \circ \beta^{-1}|$ (assertion (b)), it follows that the element of $\mathcal{E}_r^{\text{in}}$ corresponding to $\boldsymbol{p}^\beta$ is the class of $(h \circ \beta^{-1}(\tau_1'), \dots, h \circ \beta^{-1}(\tau_r'))$; this r-tuple has the property that its j-th entry is conjugate to σ_i^n, where $\beta(b_i) = b_j$. It follows that $\boldsymbol{p} \in \mathcal{H}(\mathbf{C})^{\text{in}}$ if and only if $\boldsymbol{p}^\beta \in \mathcal{H}(\mathbf{C}^n)^{\text{in}}$, where $\mathbf{C}^n = (C_1^n, \dots, C_r^n)$ (as above).

We have proved that β maps $\mathcal{H}(\mathbf{C})^{\text{in}}$ to $\mathcal{H}(\mathbf{C}^n)^{\text{in}}$. Thus $\mathcal{H}(\mathbf{C})^{\text{in}}$ is defined over $\mathcal{Q}$ if and only if $\mathcal{H}(\mathbf{C}^n)^{\text{in}} = \mathcal{H}(\mathbf{C})^{\text{in}}$ for all integers n that are prime to $|G|$. This is true if and only if $\mathrm{Ni}(\mathbf{C}^n) = \mathrm{Ni}(\mathbf{C})$ for all n prime to $|G|$. That is, if and only if $\mathbf{C}$ is rational (as defined in §1.1). This concludes the proof of Theorem 1 under the assumption that the maps ϵ_β and ϵ_β' are continuous.

4. FAMILIES OF COVERS

In this section we assume that the hypotheses of Theorem 1 hold, and additionally, that U is self-normalizing in G. Then, from (1) of §1.2, each cover $\varphi : X \to \mathcal{P}^1$ representing a point of $\mathcal{H}^{\text{ab}} = \mathcal{H}_r^{\text{ab}}(G, U)$ satisfies $\mathrm{Aut}(X/\mathcal{P}^1) = \{1\}$.

We construct a family of affine covers that represent the points of $\mathcal{H}_r^{\text{ab}}(G, U)$. It is clear how to construct the family locally, and then the condition $\mathrm{Aut}(X/\mathcal{P}^1) = \{1\}$ allows one to glue the local families uniquely. The family of corresponding compact covers was constructed in [Fr,1]. The construction there also applies to inspect the obstruction for the existence of a total representing family for $\mathcal{H}_r^{\text{ab}}(G, U)$ even when $\mathrm{Aut}(X/\mathcal{P}^1) \neq \{1\}$ (the obstruction is in the second étale cohomology group of $\mathcal{H}_r^{\text{ab}}(G, U)$ with coefficients in the locally constant "center sheaf"), but we don't need this here.

Let $\mathcal{U}$ be the set of all pairs $(\boldsymbol{a}, z) \in \mathcal{U}_r \times \mathcal{P}^1$ with $z \notin \boldsymbol{a}$. Then $\mathcal{U}$ is a Zariski-open subset of $\mathcal{U}_r \times \mathcal{P}^1$ defined over $\mathcal{Q}$. For the moment, we view $\mathcal{U}$ only as an open submanifold of $\mathcal{U}_r \times \mathcal{P}^1$.

§**4.1. The topological construction of the family:** Here the term 'covering' denotes an unramified topological covering map (of not necessarily connected spaces). We start with the covering $\Psi : \mathcal{H}^{\text{ab}} = \mathcal{H}_r^{\text{ab}}(G, U) \to \mathcal{U}_r$ of §1.2. Set

$$\mathcal{M} = \{(\boldsymbol{p}, z) \in \mathcal{H}^{\text{ab}} \times \mathcal{P}^1 : \ z \notin \Psi(\boldsymbol{p}) \ \}.$$

Then $\mathcal{M}$ is an open subspace of $\mathcal{H}^{\text{ab}} \times \mathcal{P}^1$, and the map $(\boldsymbol{p}, z) \mapsto (\Psi(\boldsymbol{p}), z)$ yields a covering $F : \mathcal{M} \to \mathcal{U}$. Let $P : \mathcal{M} \to \mathcal{H}^{\text{ab}}$ be the projection on the first coordinate.

Consider a point $\boldsymbol{p} \in \mathcal{H}^{\text{ab}}$ and a neighborhood $\mathcal{N}^{(\boldsymbol{p})} = \mathcal{N}(\boldsymbol{p}; D_1, \dots, D_r)$ of $\boldsymbol{p}$ as in §1.2. Then Ψ maps $\mathcal{N}^{(\boldsymbol{p})}$ homeomorphically onto the set $\mathcal{V}(D_1, \dots, D_r) \cong D_1 \times \cdots \times D_r$ of all $\boldsymbol{a} \in \mathcal{U}_r$ with $|\boldsymbol{a} \cap D_i| = 1$ for $i = 1, \dots, r$. In particular, $\mathcal{N}^{(\boldsymbol{p})}$ is contractible. Furthermore, F maps the set $\mathcal{M}(\boldsymbol{p}; D_1, \dots, D_r) = \mathcal{M}^{(\boldsymbol{p})} \stackrel{\text{def}}{=} P^{-1}(\mathcal{N}^{(\boldsymbol{p})})$ homeomorphically onto the set of all $(\boldsymbol{a}, z) \in \mathcal{U}$ with $\boldsymbol{a} \in \mathcal{V}(D_1, \dots, D_r)$. Thus $\mathcal{M}^{(\boldsymbol{p})}$ contains the set $\mathcal{N}^{(\boldsymbol{p})} \times \ \mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r)$ as a deformation retract. Choose a base point $a_0 \in \mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r)$. We have canonical isomorphisms

$$\pi_1(\mathcal{P}^1 \setminus \Psi(\boldsymbol{p}), a_0) \cong \pi_1(\mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r), a_0) \cong$$
$$\pi_1(\mathcal{N}^{(\boldsymbol{p})} \times \ \mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r), (\boldsymbol{p}, a_0)) \cong \pi_1(\mathcal{M}^{(\boldsymbol{p})}, (\boldsymbol{p}, a_0)).$$

Now let $\varphi : X \to \mathcal{P}^1$ be a cover representing the point $\boldsymbol{p} \in \mathcal{H}^{\rm ab}$, and let $[U_\varphi]$ be the associated class of subgroups of $\pi_1(\mathcal{P}^1 \setminus \Psi(\boldsymbol{p}))$ (see §1.2). Under the above isomorphisms, $[U_\varphi]$ corresponds to a class of subgroups of $\pi_1(\mathcal{M}^{(\boldsymbol{p})}, (\boldsymbol{p}, a_0))$, and this class of subgroups gives rise to a covering $\mathcal{T}(\boldsymbol{p}; D_1, \ldots, D_r) \to \mathcal{M}^{(\boldsymbol{p})} = \mathcal{M}(\boldsymbol{p}; D_1, \ldots, D_r)$. This covering has no non-trivial automorphisms, since U is self-normalizing in G (c.f. (1) in §1.2).

