COMMUNICATIONS IN ALGEBRA, 5(1), 17-82 (1977)

Fields of Definition of Function Fields and Hurwitz Families — Groups as Galois Groups

By

M. FRIED*

University of California at Irvine

Irvine, California

Introduction

Let G be a finite group. Hilbert ([Hi]) posed the problem: does there exist a Galois extension $\hat{L}/\varphi$ such that $G = G(\hat{L}/\varphi)$? Shafarevich ([Sha]) showed that the answer to Hilbert's problem is affirmative for G solvable. For G the alternating or symmetric group of degree n, and for many other families of groups the answer is again affirmative. In fact, no counter-example is known.

Noether suggested a generic approach to the problem. Let (G, T) be a pair consisting of a faithful transitive permutation representation $T: G \to S_n$

* The research for this paper was partially supported by an Alfred P. Sloan Foundation Grant and by a grant from the Institute for Advanced Study (Princeton) in Spring 1973.

(where S_n is the symmetric group on n = deg(T) letters). Let: $y_1,\dots,y_n$ be algebraically independent indeterminates; G act on $\varphi(y_1,\dots,y_n)$ as permutations of rational functions in $y_1,\dots,y_n$ through the representation T, and; $(\varphi(y_1,\dots,y_n))^G$ be the fixed field of the action of G. Then we have: $G(\varphi(y_1,\dots,y_n)/(\varphi(y_1,\dots,y_n))^G) = G$.

Noether's Problem [No]: Is $(\varphi(y_1,\dots,y_n))^G$ pure transcendental? Equivalently, do there exist algebraically independent indeterminates $x_1,\dots,x_n$ such that $\varphi(x_1,\dots,x_n) = (\varphi(y_1,\dots,y_n))^G$?

From Hilbert's irreducibility theorem, an affirmative answer to Noether's problem gives an affirmative answer to Hilbert's problem by use of specialization of $x_1,\dots x_n$ to values in $\mathbb{Q}$. Swan ([Sw]), however, gave counter-examples to Noether's problem even in the case where G is a cyclic group of prime order.

For many diophantine problems (including the investigation of the Hilbert and Noether problems) it is of interest to ask: does there exist a Galois regular extension $\hat{L}$ of $\varphi(x)$ such that $G(\hat{L}/\varphi(x)) = G$? The regularity property means that the algebraic closure of φ in $\hat{L}$ is just φ itself. For the purposes of easy reference we denote by the one-variable problem the following explicit version of this problem.

Let $\sigma(1), \dots, \sigma(r)$ be generators of the group G such that $\sigma(1)\cdots\sigma(r)$ is the identity element. From Riemann's existence theorem there exists a projective non-singular cover $Y \xrightarrow{\varphi(Y)} \mathbb{P}^1$ ($\mathbb{P}^1$ is projective 1-space) such that the cover has a description of its branch cycles given by $\sigma(1), \dots, \sigma(r)$ (see Section 1A). Let $K(\underset{\sim}{\sigma})$ be the intersection of all fields of definition of all pairs $(Y, \varphi(Y))$ having $\sigma(1), \dots, \sigma(r)$ as a description of their branch cycles. For a given pair (Y,φ), let K be a field of definition of (Y,φ). We denote by $\hat{K}$ the algebraic closure of K in $\widehat{K(Y)}$, the Galois closure of the field extension $K(Y)/K(\mathbb{P}^1)$. Let $\hat{K}(\underset{\sim}{\sigma})$ be the intersection of all of the fields $\hat{K}$ as K and (Y,φ) vary as above.

One-Variable Problem. For given G and $\sigma(1), \ldots, \sigma(r)$, as above, describe explicitly the fields $K(\underset{\sim}{\sigma})$ and $\hat{K}(\underset{\sim}{\sigma})$.

The main arithmetic results are in Section 5. In Corollary 5.2 we describe two cyclotomic fields K_M and $K_{\hat{M}}$ (dependent only on $\sigma(1), \ldots, \sigma(r)$) such that $K_M \subset K(\underset{\sim}{\sigma})$ and $K_{\hat{M}} \subset \hat{K}(\underset{\sim}{\sigma})$. In addition, Corollary 5.4 shows that if the Hurwitz number, $\mathrm{Hur}(\underset{\sim}{\sigma})$ of $\sigma(1), \ldots, \sigma(r)$, is 1 (see below) and if the automorphism group, $\mathrm{Aut}(Y,\varphi)$, is the identity, then $K_M = K(\underset{\sim}{\sigma})$. With the help of Proposition 2 of Section 2 these results are sufficient to gain considerable information toward determining $\hat{K}(\underset{\sim}{\sigma})$ in special cases.

These results are deduced from analogous results concerning the field of definition of a collection of quasi projective algebraic varieties consisting of a symmetrized Hurwitz family $\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r)$ and some of its structure morphisms.

We quickly describe $\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r)$. Let $\mathcal{O}(n,r)$ be the collection of isomorphism classes of covers $Y' \xrightarrow{\varphi'} \mathbf{P}^1$, (an isomorphism of covers commutes with the projections to $\mathbf{P}^1$) with: $\deg(\varphi') = n$, and; φ' has r branch points (points of $\mathbf{P}^1$ over which Y' is ramified). Consider the (coarse) topology in $\mathcal{O}(n,r)$ given by: the isomorphism classes (Y_1,φ_1) and (Y_2,φ_2) are "close" if (1) the branch points of φ_1 and φ_2 are "close" and; (2) (Y_1,φ_1) is a deformation of (Y_2,φ_2) that moves the branch points of φ_1 to those of φ_2. In this topology $\mathcal{O}(n,r)$ is a complex manifold (Section 4.A). We define $\mathcal{O}(Y,\varphi;r)$ to be the connected component of $\mathcal{O}(n,r)$ containing the isomorphism class of (Y,φ). When it exists, $\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r)$ is a total family of covers of $\mathbf{P}^1$, fibered over $\mathcal{O}(Y,\varphi;r)$ such that: the fiber $(\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r))_p$ represents the isomorphism class of $p \in \mathcal{O}(Y,\varphi;r)$. In Section 4.A and B conditions are given for the existence of $\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r)$. We can guarantee existence and uniqueness only in the case $\mathrm{Aut}(Y,\varphi) = \{\mathrm{Id.}\}$. The Hurwitz number, $\mathrm{Hur}(\underset{\sim}{\sigma})$, of Section 4.B is the number of connected components of $\mathcal{O}(n,r)$ containing isomorphism classes of covers $Y' \xrightarrow{\varphi'} \mathbf{P}^1$ for which $\underset{\sim}{\sigma}$ is a description of the branch cycles of φ'. When $\mathrm{Aut}(Y,\varphi) = \{\mathrm{Id.}\}$ and $\mathrm{Hur}(\underset{\sim}{\sigma}) = 1$ Theorem 5.1 gives the exact minimal field of definition

(K_M as in the discussion above) of the collection consisting of $\mathcal{I}(Y,\varphi;r)$, $\mathcal{O}(Y,\varphi;r)$ and their structure morphisms. The projective structure on $\mathcal{O}(Y,\varphi;r)$ comes from a cover of an open subset of $\mathbb{P}^r$ obtained by associating to a cover $Y' \xrightarrow{\varphi'} \mathbb{P}^1$ the unordered collection consisting of the branch points of φ'. From this cover and the results of Section 5 we obtain results on Hilbert's and Noether's problem applied to groups obtained as quotients of the Hurwitz monodromy group. In particular, using computations of Cohen [Co] it is shown in Section 6 that for each integer ℓ there is a quadratic extension L of $\mathbb{Q}$ and a Galois extension M of L such that $G(M/L)$ is $PSp(\mathbb{Z}/(3), 2\ell)$ (projective symplectic group over the finite field $\mathbb{Z}/(3)$).

In Section 6 the other examples include: a reinspection in our framework of a construction going back to Hilbert that shows that A_n (alternating group of degree n) can be realized as a Galois group over $\mathbb{Q}$; computations toward the realization of the Mathieu group of degree 11 as the Galois group of a Galois extension of a quadratic extension of $\mathbb{Q}$, and; computations with the so-called elementary groups.

We describe the remaining material of the paper. Section 1 contains a fairly detailed discussion of covers of $\mathbb{P}^1$ including: the simple covers of $\mathbb{P}^1$ (all branch cycles are 2-cycles) and their associated families considered by Hurwitz. It is a classical computation going back to Clebsch ([Cle]) that the Hurwitz number is 1 for a simple cover. This, combined with the fact that for $n > 2g + 2$ a curve Y of genus g can be represented as a simple branched cover of $\mathbb{P}^1$ allowed Severi to prove the irreducibility of the moduli space of curves of genus g. This problem is, indeed, the original motivation for the consideration of Hurwitz schemes (see [Fu]). In [Fr and Ja] it is shown that if Y is a projective nonsingular curve of genus g defined over a field K of characteristic zero, then there exists a cover $Y \xrightarrow{\varphi} \mathbb{P}^1$ with (Y,φ) a simple cover defined over K (the arithmetic analogue of Severi's result).

In addition, Section 1 contains a computation that shows that for the general curve $\bar{Y}$ of genus $g \geq 2$, if $\bar{Y} \xrightarrow{\varphi} \bar{Y}'$ is a cover with $\deg(\varphi) \geq 2$, then $\bar{Y}'$ is of genus zero.

In Section 2 some attention is paid to the effect of going to the Galois closure of a cover defined over a field that is not algebraically closed (the extension of constants problem). In [Fr, 1] this is considered in detail since the analysis of this problem has many exciting applications besides those stated in the problems of Hilbert and Noether.

The results of Section 4 are completed in [Fr, 2] which contains references and results on the detailed structure of representations of the Hurwitz monodramy group. There (see the end of Section 5) it is most natural to consider covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ equipped with the additional structure coming from a characteristic subgroup H of Aut (Y,φ) (H may be $\{\text{Id.}\}$ or all of Aut (Y,φ)). Results for "Hurwitz families" of such structures similar to the results of Section 5 would significantly generalize the results of this paper (see [Fr and L]).