From the lack of non-trivial automorphisms of the above covering it follows that for each inclusion $\mathcal{M}(\boldsymbol{p}; D_1, \ldots, D_r) \to \mathcal{M}(\boldsymbol{p}'; D'_1, \ldots, D'_r)$ of two of the above neighborhoods, there is a unique embedding $\mathcal{T}(\boldsymbol{p}; D_1, \ldots, D_r) \to \mathcal{T}(\boldsymbol{p}'; D'_1, \ldots, D'_r)$ making the following diagram commute (where the vertical arrows are the coverings constructed in the last paragraph):

$$\begin{array}{ccc} \mathcal{T}(\boldsymbol{p}; D_1, \ldots, D_r) & \longrightarrow & \mathcal{T}(\boldsymbol{p}'; D'_1, \ldots, D'_r) \\ \downarrow & & \downarrow \\ \mathcal{M}(\boldsymbol{p}; D_1, \ldots, D_r) & \longrightarrow & \mathcal{M}(\boldsymbol{p}'; D'_1, \ldots, D'_r) \end{array}$$

From this uniqueness and the fact that the $\mathcal{N}^{(\boldsymbol{p})}$ form a basis for the topology of $\mathcal{H}^{\rm ab}$, it follows that the coverings $\mathcal{T}(\boldsymbol{p}; D_1, \ldots, D_r) \to \mathcal{M}(\boldsymbol{p}; D_1, \ldots, D_r)$ glue together to yield a global covering $\Phi : \mathcal{T} \to \mathcal{M}$. For each $\boldsymbol{p} \in \mathcal{H}^{\rm ab}$ denote $(P \circ \Phi)^{-1}(\boldsymbol{p})$ by $\mathcal{T}_{\boldsymbol{p}}$, and let $\Phi_{\boldsymbol{p}} : \mathcal{T}_{\boldsymbol{p}} \to \mathcal{P}^1 \setminus \Psi(\boldsymbol{p})$ be the composition of Φ with projection to $\mathcal{P}^1$. By construction it is clear that the covering $\Phi_{\boldsymbol{p}}$ represents the point $\boldsymbol{p}$ of $\mathcal{H}^{\rm ab}$. Thus we call $\Phi : \mathcal{T} \to \mathcal{M}$ the (partial) family of all covers parametrized by $\mathcal{H}^{\rm ab}$. We apply the attribute 'partial' because the fibers $\mathcal{T}_{\boldsymbol{p}}$ do not yield the full compact covers of $\mathcal{P}^1$ as discussed at the beginning of §4.

§**4.2. Uniqueness of the family:** Assume we have coverings $\Psi' : \mathcal{H}' \to \mathcal{U}_r$ and $\Phi' : \mathcal{T}' \to \mathcal{M}'$, where $\mathcal{M}' = \{(\boldsymbol{q}, z) \in \mathcal{H}' \times \mathcal{P}^1 : \ z \notin \Psi'(\boldsymbol{q}) \ \}$. Define the maps $F' : \mathcal{M}' \to \mathcal{U}$ and $P' : \mathcal{M}' \to \mathcal{H}'$ analogously as F and P, respectively. Assume further that for each $\boldsymbol{q} \in \mathcal{H}'$ the fiber $\mathcal{T}'_{\boldsymbol{q}} = (P' \circ \Phi')^{-1}(\boldsymbol{q})$ has the following property: The natural map $\mathcal{T}'_{\boldsymbol{q}} \to \mathcal{P}^1 \setminus \Psi'(\boldsymbol{q})$ is a cover that represents a point $\epsilon(\boldsymbol{q})$ of $\mathcal{H}^{\rm ab}$. Then $\epsilon : \mathcal{H}' \to \mathcal{H}^{\rm ab}$ is continuous.

To prove the above, note that $\Psi \circ \epsilon = \Psi'$ from the definitions. As Ψ' is a covering, any $\boldsymbol{q} \in \mathcal{H}'$ has a neighborhood $\mathcal{N}'$ such that Ψ' maps $\mathcal{N}'$ homeomorphically onto some $\mathcal{V}(D_1, \ldots, D_r)$ (where $D_1, \ldots, D_r$ are pairwise disjoint discs on $\mathcal{P}^1$ around the elements of $\Psi'(\boldsymbol{q})$). Then F' maps $\mathcal{M}'(\boldsymbol{q}; D_1, \ldots, D_r) \stackrel{\rm def}{=} (P')^{-1}(\mathcal{N}')$ homeomorphically onto $\{(\boldsymbol{a}, z) \in \mathcal{U} : \ \boldsymbol{a} \in \mathcal{V}(D_1, \ldots, D_r) \ \}$. Thus $\mathcal{M}'(\boldsymbol{q}; D_1, \ldots, D_r)$ contains $\mathcal{N}' \times \mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r)$ as a deformation retract. Since $\mathcal{N}'$ is contractible, all covers $\mathcal{T}'_{\boldsymbol{q}'} \to \mathcal{P}^1 \setminus \Psi'(\boldsymbol{q}')$ for $\boldsymbol{q}' \in \mathcal{N}'$ restrict, up to equivalence, to the same covering of $\mathcal{P}^1 \setminus (D_1 \cup \cdots \cup D_r)$. Thus $\epsilon(\mathcal{N}') = \mathcal{N}(\boldsymbol{p}; D_1, \ldots, D_r)$ for $\boldsymbol{p} = \epsilon(\boldsymbol{q})$. This shows that ϵ is continuous, even a local homeomorphism.

§**4.3. The ϵ_β are continuous:** As in §3 view $\Psi : \mathcal{H}^{\rm ab} \to \mathcal{U}_r$ as a morphism of algebraic varieties (defined over $\mathcal{C}$ is enough here). Then also $F : \mathcal{M} \to \mathcal{U}$ is such a morphism. Similarly, the unramified covering $\Phi : \mathcal{T} \to \mathcal{M}$ equips $\mathcal{T}$ with a unique variety structure defined over $\mathcal{C}$ such that Φ becomes an algebraic morphism.

Now consider some $\beta \in {\rm Aut}(\mathcal{C})$. It is clear that the maps $\Psi^\beta : (\mathcal{H}^{\rm ab})^\beta \to \mathcal{U}_r$ and $\Phi^\beta : \mathcal{T}^\beta \to \mathcal{M}^\beta$ are again coverings. They satisfy the conditions of §4.2 with $\epsilon = \epsilon_\beta$, and so ϵ_β is continuous. Thus we have verified the continuity assumption on the ϵ_β in the case that U is self-normalizing in G.

Remark: With some additional work it is possible to give a direct construction of the variety structure on $\mathcal{H}^{\rm ab}$, without appealing to the generalized Riemann existence theorem. Consider a point $|\varphi| \in \mathcal{H}^{\rm ab}$ such that the set $\boldsymbol{a}$ of branch points of φ is a generic point of $\mathcal{U}_r$ (over $\mathcal{Q}$). Define K as the minimal field of definition of φ. Then the $\mathcal{Q}$-irreducible component of $\mathcal{H}^{\rm ab}$ containing $|\varphi|$ can be identified with the normalization of the variety $\mathcal{U}_r$ in the extension field K of $\mathcal{Q}(\boldsymbol{a}) = \mathcal{Q}(\mathcal{U}_r)$. To set up this identification, one again needs the above family $\mathcal{T} \to \mathcal{M}$, whose respective $\mathcal{Q}$-component can be constructed in that approach as the normalization of the respective component of $\mathcal{M}$ in the field $K(X)$, where $\varphi : X \to \mathcal{P}^1$. This yields the desired variety structure defined over $\mathcal{Q}$ on the spaces $\mathcal{H}^{\rm ab}_r(G, U)$, where U is self-normalizing in G. Proceed as in §5 to transfer this variety structure to the spaces $\mathcal{H}^{\rm in}_r(G)$, and $\mathcal{H}^{\rm ab}_r(G, U)$ for U not self-normalizing. □

5. CONCLUSION OF THE PROOF OF THEOREM 1

Assume the hypotheses of Theorem 1 hold. From §3 it only remains to show that for each automorphism β of $\mathcal{C}$ the maps $\epsilon_\beta : (\mathcal{H}^{\rm ab})^\beta \to \mathcal{H}^{\rm ab}$ and $\epsilon'_\beta : (\mathcal{H}^{\rm in})^\beta \to \mathcal{H}^{\rm in}$ are continuous.

§**5.1. Some reductions:** Here we make use of the covering $\Lambda : \mathcal{H}^{\rm in} \to \mathcal{H}^{\rm ab}$ with $\Psi' = \Psi \circ \Lambda$. As noted in §3, we may view Λ as an algebraic morphism (defined over $\mathcal{C}$ is enough here). Let $\beta \in {\rm Aut}(\mathcal{C})$. It is immediate from the definition of Λ in §1.2 that

$$\epsilon_\beta \circ \Lambda^\beta = \Lambda \circ \epsilon'_\beta.$$

This implies:

(5.1) If ϵ'_β is continuous, then also ϵ_β is continuous.

(5.2) Under the hypothesis ${\rm Aut}(G,U) = {\rm Inn}(G)$, the map ϵ_β is continuous if and only if ϵ'_β is continuous.

Note that if ${\rm Aut}(G,U) = {\rm Inn}(G)$ then $\mathcal{E}_r^{\rm ab}(G,U) = \mathcal{E}_r^{\rm in}(G)$ (§1.1); hence the coverings $\Psi : \mathcal{H}_r^{\rm ab}(G,U) \to \mathcal{U}_r$ and $\Psi' : \mathcal{H}_r^{\rm in}(G) \to \mathcal{U}_r$ are equivalent (§1.3), and therefore Λ is an isomorphism. This proves (5.2).

Combining (5.2) and §4.3 we get:

(5.3) If U is self-normalizing in G and ${\rm Aut}(G,U) = {\rm Inn}(G)$, then ϵ'_β is continuous.

§**5.2. The ϵ'_β are continuous:** By (5.1) it only remains to show that the ϵ'_β are continuous. We will reduce this to the special case of (5.3), by constructing a finite group $\tilde{G}$ that satisfies the hypothesis of (5.3) and maps surjectively to G. First we need to study how the spaces $\mathcal{H}^{\rm in}$ behave under surjections $\lambda : \tilde{G} \to G$ of finite groups.

Let N be the kernel of λ. Define a map Ω from $\mathcal{H}_r^{\rm in}(\tilde{G})$ to the disjoint union $\bigcup_{s=2}^r \mathcal{H}_s^{\rm in}(G)$ as follows: Suppose that we are given $|\tilde{\chi}, \tilde{h}|$ in $\mathcal{H}_r^{\rm in}(\tilde{G})$, where $\tilde{\chi} : \tilde{X} \to \mathcal{P}^1$ and $\tilde{h} : {\rm Aut}(\tilde{X}/\mathcal{P}^1) \to \tilde{G}$ is an isomorphism. Let $\chi : \hat{X} \stackrel{\rm def}{=} \tilde{X}/\tilde{h}^{-1}(N) \to \mathcal{P}^1$ be the induced cover and let $h : {\rm Aut}(\hat{X}/\mathcal{P}^1) \to G$ be the isomorphism making the following diagram commute (the left vertical arrow is the canonical map):

$$\begin{array}{ccc} {\rm Aut}(\tilde{X}/\mathcal{P}^1) & \stackrel{\tilde{h}}{\longrightarrow} & \tilde{G} \\ \downarrow & & \downarrow \\ {\rm Aut}(\hat{X}/\mathcal{P}^1) & \stackrel{h}{\longrightarrow} & G \end{array}$$

Then Ω maps $|\tilde{\chi}, \tilde{h}|$ to $|\chi, h|$.

Equip $\bigcup_{s=2}^r \mathcal{H}_s^{\rm in}(G)$ with the topology of a disjoint union of open (and closed) spaces. Then Ω is continuous (easy to check from the set-up of §1.2). Further, the number of branch points of $\Omega(\boldsymbol{p})$ is locally constant for $\boldsymbol{p} \in \mathcal{H}_r^{\rm in}(\tilde{G})$. Thus $\tilde{\mathcal{H}} = \Omega^{-1}(\mathcal{H}_r^{\rm in}(G))$ is a union of connected components of $\mathcal{H}_r^{\rm in}(\tilde{G})$. (It could be empty.) Now assume $\tilde{G}$ can be generated by $r-1$ elements. Then a theorem of Gaschütz implies that for each $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r(G)$ there exists $(\tau_1, \ldots, \tau_r) \in \mathcal{E}_r(\tilde{G})$ with $\lambda(\tau_i) = \sigma_i$ for all i (e.g., [FrJ, Lemma 15.30]). Since $\pi_1(\mathcal{P}^1 \setminus \boldsymbol{a}, a_0)$ is free of rank $r-1$ (where $\boldsymbol{a} = \{a_1, \ldots, a_r\}$ as in §1.2), Ω maps $\tilde{\mathcal{H}}$ surjectively to $\mathcal{H}_r^{\rm in}(G)$. From now on $\Omega : \tilde{\mathcal{H}} \to \mathcal{H}_r^{\rm in}(G)$ denotes the restriction of the above map to $\tilde{\mathcal{H}}$.

We have $\Psi' \circ \Omega = \tilde{\Psi}$, where $\tilde{\Psi} : \tilde{\mathcal{H}} \to \mathcal{U}_r$ is the natural covering that sends $|\tilde{\chi}, \tilde{h}|$ to the set of branch points of $\tilde{\chi}$. Therefore, Ω is a covering since it is continuous. Again it follows that Ω is an algebraic morphism (defined over $\mathcal{C}$).

Now consider $\beta \in {\rm Aut}(\mathcal{C})$. With $\tilde{\epsilon}_\beta : (\tilde{\mathcal{H}})^\beta \to \tilde{\mathcal{H}}$ defined analogously to ϵ'_β, one checks easily that

$$\Omega \circ \tilde{\epsilon}_\beta = \epsilon'_\beta \circ \Omega^\beta$$

Thus if $\tilde{\epsilon}_\beta$ is continuous, then also ϵ'_β is continuous. Now choose $\tilde{G}$ as in Lemma 3 below. Then $\tilde{G}$ satisfies the hypothesis of (5.3), hence $\tilde{\epsilon}_\beta$ is continuous. Thus also ϵ'_β is continuous, and the proof of Theorem 1 is complete.

§**5.3. Another group-theoretic Lemma:**

Lemma 3: *Each finite group that can be generated by $r-1$ elements ($r \geq 3$) is the quotient of a finite group $\tilde{G}$ that can be generated by $r-1$ elements and has a subgroup $\tilde{U}$ with the following properties:*

(i) $\tilde{U}$ contains no non-trivial normal subgroup of $\tilde{G}$.
(ii) $\tilde{U}$ is self-normalizing in $\tilde{G}$.
(iii) $Aut(\tilde{G}, \tilde{U}) = Inn(\tilde{G})$.

Proof: Suppose G is a finite group generated by $g_1, \ldots, g_n$, where $n = r-1 \geq 2$.

Part 1: *Reduction to the case that G has trivial center.* We need only present G as quotient of a finite group H with trivial center that can also be generated by n elements. This is quite elementary, but we give the argument for completeness. Let p be a prime not dividing the order of G. We may assume that the center of G has a non-trivial element g. Then g acts non-trivially on the regular $\mathcal{F}_p$ module M of G (the group ring over $\mathcal{F}_p$). The module M is completely reducible by Maschke's theorem. Thus there is an irreducible summand V of M on which g acts non-trivially.

Now consider the semi-direct product H of G and V. Let $q = |V|$. There are q^n tuples $(h_1, \ldots, h_n)$ in H^n with $h_i \mapsto g_i$ for $i = 1, \ldots, n$. Since V is irreducible, the group $< h_1, \ldots, h_n >$ is either all of H, or it is a complement to V in H. These complements are all conjugate under V (Schur-Zassenhaus theorem), hence their number is at most q. And in each such complement there is a unique lift of the g_i's. Since $n \geq 2$, conclude there is a lift $(h_1, \ldots, h_n)$ with $H =< h_1, \ldots, h_n >$. The center of H maps injectively into the center of G, but its image does not contain g. Hence H has a center of strictly smaller order than G. By induction, this completes the argument.

Part 2: *Construction of $\tilde{G}$.* From now on assume G has trivial center. Let S be a non-abelian finite simple group with $\mathrm{Aut}(S) = \mathrm{Inn}(S)$, generated by two elements a, b, and such that S has a collection of pairwise non-conjugate, self-normalizing proper subgroups U_g indexed by the elements g of G. For example, take S to be the symplectic group $\mathrm{Sp}_{2m}(2)$ for large enough m, whereby the U_g's can be taken as distinct parabolics containing a common Borel subgroup [Ca; Chapter 11].