We would like to thank William Messing for his careful reading of this paper.

Section 0. Notation and Terminology

As usual $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote respectively the ring of rational integers, the rational number field, the field of real numbers, and the field of complex numbers. An algebraic number field is a finite extension of $\mathbb{Q}$, usually denoted by K or L with possible additional notation (e.g., $\hat{K}$, L_1, etc). For a number field K, the ring of integers is denoted $\mathcal{O}_K$. Depending on the context, the prime ideals of $\mathcal{O}_K$ will be p, or $\mathfrak{p}$, or $\wp$; and the residue class field of $\mathfrak{p}$ is denoted $\mathcal{O}_K/\mathfrak{p}$. Also: $\mathbb{F}(q)$ is the finite field with q elements; F(x) is the field of rational functions in x with coefficients in F.

0.A) General Field Notation.

We write E/F for a finite separable extension of fields. When the context permits, $\bar{F}$ is a fixed algebraic closure of F containing E. Again, when the context is clear, $\hat{E}$ is the Galois closure of E/F, and $G(\hat{E}/F)$ is the associated Galois group. If we write E as a simple extension of F, say $E = F(\theta)$, the action of $G(\hat{E}/F)$ on the conjugates of θ over F determines a permutation representation $T(E,F)$ of $G(\hat{E}/F)$. This is an embedding of $G(\hat{E}/F)$ into S_n, the symmetric group on $n = [E:F]$ letters. For different choices of θ, the corresponding permutation representations are equivalent (see below). The representation $T(E,F)$ is faithful and transitive.

0.B) Permutation Groups

Finite groups are denoted by capital letters G, H combined with extra symbols (e.g., $\hat{G}$, H(1), etc.). For H a subgroup of the group G, the normalizer of H in G is denoted $N_G(H)$. For $\sigma(1),\ldots,\sigma(r) \in G$, the subgroup of G generated by $\sigma(1),\ldots,\sigma(r)$ is denoted $G(\underline{\sigma})$. The conjugacy class in G of $\sigma \in G$ is denoted $Con(\sigma,G) = \{g\sigma g^{-1} \mid g \in G\}$. There is a need to consider the conjugacy classes of σ as an element of several groups.

For a pair (G, T) consisting of a group G equipped with a permutation representation $T : G \to S_n$, we say that n is the degree of T (deg(T)). We adopt the convention that permutations act on the right of the integers $1,2,\ldots,n$ (e.g. for $\sigma \in G$, $T(\sigma)$ maps i to $(i)T(\sigma)$, $i = 1,\ldots,n$). For H a subgroup of a finite group G, the permutation representation of G obtained by multiplication on the (right of) right cosets of H in G is denoted by $T_{H.}$.

We say that (G, T_1) and (G, T_2) are equivalent (as permutation representations) if there exists $\gamma \in S_n$ such that

$$\gamma^{-1} \cdot T_1(\sigma) \cdot \gamma = T_2(\sigma) \quad \text{for all } \sigma \in G.$$

For $\sigma \in S_n$ we may decompose σ as a product of disjoint cycles, $\sigma = \gamma_1 \cdot \gamma_2 \cdot \cdots \cdot \gamma_t$ where γ_i is a cycle of s(i) letters, $i = 1,\ldots,t$. By

abuse: $\sigma = (s(1))\ldots(s(t))$ where it is understood that the cycles of length 1 are usually omitted. Denote by ind(σ) (index of σ) the quantity $\sum_{i=1}^{t}(s(i)-1)$.

0.C Coverings

Throughout this article, the use of the term algebraic variety is restricted to reduced, irreducible algebraic sets which are embedded as Zariski locally closed subsets of projective N-space, $\mathbb{P}^N(\mathbb{C})$ (for some integer N). That is, our varieties are quasi-projective. If W is an algebraic variety, we say that W is projective if W is a closed subvariety of $\mathbb{P}^N(\mathbb{C})$. With few exceptions all varieties are normal. In particular, 1 dimensional varieties (curves) are non-singular ([Mum, p. 388]).

Let $W \xrightarrow{\varphi} V$ be a morphism of algebraic varieties. Unless otherwise stated, all morphisms will be assumed to be flat ([Mum, p. 424]). Since our desire is to avoid any heavy use of the language of schemes, all points are to be considered as geometric points (coordinates are in $\mathbb{C}$).

For X an algebraic subset of V we let W_X denote the fiber product (not necessarily irreducible) of $X \subset V$ and $W \to V$ over V. We say that φ is a covering morphism (by abuse: a cover) if φ is surjective and finite ([Mum, p.243]). We remind that φ is finite iff the fibers of φ consist of a finite set of points, and φ is proper ([Mum, p. 237]). Since φ is finite (and flat), for each point $p \in V$ there is an affine neighborhood Spec (A) of p such that $W_{\mathrm{Spec}(A)} = \mathrm{Spec}(B)$ where: A and B are rings of finite type over $\mathbb{C}$, and B is a free A-module of dimension n, for some integer n. We say that degree of φ (deg(φ)) is n. We say that φ is unramified at p if the fiber W_p consists of n distinct points. Then φ is unramified (or etale) if φ is unramified at each point of V. The points of V where φ is ramified are called branch points of φ.

Each of the algebraic sets W, V, and φ (φ identified with its graph) are described as the zero sets of a finite collection of homogeneous poly-

nomials. We say that (W, V, φ) is defined over a field F if these polynomials can be selected to have their coefficients in F.

Assume that (W, V, φ) is defined over F. Let F(W) denote the field of algebraic functions f on W which are defined over F (f regarded as a cycle on $W \times \mathbf{P}^1$ is defined over F). Then we canonically induce a map of fields $F(V) \to F(W)$ so that F(W) is an extension of F(V) of degree n. We let $\mathrm{Aut}(W, \varphi)$ (or $\mathrm{Aut}(W/V)$) denote the group of morphisms $\psi : W \xrightarrow{\varphi} W$ (with $W \xrightarrow{\varphi} V$ and $W \xrightarrow{\varphi} V$). We let $\mathrm{Aut}(W, \varphi, F)$ be the subgroup of those automorphisms which are defined over F. Then, if W is normal, $\mathrm{Aut}(W, \varphi, F)$ may be identified with the field automorphisms of F(W) which are the identity when restricted to F(V).

We say that the covers $W \xrightarrow{\varphi} V$ and $W' \xrightarrow{\varphi'} V$ are isomorphic if there exists a commutative diagram $W' \xrightarrow{\psi} W$, $\varphi' : W' \to V$, $\varphi : W \to V$ where ψ is an isomorphism of algebraic varieties. The cover $W \xrightarrow{\varphi} V$ is said to be a Galois cover over F if the order of $\mathrm{Aut}(W, \varphi, F)$ is equal to $\deg \varphi$. In this case, the extension F(W)/F(V) is a Galois extension.

Section 1. Riemann's Existence Theorem: Examples of Covers of $\mathbf{P}^1$

1.A) Riemann's Existence Theorem: Application to the Generic Curve of Genus $g \geq 2$.

Let $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$ be a finite set of distinct points on the non-singular projective curve X. Let $\mathrm{Cov}(X; \mathcal{Y}_1, \ldots, \mathcal{Y}_r)$ be the collection of isomorphism classes of connected covers $Y \xrightarrow{\varphi} X$ of non-singular curves (over $\mathbb{C}$) such that the branch points of φ are among the points $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$. Riemann's Existence Theorem gives an explicit description of $\mathrm{Cov}(X; \mathcal{Y}_1, \ldots, \mathcal{Y}_r)$. We review this (see [Fr and L; Section III. 4)] or [Sp; Section 5. 5] or [Tre]).

Let $2 \cdot g(X)$ be the rank of $H_1(X, \mathbb{Z})$, the first integral homology group. Let P be a point of $X - \{\mathcal{Y}_1, \ldots, \mathcal{Y}_r\} = U$. Then the topological fundamental

group $\pi^1(U, P)$ is a free group on $2g(X) + r$ generators $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_g, \tilde{\beta}_1, \ldots, \tilde{\beta}_g$, $\tilde{\sigma}(1), \ldots, \tilde{\sigma}(r)$ with one relation,

$$(1.1)\quad \tilde{\alpha}_1 \cdot \tilde{\beta}_1 \cdot \tilde{\alpha}_1^{-1} \cdot \tilde{\beta}_1^{-1} \cdot \tilde{\alpha}_2 \cdot \tilde{\beta}_2 \cdot \tilde{\alpha}_2^{-1} \cdot \tilde{\beta}_2^{-1} \cdots \tilde{\alpha}_g \cdot \tilde{\beta}_g \cdot \tilde{\alpha}_g^{-1} \cdot \tilde{\beta}_g^{-1} \cdot \tilde{\sigma}(1) \cdots \tilde{\sigma}(r) = \mathrm{Id}.$$

We wish to normalize to some extent our choice of $\tilde{\sigma}(1), \ldots, \tilde{\sigma}(r)$. To do this we demand that $\tilde{\sigma}(i)$ is represented by a path on U consisting of 3 parts (see Figure 1 of Lemma 1.1): $\theta^+(i)$ going from P to a neighborhood of $\wp_i$; L, a closed path which is the oriented boundary of a neighborhood of $\wp_i$ (oriented by the orientation on X), and; $\theta^-(i)$, going from the endpoint of $\theta^+(i)$ back to P. There is a one-one correspondence between the following sets: conjugacy classes of subgroups of $\pi^1(U, P)$ of index n; isomorphism classes of connected unramified covers of U of degree n; and isomorphism classes of non-singular covers of X of degree n in $\mathrm{Cov}(X; \wp_1, \ldots, \wp_r)$. Let $Y \xrightarrow{\varphi} X$ represent an element of $\mathrm{Cov}(X; \wp_1, \ldots, \wp_r)$. Let H be a subgroup of $\pi^1(U, P)$ corresponding to this cover. Then we obtain a transitive permutation representation T_H of $\pi^1(U, P)$ (Section 0.B). We denote the images of