Define $\tilde{G}$ to be the semi-direct product $\tilde{G} = A \times^s G$ where A is the group of all (not necessarily homomorphic) functions $\alpha : G \to S$ (with pointwise multiplication) and G acts on A by translation of functions:

$$^g\alpha(h) = \alpha(hg) \quad \text{for} \quad g, h \in G.$$

Clearly $A \cong S^m$, the direct product of $m = |G|$ copies of S, and G permutes these factors sharply transitively ($\tilde{G}$ is the wreath product of G and S). Further, A is minimal normal in $\tilde{G}$, and the centralizer of A in $\tilde{G}$ is trivial. Since distinct minimal normal subgroups centralize each other, A is the unique minimal normal in $\tilde{G}$.

Part 3: *Conditions (i)-(iii) hold.* We define $\tilde{U}$ as the group of all $\alpha \in A$ with $\alpha(g) \in U_g$ for all $g \in G$. As S is simple, condition (i) holds. Since $\tilde{G}$ has trivial center, we can identify $\tilde{G}$ with $\mathrm{Inn}(\tilde{G}) \leq \mathrm{Aut}(\tilde{G})$. We are going to show that $\tilde{U}$ is self-normalizing in $\mathrm{Aut}(\tilde{G})$, which proves (ii) and (iii).

Let h be an element of the normalizer of $\tilde{U}$ in $\mathrm{Aut}(\tilde{G})$. Since A is the unique minimal normal subgroup of $\tilde{G}$, the element h fixes A. Recall that the U_g are pairwise non-conjugate and self-normalizing in $S \cong \mathrm{Aut}(S)$. From this it follows that h fixes all the simple factors of A, and it acts on A as some element of $\tilde{U}$. Thus we may assume that h centralizes A. But the centralizer C of A in $\mathrm{Aut}(\tilde{G})$ is normal in $\mathrm{Aut}(\tilde{G})$, and $C \cap \tilde{G} = 1$; hence C centralizes $\tilde{G}$, and so $C = 1$. Thus $h = 1$, and we have proved that $\tilde{U}$ is self-normalizing in $\mathrm{Aut}(\tilde{G})$.

Part 4: *$\tilde{G}$ can be generated by n elements.* For $i = 1, \ldots, n$ define $\alpha_i \in A$ by:

$$\alpha_i(1) = a \quad \text{if} \quad i = 1, \qquad \alpha_i(1) = b \quad \text{if} \quad i > 1$$
$$\alpha_i(g) = 1 \quad \text{for} \quad g \neq 1.$$

Denote (α_i, g_i) by $\tilde{g}_i$, and let H be the subgroup of $\tilde{G}$ generated by these elements. We are going to show that $\tilde{G} = H =< \tilde{g}_1, \ldots, \tilde{g}_n >$. It suffices to show that $A \leq H$. Set $B = A \cap H$.

For each i, let e_i be the order of g_i. Then $\beta_i \stackrel{\text{def}}{=} \tilde{g}_i^{e_i} \in B$, and we have for any $g \in G$:

$$\beta_i(g) = \alpha_i(g)\alpha_i(gg_i)\cdots\alpha_i(gg_i^{e_i-1}).$$

This equals a for $i = 1$ and $g \in < g_i >$; b for $i > 1$ and $g \in < g_i >$; and 1 if $g \notin < g_i >$.

We know there exist elements $\beta \in B$ with $\beta(1) \neq 1$. Among these elements, choose one with the property the set $M = \{g \in G | \beta(g) \neq 1\}$ has minimal cardinality. Set $c = \beta(1)$; then $c \neq 1$. Since $S =< a, b >$ we may conjugate β with products of the β_i's to assume that neither of the commutators $[a, c]$ and $[b, c]$ is trivial. Then the function $\beta_i' = [\beta, \beta_i]$ has $\beta_i'(1) \neq 1$, and vanishes outside M. By the minimality of M it follows that $\beta_i'(m) \neq 1$ for all $m \in M$. But, β_i, and therefore also β_i', vanishes outside $< g_i >$. Thus $M \subset < g_i >$ for $i = 1, \ldots, n$. Hence M centralizes all g_i, and therefore lies in the center of G. Thus $M = \{1\}$.

We have found $\beta \neq 1$ in B with $\beta(g) = 1$ for all $g \neq 1$. Since $S =< a, b >$ it is clear that the conjugates of β by products of the β_i's generate the full group $\{\alpha \in A : \alpha(g) = 1 \text{ for all } g \neq 1\}$. Thus this group lies in B. Clearly, the H-conjugates of this group generate A, which proves $A \leq H$, as claimed. This completes the proof of the Lemma. □

6. A RESULT FOR LATER USE

The goal of this section is to prove Proposition 3 below. This Proposition is crucial in the paper [FrVo]. Let G be a finite group with trivial center, satisfying the *Schur multiplier condition* (*) from §2.2. Take $U = \{1\}$. All the notation such as $\mathcal{H}^{\text{ab}} = \mathcal{H}_r^{\text{ab}}(G, U)$, $\mathcal{E}_r^{\text{ab}}$, $\text{Ni}(\mathbf{C})^{\text{ab}}$, $\mathcal{H}(\mathbf{C})^{\text{ab}}$ etc. from §1 refers now to this special case $U = \{1\}$. As usual, $r \geq 3$ is a fixed integer (to be specified later), and $\mathcal{H}^{\text{in}} = \mathcal{H}_r^{\text{in}}(G)$.

§6.1. The automorphisms δ_A of $\mathcal{H}^{\text{in}}$ over $\mathcal{H}^{\text{ab}}$: This subsection refers only to the (complex) topology of our moduli spaces. Recall that $\mathcal{H}^{\text{ab}} = \mathcal{H}_r^{\text{ab}}(G, \{1\})$ is the space of equivalence classes of Galois covers $\chi : X \to \mathcal{P}^1$ with r branch points and with $\text{Aut}(X/\mathcal{P}^1) \cong G$; and $\Lambda : \mathcal{H}^{\text{in}} \to \mathcal{H}^{\text{ab}}$ is the map sending the class of the pair (χ, h) to the class of χ. Thus on the fibers over the base point $\boldsymbol{b} \in \mathcal{U}_r$, the covering Λ induces the canonical map $\mathcal{E}_r^{\text{in}} \to \mathcal{E}_r^{\text{ab}}$ sending the class of $(\sigma_1, \ldots, \sigma_r)$ modulo $\text{Inn}(G)$ to its class modulo $\text{Aut}(G)$ (via the identifications of §1.3). It follows that the covering $\Lambda : \mathcal{H}^{\text{in}} \to \mathcal{H}^{\text{ab}}$ has degree $|\text{Out}(G)|$ (where $\text{Out}(G) = \text{Aut}(G)/\text{ Inn}(G)$).

Indeed, the group $\mathrm{Out}(G)$ acts faithfully as a group of automorphisms of the covering Λ: For $A \in \mathrm{Aut}(G)$, let $\delta_A : \mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{in}}$ be the map sending $|\chi, h|$ to $|\chi, Ah|$. One checks that δ_A is well-defined and continuous. Clearly $\Lambda \circ \delta_A = \Lambda$. Thus δ_A is an automorphism of the cover Λ. Further, δ_A depends only on the class of A modulo $\mathrm{Inn}(G)$. Hence the δ_A yield the desired action of $\mathrm{Out}(G)$.

Let c be the number of conjugacy classes $\neq \{1\}$ of G. Suppose that $r = cs$, and that $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_r)$ is an r-tuple containing each conjugacy class $\neq \{1\}$ of G exactly s times. Since $\mathrm{Aut}(G)$ permutes $\mathrm{C}_1, \ldots, \mathrm{C}_r$, it follows that $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ is the full inverse image of $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$ under the canonical map $\mathcal{E}_r^{\mathrm{in}} \to \mathcal{E}_r^{\mathrm{ab}}$ (see §1.1). This implies that the Hurwitz space $\mathcal{H}' = \mathcal{H}(\mathbf{C})^{\mathrm{in}}$ is the full inverse image of $\mathcal{H} = \mathcal{H}(\mathbf{C})^{\mathrm{ab}}$ under Λ (c.f. §1.3). Thus Λ restricts to a covering $\Lambda' : \mathcal{H}' \to \mathcal{H}$ of degree $|\mathrm{Out}(G)|$, and the group $\mathrm{Out}(G)$ also acts faithfully as a group of automorphisms of this covering. Conclude that if $\mathcal{H}'$ and $\mathcal{H}$ are connected then Λ' is a Galois covering, and the automorphism group of this covering is isomorphic to $\mathrm{Out}(G)$, via the map $A \mapsto \delta_A$. From now on, δ_A denotes the restriction of the original map to $\mathcal{H}'$.