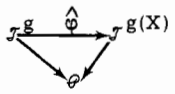
$\tilde{\alpha}_1, \ldots, \tilde{\alpha}_g, \tilde{\beta}_1, \ldots, \tilde{\beta}_g$, $\tilde{\sigma}(1), \ldots, \tilde{\sigma}(r)$ in S_n by $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$, $\sigma(1), \ldots, \sigma(r)$. Two $2 \cdot g + r$-tuples of elements, $(\underset{\sim}{\alpha}, \underset{\sim}{\beta}, \underset{\sim}{\sigma})$ and $(\underset{\sim}{\alpha}', \underset{\sim}{\beta}', \underset{\sim}{\sigma}')$ from S_n are equivalent if there exists $\gamma \in S_n$ such that $\gamma \cdot \alpha_i \cdot \gamma^{-1} = \alpha_i'$, $\gamma \cdot \beta_i \cdot \gamma^{-1} = \beta_i'$, and $\gamma \cdot \sigma(j) \cdot \gamma^{-1} = \sigma(j)'$ for $i = 1, \ldots, g$, $j = 1, \ldots, r$.

Riemann's Existence Theorem. The elements of $\mathrm{Cov}(X; \wp_1, \ldots, \wp_r)$ of degree n are in one-one correspondence with the equivalence classes of $2g + r$-tuples $(\underset{\sim}{\alpha}, \underset{\sim}{\beta}, \underset{\sim}{\sigma})$ of elements of S_n such that: $\underset{\sim}{\alpha}, \underset{\sim}{\beta}, \underset{\sim}{\sigma}$ together generate a transitive subgroup $G(\underset{\sim}{\alpha}, \underset{\sim}{\beta}, \underset{\sim}{\sigma})$ of S_n; and $\alpha_1 \cdot \beta_1 \cdot \alpha_1^{-1} \cdot \beta_1^{-1} \cdots \alpha_g \cdot \beta_g \cdot \alpha_g^{-1} \cdot \beta_g^{-1} \cdot \sigma(1) \cdots \sigma(r) = \mathrm{Id}$. (The identity element of S_n). In this correspondence, the genus, g(Y), of the cover $Y \xrightarrow{\varphi} X$ is given by the Riemann Hurwitz formula

$$(1.2)\quad 2 \cdot (g(Y)-1) = 2 \cdot \deg(\varphi)\,(g(X)-1) + \sum_{i=1}^{r} \mathrm{ind}(\sigma(i)).$$

The group $G(\alpha,\beta,\sigma)$ is sometimes called the monodromy group of the cover $Y \xrightarrow{\varphi} X$. Our main concern in this paper is the case when $X = \mathbf{P}^1$.

It is interesting to note* that, for the general curve Y of genus $g(Y) > 1$, if $Y \xrightarrow{\varphi} X$ is a cover, then either $\deg \varphi = 1$ or $g(X) = 0$. We outline a proof of this fact. Suppose that the general curve of genus $g > 1$ covers X where $g(X) \geq 1$. Since there is an algebraic family of curves of genus g(see [Fu]), it can be shown that there is a morphism



of algebraic varieties having the following properties: for each point $p \in \mathcal{P}$,

(1.3) $\mathcal{T}^g_p \xrightarrow{\hat{\varphi}_p} \mathcal{T}^{g(X)}_p$ is a cover of a curve of genus g(X) by a curve of genus g with r (fixed number) distinct branch points, and;

(1.4) $\mathcal{T}^g$ is obtained by pullback from a Zariski open subset of the moduli family of curves of genus g.

Let $p^{(0)}$ be a generic point of $\mathcal{P}$. Let $T(\mathcal{P})_{p^{(0)}}$ be the Zariski tangent space to $\mathcal{P}$ at $p^{(0)}$; $T(\mathcal{T}^g_{p^{(0)}})$, the Zariski tangent bundle to $\mathcal{T}^g_{p^{(0)}}$. Then deformation theory ([Ko and Sp]) shows that there is surjective map $T(\mathcal{P})_{p^{(0)}} \to H^1(\mathcal{T}^g_{p^{(0)}}, T^g_{p^{(0)}})$ where $H^1(\mathcal{T}^g_{p^{(0)}}, T(\mathcal{T}^g_{p^{(0)}}))$ is a vector space of dimension $3\cdot g - 3$. This may be interpreted as: there are $3\cdot g - 3$ deformation parameters for the complex structures on a compact topological surface of genus g. Let $x(p,1),\ldots,x(p,r)$ be the (distinct) branch points of the cover (1.3). For a space W we let $W^{(r)}$ denote the symmetric product of r copies of W.

We obtain a map $\mathcal{P} \to (\mathcal{T}^{g(X)})^{(r)}$ by associating to $p \in \mathcal{P}$ the collection $\{x(1,p),\ldots,x(r,p)\}$. From this we induce a map

(1.5) $T(\mathcal{P})_{p^{(0)}} \to H^1(\mathcal{T}^{g(X)}_{p^{(0)}}, T(\mathcal{T}^{g(X)}_{p^{(0)}})) \times (\mathcal{T}^{g(X)}_{p^{(0)}})^{(r)}$

---

*this will not be used in the rest of the paper.