§6.2. Choosing suitable Hurwitz spaces: By §2.2 we can choose $r = cs$ for suitably large s so that each (rational) r-tuple $\mathbf{C}$ as in the preceding paragraph has the following property: $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ is non-empty and the Hurwitz group H_r acts transitively on this set. Then the Hurwitz spaces $\mathcal{H}' = \mathcal{H}(\mathbf{C})^{\mathrm{in}}$ and $\mathcal{H} = \mathcal{H}(\mathbf{C})^{\mathrm{ab}}$ are absolutely irreducible varieties defined over $\mathcal{Q}$, and the covering $\Lambda' : \mathcal{H}' \to \mathcal{H}$ is a morphism defined over $\mathcal{Q}$ (by Theorem 1). All complex-analytic automorphisms δ_A of Λ' are algebraic and defined over $\bar{\mathcal{Q}}$. Indeed, they are even defined over $\mathcal{Q}$: Namely, for all $\beta \in G_{\mathcal{Q}}$ and $|\chi, h| \in \mathcal{H}'$ we have

$$(\delta_A)^\beta(|\chi, h|^\beta) = (\delta_A(|\chi, h|))^\beta = |\chi, A \circ h|^\beta = \\ |\chi^\beta, A \circ h \circ \beta^{-1}| = \delta_A(|\chi^\beta, h \circ \beta^{-1}|) = \delta_A(|\chi, h|^\beta).$$

It follows that if $\boldsymbol{p}$ is a point of $\mathcal{H}$, rational over some field k, and $\boldsymbol{p}'$ is a point of $\mathcal{H}'$ with $\Lambda'(\boldsymbol{p}') = \boldsymbol{p}$, then the field $k' = k(\boldsymbol{p}')$ is Galois over k.

§6.3. The main result of §6: Fix a point $\boldsymbol{p}' = |\chi, h|$ of $\mathcal{H}'$, where $\chi : X \to \mathcal{P}^1$ and $h : \mathrm{Aut}(X/\mathcal{P}^1) \to G$ as usual. Let $\boldsymbol{p} = \Lambda(\boldsymbol{p}') = |\chi|$ be its image in $\mathcal{H}^{\mathrm{ab}}$, and let k be a field containing $\mathcal{Q}(\boldsymbol{p})$. By Corollary 1 the (Galois) cover χ can be defined over $k' = k(\boldsymbol{p}')$ so that all its automorphisms are defined over k', and k' is the minimal extension of k with this property. The resulting function field $L = k'(X)$ is Galois over $k'(x) = k'(\mathcal{P}^1)$, and the group $G_0 \stackrel{\mathrm{def}}{=} G(L/k'(x))$ is isomorphic to G, via the isomorphism h_0 which is the composition of the canonical isomorphism $G_0 \to \mathrm{Aut}(X/\mathcal{P}^1)$ with h. We claim that L is even Galois over $k(x)$.

Indeed, the cover χ can be defined over k by Corollary 1. Let M denote the corresponding k-form of the field $\bar{L} = \bar{k}(X)$. (The field M is not necessarily contained in $L = k'(X)$, thus we do *not* write $M = k(X)$). The field $\bar{L}$ is Galois over $k(x)$, since $k(x)$ is the fixed field of the group of automorphisms of $\bar{L}$ generated by $G(\bar{L}/M)$ and $G(\bar{L}/\bar{k}(x))$. Since $L \cap \bar{k}(x) = k'(x)$, elementary Galois theory implies that $G(\bar{L}/k'(x))$ is the direct product of $G(\bar{L}/\bar{k}(x)) \cong G$ and $G(\bar{L}/L)$. Therefore, as G has trivial center, $G(\bar{L}/L)$ is the centralizer of $N_1 = G(\bar{L}/\bar{k}(x))$ in $N_2 = G(\bar{L}/k'(x))$. From §6.2, k' is Galois over k and so both N_1 and N_2 are normal in $G(\bar{L}/k(x))$. It follows that $G(\bar{L}/L)$ is normal in $G(\bar{L}/k(x))$. Thus L is Galois over $k(x)$, as claimed.

Set $\Omega = G(L/k(x))$. Let C be the centralizer of $G_0 = G(L/k'(x))$ in Ω. Then C is normal in Ω, and $C \cap G_0 = 1$ (since G has trivial center). Let L'' be the fixed field of C in L; then $k'(x) \cap L'' = k''(x)$ for some field k'' between k and k'. It follows that L'' is a k''-form of $\bar{L}$ that is Galois over $k''(x)$. Thus the cover χ together with all its automorphisms can be defined over k'', and so $k'' = k'$ (by minimality of k'). This means $L'' = L$, hence $C = 1$. Thus we have proved that the centralizer of G_0 in Ω is trivial. Hence Ω embeds into $\mathrm{Aut}(G_0)$ (via conjugation action). Thus the above isomorphism $h_0 : G_0 \to G$ induces an injection $h_1 : \Omega \to \mathrm{Aut}(G)$. The remaining task is to identify the image of Ω in $\mathrm{Aut}(G)$.

Proposition 3: *Let G be a finite group with trivial center such that the Schur multiplier of G is generated by commutators (condition (*)). Then the unramified Galois covering $\Lambda' : \mathcal{H}' \to \mathcal{H}$ constructed above is a morphism of absolutely irreducible varieties defined over $\mathcal{Q}$, and all automorphisms of this covering are defined over $\mathcal{Q}$. The group $Out(G)$ acts faithfully on $\mathcal{H}'$, inducing the full automorphism group of the covering Λ'; for each $A \in Aut(G)$, let δ_A denote the automorphism of $\mathcal{H}'$ induced by the image of A in $Out(G)$. Then for each point $\boldsymbol{p} \in \mathcal{H}$, rational over some field k, and for each point $\boldsymbol{p}' \in \mathcal{H}'$ with $\Lambda'(\boldsymbol{p}') = \boldsymbol{p}$, there is a Galois extension $L/k'(x)$, regular over $k' = k(\boldsymbol{p}')$, such that the following holds:*

L is Galois over $k(x)$, and there is an isomorphism h_1 from $G(L/k(x))$ onto the group Δ of those $A \in Aut(G)$ for which $\delta_A(\boldsymbol{p}')$ is conjugate to $\boldsymbol{p}'$ under $G(k'/k)$. Furthermore, h_1 restricts to an isomorphism between $G(L/k'(x))$ and $Inn(G)$.

Proof: It only remains to show that $h_1(\Omega) = \Delta$ where $h_1 : \Omega \to \mathrm{Aut}(G)$ is as defined above. Indeed, it suffices to show that $h_1(\Omega) \subset \Delta$ because:

$$|h_1(\Omega)| = |\Omega| = |G_0| \cdot |G(k'(x)/k(x))| = |G| \cdot [k' : k] = |\Delta|$$

Since G has trivial center, we can (and will) identify G with the subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$; similarly for G_0 and for $\bar{G} \stackrel{\text{def}}{=} G(\bar{L}/\bar{k}(x))$. The map $h_0 : G_0 \to G$ extends naturally to an isomorphism $\mathrm{Aut}(G_0) \to \mathrm{Aut}(G)$, which we again denote by h_0. The restriction map $\bar{G} \to G_0$ is an isomorphism; let $R : \mathrm{Aut}(\bar{G}) \to \mathrm{Aut}(G_0)$ be its natural extension. Define the isomorphism $\bar{h} : \mathrm{Aut}(\bar{G}) \to \mathrm{Aut}(G)$ by $\bar{h} = h_0 \circ R$. Clearly, the image $\bar{\Omega}$ of $G(\bar{L}/k(x))$ in $\mathrm{Aut}(\bar{G})$ (via conjugation action) corresponds under R to the image of $\Omega = G(L/k(x))$ in $\mathrm{Aut}(G_0)$. Thus $h_1(\Omega) = h_0 R(\bar{\Omega}) = \bar{h}(\bar{\Omega})$. From the previous paragraph, it remains to show that $\bar{h}(\bar{\Omega}) \subset \Delta$.