The image of the map in (1.5) may be interpreted as: the space of deformations of the cover $\mathfrak{I}^g_{\underline{p}^{(0)}} \xrightarrow{\varphi_{\underline{p}^{(0)}}} \mathfrak{I}^{g(X)}_{\underline{p}^{(0)}}$ by Riemann's existence theorem. Therefore, the dimension of the image space of the map in (1.5) is less than or equal to $3\cdot g - 3$, or:

$$(1.6) \qquad 3\cdot g - 3 \leq 3\cdot g(X) - 3 + r \ .$$

Let $\sigma(1,\underline{p}^{(0)}),\ldots,\sigma(r,\underline{p}^{(0)})$ correspond, in the cover $\mathfrak{I}^g_{\underline{p}^{(0)}} \to \mathfrak{I}^{g(X)}_{\underline{p}^{(0)}}$, to elements $\sigma(1),\ldots,\sigma(r)$ in the statement of Riemann's Existence Theorem. From the Riemann-Hurwitz formula:

$$(1.7) \qquad 2g-2 = \deg(\varphi)\ (2g(X)-2) + \sum_{i=1}^{r} \operatorname{ind}(\sigma(i,\underline{p}^{(0)})).$$

Therefore

$\sum_{i=1}^{r} \operatorname{ind}(\sigma(i,\underline{p}^{(0)})) \geq r$. From (1.6) and (1.7) we obtain

$$g(X) - 1 + r/3 \geq \deg(\varphi)\,(g(X) - 1) + r/2.$$

If $g(X) = 1$, then $r = 0$, and we deduce that $g = 1$. If $g(X) \geq 2$, we have a contradiction unless $\deg(\varphi) = 1$. This proves our assertion.

1.B) Examples of Covers of $\mathbb{P}^1$

Let Y be a non-singular curve. We obtain covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ from non-constant elements of $\mathbb{C}(Y)$. For example, if $Y \subseteq \mathbb{P}^N(\mathbb{C})$ we obtain a cover of $\mathbb{P}^1$ by projection on a coordinate axis of $\mathbb{P}^N(\mathbb{C})$. As long as this projection is surjective, the degree of the cover is at most the degree of Y as a subspace of $\mathbb{P}^N(\mathbb{C})$. (the cardinality of the intersection of Y with a generic hyperplane on $\mathbb{P}^N(\mathbb{C})$).

Elements of $\sigma(1),\ldots,\sigma(r) \in S_n$ ($n = \deg \varphi$) corresponding to $Y \xrightarrow{\varphi} \mathbb{P}^1$ in the statement of Riemann's Existence Theorem are called a <u>description of the branch cycles</u> of (Y,φ). Assume that $(\tau(1),\ldots,\tau(r)) = \mathcal{I}$ is another description

of the branch cycles of (Y,φ). We denote: the branch points of φ by $u(1),\dots,u(r)$; $\mathbb{P}^1 - \{u(1),\dots,u(r)\} = U$.

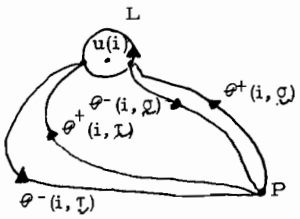
Lemma 1.1. There exists $\gamma \in S_n$ such that

(1.8) $\quad \mathrm{Con}(\sigma(i), G(\underset{\sim}{\mathcal{G}})) = \mathrm{Con}(\gamma\,\tau(i)\,\gamma^{-1}, G(\underset{\sim}{\mathcal{G}}))$, $i = 1,\dots,r$.

Proof. The elements $\sigma(1),\dots,\sigma(r)$ depend on the choice of: base point P; naming of the points of fiber above P; and generators $\breve{\sigma}(1),\dots,\breve{\sigma}(r)$ of $\pi^1(U,P)$. It is well-known that a change of P and naming of the points of the fiber results in a replacement of $\sigma(1),\dots,\sigma(r)$ by $\gamma\cdot\sigma(1)\cdot\gamma^{-1},\dots,\gamma\cdot\sigma(r)\cdot\gamma^{-1}$ for some $\gamma \in S_n$. Therefore, we may assume that $\underset{\sim}{\mathcal{G}}$ and $\underset{\sim}{\tau}$ are computed with respect to the same base point P and the same naming of the fiber above P.

Let $\theta(1,\underset{\sim}{\mathcal{G}}),\dots,\theta(r,\underset{\sim}{\mathcal{G}})$ (respectively, $\theta(1,\underset{\sim}{\tau}),\dots,\theta(r,\underset{\sim}{\tau})$) be paths representing $\breve{\sigma}(1),\dots,\breve{\sigma}(r)$ (respectively, $\breve{\tau}(1),\dots,\breve{\tau}(r)$). We break up $\theta(i,\underset{\sim}{\mathcal{G}})$ into 3 pieces (as in Figure 1): $\theta^+(i,\underset{\sim}{\mathcal{G}})$, going from P to a neighborhood of u(i); L, an oriented boundary of a neighborhood of u(i), and; $\theta^-(i,\underset{\sim}{\mathcal{G}})$, going from L back to P.