From the definitions, $\bar{h}$ is induced from the map $\bar{G} \to G$ that is the composition of the canonical isomorphism $\bar{G} \to \mathrm{Aut}(X/\mathcal{P}^1)$ with h. Thereby, this canonical isomorphism is explicitly given as follows: It sends B^* to B, where B is any element of $\mathrm{Aut}(X/\mathcal{P}^1)$ and $B^* \in \bar{G} = G(\bar{L}/\bar{k}(x))$ is defined by $B^*(f) = f \circ B^{-1}$ (pulling back of functions), for $f \in \bar{L} = \bar{k}(X)$. Therefore:

(7) $\bar{h}(B^*) = h(B)$ for all $B \in \mathrm{Aut}(X/\mathcal{P}^1)$.

Now let $\bar{\alpha}$ be an element of $\bar{\Omega}$, and let $\alpha \in G(\bar{L}/k(x))$ be a pre-image of $\bar{\alpha}$. Let $\beta \in G(\bar{k}/k)$ be the image of α^{-1} under $G(\bar{L}/k(x)) \to G(\bar{k}(x)/k(x)) \cong G(\bar{k}/k)$ (where the first map is restriction). We claim that the element $A = \bar{h}(\bar{\alpha})$ of $\mathrm{Aut}(G)$ satisfies

$$\delta_A(\boldsymbol{p}') = (\boldsymbol{p}')^{\beta}. \tag{8}$$

This means that $A = \bar{h}(\bar{\alpha})$ lies in Δ, and $\bar{h}(\bar{\Omega}) \subset \Delta$ as desired. Thus it only remains to prove (8).

By Corollary 1(a) the cover $\chi : X \to \mathcal{P}^1$ can be defined over k. This is compatible with the $\bar{k}$-structure, but not necessarily with the k'-structure on X considered above. However, the remainder of the proof does not refer to this k'-structure anymore, so we assume now that X and χ are defined over k. This yields an action of $G(\bar{k}/k)$ on $\bar{L} = \bar{k}(X)$, denoted $f \mapsto f^{\sigma}$ ($f \in \bar{L}$, $\sigma \in G(\bar{k}/k)$). The map $f \mapsto f^{\sigma}$ acts on the subfield $\bar{k}(x)$ in the natural way (i.e., through the canonical isomorphism $G(\bar{k}(x)/k(x)) \to G(\bar{k}/k)$), since χ is defined over k. Thus the map $f \mapsto f^{\beta}$ and the map $\alpha^{-1} \in G(\bar{L}/k(x))$ restrict to the same element of $G(\bar{k}(x)/k(x))$, and so there is some $D \in G(\bar{L}/\bar{k}(x)) = \bar{G}$ with $f^{\beta} = D\alpha^{-1}(f)$ for all $f \in \bar{L}$. Replacing α by αD^{-1} changes $A = \bar{h}(\bar{\alpha})$ only by the inner automorphism $\bar{h}(D^{-1})$ of G, and the map δ_A remains unchanged. Thus we may assume $D = 1$, so that $f^{\beta} = \alpha^{-1}(f)$ for all $f \in \bar{L}$. Then we have for all $B \in \mathrm{Aut}(X/\mathcal{P}^1)$, $f \in \bar{L}$:

$$(B^{\beta^{-1}})^*(f) = f \circ (B^{-1})^{\beta^{-1}} = [f^{\beta} \circ B^{-1}]^{\beta^{-1}} = \alpha B^* \alpha^{-1}(f) = \bar{\alpha}(B^*)(f)$$

hence

$$(B^{\beta^{-1}})^* = \bar{\alpha}(B^*) \tag{9}$$

Finally, Theorem 1 gives $(\boldsymbol{p}')^{\beta} = |\chi, h|^{\beta} = |\chi^{\beta}, h \circ \beta^{-1}| = |\chi, h \circ \beta^{-1}|$, where $h \circ \beta^{-1} : \mathrm{Aut}(X/\mathcal{P}^1) \to G$ is the isomorphism sending B to $h(B^{\beta^{-1}})$. By (7) and (9) we have

$$h(B^{\beta^{-1}}) = \bar{h}((B^{\beta^{-1}})^*) = \bar{h}(\bar{\alpha}(B^*)) = \bar{h}(\bar{\alpha})(\bar{h}(B^*)) = \bar{h}(\bar{\alpha})(h(B)) = A \circ h(B)$$

Thus $(\boldsymbol{p}')^{\beta} = |\chi, A \circ h| = \delta_A(\boldsymbol{p}')$, which proves (8). This completes the proof of Proposition 3.

APPENDIX

This is a slightly modified exposition on a result of Conway and Parker [CP]. We only consider the case that the union S of conjugacy classes of G that occurs in [CP] is all of $G \setminus \{1\}$, and that $M(G)$ is generated by commutators. This is what is needed above. The restriction to this special case allows for some simplifications. Further, we correct some errors from [CP].

A. Introduction: Let G be a finite group, and let $r \geq 3$ be an integer. For $i = 1, \ldots, r-1$ let $Q_i : G^r \to G^r$ be given by expression (2) of §1.3.

The *Hurwitz class* of $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r) \in G^r$ is defined to be the orbit of $\boldsymbol{\sigma}$ under the group generated by $Q_1, ..., Q_{r-1}$. Clearly, the evaluation function $E(\boldsymbol{\sigma}) = \sigma_1 \cdots \sigma_r$ is constant on Hurwitz classes. The same is true for the *shape function* $S(\boldsymbol{\sigma}) = (n_C(\boldsymbol{\sigma}))_{\mathrm{C}}$, which maps $\boldsymbol{\sigma}$ to the *shape vector* containing the numbers $n_C(\boldsymbol{\sigma}) = \#\{i : \sigma_i \in \mathrm{C}\}$, where C runs through the set of conjugacy classes of G. In certain cases, these functions form a complete set of invariants for the Hurwitz classes:

Theorem (Conway-Parker): *Suppose the Schur multiplier $M(G)$ is generated by commutators (as defined in §2.4). Then there exists an integer N with the following property: If $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_r) \in G^r$ satisfies $n_C(\boldsymbol{\sigma}) \geq N$ for all conjugacy classes $\mathrm{C} \neq \{1\}$ of G, then the Hurwitz class of $\boldsymbol{\sigma}$ consists of all $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_r) \in G^r$ with $\tau_1 \cdots \tau_r = \sigma_1 \cdots \sigma_r$ and $S(\boldsymbol{\tau}) = S(\boldsymbol{\sigma})$.*

In the remainder of this Appendix we give a proof of this theorem, adapted from [CP].

B. Central Extensions: Let $\varphi : \hat{G} \to G$ be a central extension (of groups), such that $\hat{G}$ is generated by elements $\hat{a}$ ($a \in G$) with $\varphi(\hat{a}) = a$. Use the notation $a^b = b^{-1}ab$. We assume that the following relations hold:

$$(I) \qquad \hat{a}\hat{b} = \hat{b}\widehat{a^b}$$

Proposition: *Suppose $M(G)$ is generated by commutators. If $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_r)$, $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_r) \in G^r$ satisfy $\sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_r$ and $S(\boldsymbol{\sigma}) = S(\boldsymbol{\tau})$, then $\hat{\sigma}_1 \cdots \hat{\sigma}_r = \hat{\tau}_1 \cdots \hat{\tau}_r$.*

Proof: Let $\mathcal{F}$ be the free group on generators $\bar{a}$ ($a \in G$), let $\mathcal{R}$ be the kernel of the homomorphism $\mathcal{F} \to G$ sending $\bar{a}$ to a, and let $\psi : \mathcal{F} \to \hat{G}$ be the homomorphism sending $\bar{a}$ to $\hat{a}$. We prove:

$$(II) \qquad \psi(\mathcal{R} \cap [\mathcal{F}, \mathcal{F}]) = 1$$

Since $\psi(\mathcal{R}) \leq \ker(\varphi) \leq Z(\hat{G})$, the center of $\hat{G}$, clearly $\psi([\mathcal{R}, \mathcal{F}]) = 1$. By the general theory of the Schur multiplier (e.g., [Hu; p. 631]) the quotient of $\mathcal{R} \cap [\mathcal{F}, \mathcal{F}]$ by $[\mathcal{R}, \mathcal{F}]$ is isomorphic to the Schur multiplier $M(G)$. The hypothesis that $M(G)$ is generated by commutators means that the group $\mathcal{R} \cap [\mathcal{F}, \mathcal{F}]$ is generated modulo $[\mathcal{R}, \mathcal{F}]$ by commutators $z = [x, y]$, $x, y \in \mathcal{F}$. Since $a = \varphi \circ \psi(x)$ and $b = \varphi \circ \psi(y)$ commute in G, the relations (I) imply that $\hat{a}$ and $\hat{b}$ commute in $\hat{G}$. Since $\psi(x) \in \hat{a}Z(\hat{G})$ and $\psi(y) \in \hat{b}Z(\hat{G})$, we get $\psi(z) = [\psi(x), \psi(y)] = [\hat{a}, \hat{b}] = 1$. This proves (II).

¿From (II) the map $\psi : \mathcal{F} \to \hat{G}$ induces $\bar{\psi} : \bar{\mathcal{F}} \to \hat{G}$, where $\bar{\mathcal{F}} = \mathcal{F}/(\mathcal{R} \cap [\mathcal{F}, \mathcal{F}])$. Clearly $\bar{\mathcal{R}} \cap [\bar{\mathcal{F}}, \bar{\mathcal{F}}] = 1$, where $\bar{\mathcal{R}}$ is the image of $\mathcal{R}$ in $\bar{\mathcal{F}}$. The kernel of $\bar{\psi}$ lies in $\bar{\mathcal{R}}$, hence $\bar{\psi}(\bar{\mathcal{R}}) \cap [\hat{G}, \hat{G}] = 1$. Let A be the abelian group $\hat{G}/[\hat{G}, \hat{G}]$. Since $\bar{\psi}(\bar{\mathcal{R}}) = \ker(\varphi)$, it follows that $\hat{G}$ embeds as a subgroup of $G \times A$, via the map that sends $g \in \hat{G}$ to $(\varphi(g), g[\hat{G}, \hat{G}])$.

Viewing $\hat{G}$ as a subgroup of $G \times A$ via this embedding, we have $\hat{a} = (a, t_a)$ for each $a \in G$, where $t_a \in A$. The relations (I) yield $t_a = t_{a^b}$ for all $a, b \in G$. Thus t_a depends only on the conjugacy class of a. Now the Proposition follows:

$$\prod \hat{\sigma}_i = \prod (\sigma_i, t_{\sigma_i}) = (\prod \sigma_i, \prod t_{\sigma_i}) = (\prod \tau_i, \prod t_{\tau_i}) = \prod \hat{\tau}_i. \qquad \square$$

The final section produces an equivalence relation on the semigroup of Hurwitz classes of arrays of elements of G. The quotient by this equivalence relation turns out to be a group $\hat{G}$, satisfying the hypotheses of the Proposition.

C. Congruence Classes of Words: Consider the semi-group of words in the symbols $\tilde{a}$ ($a \in G\backslash\{1\}$), under concatenation. Define the Hurwitz class $H(w)$ of a word $w = \tilde{a}_1 \cdots \tilde{a}_r$ to be the set of all words that can be obtained from w by iteration of the operations Q_i given by expression (2) of §1.3 (where we now write $\tilde{a}_1 \cdots \tilde{a}_r$ instead of $(a_1, \ldots, a_r)$). By abuse of notation, we will denote the Hurwitz class $H(\tilde{a}) = \{\tilde{a}\}$ again by $\tilde{a}$. Denote the set of Hurwitz classes by $\mathcal{H} = \mathcal{H}(G)$. The multiplication $H(w_1)H(w_2) = H(w_1 w_2)$ is well-defined and makes $\mathcal{H}$ into a semi-group, generated by the elements $\tilde{a}$ ($a \in G \setminus \{1\}$). They satisfy the relations

$$(I') \qquad \tilde{a}\tilde{b} = \tilde{b}\widetilde{a^b}$$

We fix the notation $A = \tilde{a}_1 \cdots \tilde{a}_r,\ B = \tilde{b}_1 \cdots \tilde{b}_s$ for general elements of $\mathcal{H}$. As in the Introduction, we have the evaluation function $E(A) = a_1 \cdots a_r$ and the shape function $S(A)$ on Hurwitz classes; both are semi-group homomorphisms.

Lemma 1: *If $E(A) = 1$ then $A \in Z(\mathcal{H})$.*

Proof: For $b \in G$ we have $\tilde{b}A = \tilde{b}\tilde{a}_1 \cdots \tilde{a}_r = \tilde{a}_1 \widetilde{b^{a_1}} \tilde{a}_2 \cdots \tilde{a}_r = \tilde{a}_1\tilde{a}_2\widetilde{b^{a_1 a_2}}\tilde{a}_3 \cdots \tilde{a}_r = \cdots = A\widetilde{b^{a_1 a_2 \cdots a_r}} = A\tilde{b}$. Since $\mathcal{H}$ is generated by the $\tilde{b}$, the claim follows. □

Let $o(a)$ denote the order of an element $a \in G$. Set

$$U = \prod_{a \in G\backslash\{1\}} \tilde{a}^{o(a)}$$

The factors in this product are in the center of $\mathcal{H}$ by Lemma 1. Therefore the ordering in the product does not matter. Then also U lies in the center of $\mathcal{H}$, and for any $b \in G\backslash\{1\}$, we can write U in the form $U = \tilde{b}A = A\tilde{b}$ for some A. Set $A \equiv B$ iff there exist integers $n, k \geq 0$ with $U^n A = U^k B$. It is easy to check that this yields a congruence relation on the semi-group $\mathcal{H}$. We let $\hat{G}$ denote the quotient of $\mathcal{H}$ by this congruence relation. The following Lemma allows us to apply the results of the previous section.

Lemma 2: *The semigroup $\hat{G}$ is in fact a group, which is a central extension of G via the map $\varphi : \hat{G} \to G$ induced by the evaluation function E. If we let $\hat{a}$ denote the image of $\tilde{a}$ in $\hat{G}$, then $\varphi(\hat{a}) = a$, the relations (I) hold and the elements $\hat{a}$ generate $\hat{G}$.*

Proof: Lemma 1 shows that the semi-group $\hat{G}$ is a central extension of G via φ. It only remains to show that $\hat{G}$ is in fact a group, the other assertions are clear.