Figure 1.



Then: $\theta(i,\underset{\sim}{\mathcal{G}}) = \theta^+(i,\underset{\sim}{\mathcal{G}})\cdot L\cdot\theta^-(i,\underset{\sim}{\mathcal{G}})$, and; $\theta(i,\underset{\sim}{\tau}) = \theta^+(i,\underset{\sim}{\tau})\cdot L\cdot\theta^-(i,\underset{\sim}{\tau})$. Let $\theta = \theta^+(i,\underset{\sim}{\mathcal{G}})\cdot\theta^-(i,\underset{\sim}{\tau})$. The path $\theta^{-1}\cdot\theta^+(i,\underset{\sim}{\mathcal{G}})\cdot L\cdot\theta^-(i,\underset{\sim}{\mathcal{G}})\cdot\theta$ is: conjugate (in the space of paths) to $\theta(i,\underset{\sim}{\mathcal{G}})$, and; homotopic to $\theta(i,\underset{\sim}{\tau})$. Therefore, $\breve{\tau}(i)$ and $\breve{\sigma}(i)$ are conjugate $\pi^1(U,P)$, and $\tau(i)$ and $\sigma(i)$ are conjugate in $G(\underset{\sim}{\mathcal{G}})$. ∎

Remark 1. Suppose $\underset{\sim}{\mathcal{G}}$ is a description of the branch cycles of (Y,φ), and $\underset{\sim}{\tau}$ is any r-tuple of elements of S_n satisfying: (1.8), and; $\prod_{i=1}^{r}\tau(i) = \mathrm{Id}$. It is

reasonable to ask if $\mathcal{T}$ is also a description of the branch cycles of (Y,φ). This is not true in general, though it is true in many important special cases (e.g., when φ has simple branching: see below). In fact, it is true iff the Hurwitz number of $\mathcal{C}$ is 1 (see Section 4B).

Lemma 1.2. Let $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ be a cover of projective non-singular curves such that the branch points of $\varphi(Z)$ are rational over a field L with $[L : \mathbb{Q}] < \infty$. Then there exists a cover $Z^\circ \xrightarrow{\varphi(Z^\circ)} \mathbb{P}^1$ with: Z° and $\varphi(Z^\circ)$ are defined over a field $L' \supset L$; $[L' : \mathbb{Q}] < \infty$, and; there exists an isomorphism $\alpha(Z^\circ) : Z^\circ \longrightarrow Z$ such that the diagram $\alpha(Z^\circ)$: $\begin{array}{ccc} Z^\circ & \longrightarrow & Z \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array}$ is commutative.

Note: We say that the cover (Z,φ) can be defined over L'.

Proof. Let M be a field, finitely generated over $\mathbb{Q}$, containing L and containing a field of definition of Z and of $\varphi(Z)$. Let θ be an absolutely irreducible algebraic variety defined over a field K with: $[K : \mathbb{Q}] < \infty$, and; the function field $K(\theta)$ is isomorphic to M. The construction of θ is easy to affect by: let K be the algebraic closure of $\mathbb{Q}$ in M; let $x_1,\dots,x_t$ be a transcendence basis for M over K; let $\beta \in M$ be a primitive generator for M over $K(x_1,\dots,x_t)$ such that β is integral over $K[x_1,\dots,x_t]$, and; let $f(x_1,\dots,x_t,Y) \in K[x_1,\dots,x_t,Y]$ be the polynomial for β over $K[x_1,\dots,x_t]$. It is easy now to describe θ as a hypersurface in affine $t+1$-space. Also, we easily describe a morphism $\mathcal{Z} \xrightarrow{\varphi(\mathcal{Z})} \theta \times \mathbb{P}^1$ such that there exists a Zariski open subset U of θ with: for $p \in U$ the fiber $\mathcal{Z}_p \xrightarrow{\varphi(\mathcal{Z}_p)} \mathbb{P}^1$ is a cover, and; for p^{gen} a generic point of U, there is an isomorphism $\alpha(\mathcal{Z}_{p^{gen}}) : \mathcal{Z}_{p^{gen}} \longrightarrow Z$ making the diagram $\alpha(\mathcal{Z}_{p^{gen}})$: $\begin{array}{ccc} \mathcal{Z}_{p^{gen}} & \longrightarrow & Z \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array}$ commutative.

Also we may assume $\mathcal{Z}$ and $\varphi(\mathcal{Z})$ are defined over K. Since K contains L, all the covers in the family $\mathcal{Z}\,|_U \longrightarrow U \times \mathbb{P}^1$ have the same branch points as

does $Z \xrightarrow{\varphi} \mathbb{P}^1$. Therefore, from Riemann's existence theorem, all the covers in this family are isomorphic.

We easily finish the proof of the lemma by taking a point $p^\circ \in U$ such that $[K(p^\circ) : \mathbb{Q}] < \infty$. Now take $Z^\circ \xrightarrow{\varphi(Z^\circ)} \mathbb{P}^1$ to be given by $\mathfrak{p} \xrightarrow{\varphi(\mathfrak{p}^\circ)} \mathbb{P}^1$. ■

Example 1: Simple Covers of $\mathbb{P}^1$.