For any $b \in G\backslash\{1\}$ we have $U = \tilde{b}A = A\tilde{b}$ for some A, by the above remark. Thus $\hat{b}$ is invertible in $\hat{G}$. Since the $\hat{b}$ generate $\hat{G}$, all elements of $\hat{G}$ are invertible, and $\hat{G}$ is a group. □

Lemma 3: *If $g, h \in G$ are conjugate elements of order $m > 1$, and $G =< a_1, \ldots, a_r >$, then $\tilde{g}^m\tilde{a}_1 \cdots \tilde{a}_r = \tilde{h}^m\tilde{a}_1 \cdots \tilde{a}_r$.*

Proof: By Lemma 1 we have $\tilde{g}^m \in Z(\mathcal{H})$. Hence

$$\begin{aligned}\tilde{g}^m\tilde{a}_1 \cdots \tilde{a}_r = \tilde{a}_1 \cdots \tilde{a}_{j-1}\tilde{g}^m\tilde{a}_j \cdots \tilde{a}_r &= \tilde{a}_1 \cdots \tilde{a}_{j-1}\tilde{g}^{m-1}\tilde{a}_j\widetilde{g^{a_j}}\tilde{a}_{j+1} \cdots \tilde{a}_r \\ &= \cdots = \tilde{a}_1 \cdots \tilde{a}_{j-1}\tilde{a}_j(\widetilde{g^{a_j}})^m\tilde{a}_{j+1} \cdots \tilde{a}_r = (\widetilde{g^{a_j}})^m\tilde{a}_1 \cdots \tilde{a}_r.\end{aligned}$$

Since $a_1, \ldots, a_r$ generate the finite group G, the claim follows by induction. □

Lemma 4: *If $S(B) \geq S(XU)$ (componentwise) for some $X \in \mathcal{H}$ then $B = XV$ for some $V \in \mathcal{H}$. In particular, if $S(B) \geq S(U^2)$ then $B = UV$ for some $V \in \mathcal{H}$.*

Proof: By induction it suffices to consider the case $X = \tilde{a}$. Let m be the order of a, and Γ the conjugacy class of a (in G). Since $S(B) \geq S(\tilde{a}U)$, there are more than $m|\Gamma|$ indices $i = 1, \ldots, s$ for which $b_i \in \Gamma$ (where $B = \tilde{b}_1 \cdots \tilde{b}_s$). Hence there is some $g \in \Gamma$ such that $b_i = g$ for more than m indices i. Use (I') to conclude that B can be written as $B = \tilde{g}^m\tilde{w}_1 \cdots \tilde{w}_k$ with $w_1 = g$. Then each nontrivial conjugacy class of G contains some w_i. Therefore the union of the conjugates of the subgroup $< w_1, \ldots, w_k >$ is all of G. It is well-known that this implies that $G =< w_1, \ldots, w_k >$ (e.g., [FrJ, 12.4]). Thus Lemma 3 yields $B = \tilde{g}^m\tilde{w}_1 \cdots \tilde{w}_k = \tilde{a}^m\tilde{w}_1 \cdots \tilde{w}_k = \tilde{a}V$ for some V. □

Let $\mathcal{H}_i$ be the set of all $V \in \mathcal{H}$ with $S(V) = S(U^i)$. By Lemma 4 the map $\mathcal{H}_i \to \mathcal{H}_{i+1}$, $V \mapsto UV$, is surjective for $i \geq 1$. Since the $\mathcal{H}_i$ are finite sets, there must be some integer K such that for all $i \geq K$ this map is bijective. Thus for $A, B \in \mathcal{H}_K$ and $n \geq 0$ the relation $U^n A = U^n B$ implies $A = B$.

Conclusion: *Suppose $M(G)$ is generated by commutators. Let $A = \tilde{a}_1 \cdots \tilde{a}_r,\ B = \tilde{b}_1 \cdots \tilde{b}_r$ be elements of $\mathcal{H}$ with $S(A) = S(B) \geq S(U^K)$ and $a_1 \cdots a_r = b_1 \cdots b_r$. Then $A = B$. That is, $(b_1, \ldots, b_r)$ is in the Hurwitz class of $(a_1, \ldots, a_r)$.*

Proof: By Lemma 2 and the Proposition of §B, we have $\prod \hat{a}_i = \prod \hat{b}_i$. Hence $U^n A = U^k B$ for some $n, k \geq 0$. Since $S(A) = S(B)$ we have $n = k$. By Lemma 4 we have $A = XW,\ B = XV$ for some $V, W \in \mathcal{H}_K,\ X \in \mathcal{H}$. Since $\hat{G}$ is a group, we have $YX = U^t$ for some $Y \in \mathcal{H},\ t \geq 0$.

Summarizing, we have $U^n A = U^n B$, hence $U^n XW = U^n XV$. Multiplying both sides by Y from the left we get $U^{n+t} W = U^{n+t} V$. Since $W, V \in \mathcal{H}_K$ this implies $W = V$ by the remarks after Lemma 4. Thus $A = XW = XV = B$. □

The Theorem of §A now follows from this Conclusion.

Bibliography

[Ax] J. Ax, The elementary theory of finite fields, *Annals of Math.* **88** (1968), 239–271.

[BF] R. Biggers and M. Fried, Moduli Spaces of Covers of $\mathcal{P}^1$ and the Hurwitz Monodromy Group, *J. für die reine und angew. Math.* **335** (1982), 87–121.

[C] R. Carter, Simple Groups of Lie Type, *John Wiley and Sons, Pure and Applied Mathematics* **XXVIII** (1972).

[Cl] A. Clebsch, Zur Theorie der Riemann'schen Fläche, *Math. Annalen* **6** (1872), 216-230.

[CP] J. H. Conway and R. A. Parker, On the Hurwitz number of arrays of group elements, *unpublished preprint*, September 1988.

[CHa] K. Coombs and D. Harbater, Hurwitz families and arithmetic Galois groups, *Duke Math. J.* **52** (1985), 821–839.

[DFr] P. Debes and M. Fried, Regular extensions of $\mathcal{R}(x)$ and Rigidity, *preprint.*

[Fr, 1] M. Fried, Fields of definition of function fields and Hurwitz families—groups as Galois groups, Comm. in Algebra **5(1)** (1977), 17–82.

[Fr, 2] M. Fried, Galois groups and Complex Multiplication, *TAMS* **235** (1978), 141–162.

[Fr, 3] M. Fried, Arithmetic of 3 and 4 branch point covers: a bridge provided by non-congruence subgroups of $\mathrm{SL}_2(\mathcal{Z})$, *Progress in Math. Birkhäuser* **81** (1989), 77-117.

[FrJ] M. Fried and M. Jarden, Field Arithmetic, *Springer–Ergebnisse* **11** (1986).

[FrJ, 2] M. Fried and M. Jarden, Diophantine properties of subfields of $\mathcal{Q}$, *Amer. J. Math.* **100** (1978), 653–666.

[FrVo] M. Fried and H. Völklein, The embedding problem over a Hilbertian PAC-field, *preprint.*

[Fu] W. Fulton, Hurwitz schemes and irreducibility of moduli of algebraic curves, *Annals of Math.* **90** (1969), 542–575.

[Fy] G. Frey, Pseudo-algebraically closed fields with non-archimedean real valuations, *J. of Algebra* **26** (1973), 202–207.

[Hu] B. Huppert, Endliche Gruppen I, *Graduate Texts-Springer* (1967), Berlin, Heidelberg, New York.

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

[LD] A. Lubotzky and L. v. d. Dries, Subgroups of free profinite groups and large subfields of $\bar{\mathcal{Q}}$, *Israel J. Math.* **39** (1981), 25–45.

[Ma,1] H. Matzat, Konstruktive Galoistheorie, *Lecture Notes in Math.* **1284**, *Springer Verlag* (1986).

[Ma,2] H. Matzat, Zöpfe und Galois'sche Gruppen, *preprint 1990.*

[P] F. Pop, The totally real numbers are PRC, preprint as of Oct. '90.

[Se] J.-P. Serre, Topics in Galois Theory, *notes by H. Darmon, Harvard* 1989.

[SGA1] A. Grothendieck, Revêtements étale et groupes fondamental, *Lecture Notes in Math.* **224**, *Springer Verlag* (1971).

[Th] J.G. Thompson, Some finite groups which occur as $\mathrm{Gal}(L/K)$ where $K \leq \mathcal{Q}(\mu_n)$, *J. of Algebra* **89** (1984), 437–499.

[Vo] H. Völklein, $\mathrm{PSL}_2(q)$ and extensions of $\mathcal{Q}(x)$, *BAMS* **24** (1991), 145–153.

[W] A. Weil, The field of definition of a variety, *Amer. J. Math* **78** (1956), 509–524.

[Ws] R. Weissauer, Der Hilbertsche Irreduzibilitätssatz, *J. für die reine und angew. Math.* **334** (1982), 203–220.

Mike Fried
Department of Mathematics
UC Irvine
Irvine, California 92717

Helmut Völklein
Department of Mathematics
University of Florida
Gainesville, Fl 32611