We say that a cover $Y \xrightarrow{\varphi} \mathbb{P}^1$ of degree n is simple if the support of a fiber Y_φ consists of at least n-1 points for each $\mathfrak{p} \in \mathbb{P}^1$. Let $Y^{(n)}$ be the symmetric product of n copies of Y (as in 1.5)). Let $J^{(n)}$ be the connected component of the Picard scheme of Y representing divisors of degree n. Then we have a morphism

$$Y^{(n)} \xrightarrow{\psi^{(n)}} J^{(n)} \tag{1.10}$$

that maps each divisor of degree n to its linear equivalence class. Let $\mathcal{B}^1$ be the subset of $Y^{(n)}$ consisting of divisors $D = \sum_{i=1}^{t} m_i \cdot p_i$ ($p_1, \ldots, p_t$ distinct places of Y; $m_1, \ldots, m_t$ positive integers) for which $t \leq n - 1$, and let $\mathcal{B}^2$ be the subset of divisors D for which $t \leq n-2$. For $D \in Y^{(n)}$, the fiber $Y^{(n)}_{\psi^{(n)}(D)}$ consists of the positive divisors of degree n linearly equivalent to D. Therefore, this fiber has the structure of $\mathbb{P}^N(C)$ for some integer N. Consider a line L in this space, and let $f \in C(\bar{Y})$ be a function such that the divisor of f is the the difference of divisors corresponding to two distinct points on L. In addition, the cover $Y \xrightarrow{\varphi(f)} \mathbb{P}^1$ (where $\varphi(f)(\mathfrak{p}) = f(\mathfrak{p}) \in \mathbb{P}^1$ for $\mathfrak{p} \in Y$) is simple if $L \cap \mathcal{B}^2$ is empty. For n large such lines L exist. This follows from an argument of Severi modernized in [Fu]. The idea is that since $\mathcal{B}^2$ is of codimension 2 in $Y^{(n)}$ for n large, the intersection of $\mathcal{B}^2$ with the general fiber of $\varphi^{(n)}$ is of codimension 2([Mum; p. 93, Theorem 3]).

For a simple cover $Y \xrightarrow{\varphi} \mathbb{P}^1$, the monodromy group of the cover is S_n. In [Fr and Ja] it is shown that if Y is a non-singular projective curve defined over a field K (of 0 characteristic) then for n large there is a simple cover $Y \xrightarrow{\varphi} \mathbb{P}^1$ with (Y, φ) defined over K. □

Section 2. Arithmetic Theory of the Galois Closure of a Cover

Let F be a perfect field. Let $Y \xrightarrow{\varphi} X$ be a cover of non-singular projective curves such that Y, φ and X are defined over F. We assume also that φ is separable ($F(Y)/F(X)$ is a separable extension). As in Section (0.A) we let: $G(\widehat{F(Y)}/F(X))$ be the Galois group of the Galois closure $\widehat{F(Y)}$ of $F(Y)/F(X)$; $T(Y,X)$ is an associated permutation representation; and $\hat{F}$ the absolute constants of $\widehat{F(Y)}$.

Lemma 2.1. Let $T : G \to S_n$ be a faithful transitive permutation representation of the group G. Let $G(i) = \{\sigma \in G \mid (i)T(\sigma)=i\}$. Then $N(G(1))/G(1) \cong Cen_T(G)$ where: $N(G(1))$ is the normalizer of $G(1)$ in G; and $Cen_T(G)$ is the set of $\tau \in S_n$ such that $\tau\sigma\tau^{-1} = \sigma$ for all $\sigma \in G$.

Proof. The representation T is equivalent to the representation $T_{G(1)}$ (Section (0.B)). Let $G(1)g_1, \ldots, G(1)g_n$ be the right cosets of G(1) in G. The elements of G that permute these cosets under multiplication on the left are exactly the elements of $N(G(1))$. The elements that stabilize all these cosets are the elements of G(1). Therefore, $N(G(1))/G(1)$ acts faithfully by multiplication on the left of these cosets. Since G acts by multiplication on the right of these cosets this gives an embedding of $N(G(1))/G(1)$ in $Cen_T(G)$. Let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_k$ be the integers left invariant by all elements of G(1) (under T). For each integer j we show that there is a unique element $\tau \in Cen_T(G)$ such that

$$(1)\tau = \alpha_j;\ j = 1, \ldots, k.$$ In fact, consider the relations

$$\tau\, T(\sigma) = T(\sigma)\cdot\tau \text{ for } \sigma \in G, \text{ and } (1)\tau = \alpha_j. \tag{2.1}$$

For each integer ℓ we choose $\sigma \in G$ such that $(1)T(\sigma)=\ell$. Then, condition (2.1) determines $(\ell)\tau = (\alpha_j)T(\sigma)$, independent of the choice of σ. This shows the existence of τ. Therefore, the orders of $Cen_T(G)$ and $N(G(1))/G(1)$ are both equal to k. This establishes the isomorphism of these two groups. ∎

Lemma 2.2 Let $G = G(\widehat{F(Y)}/F(X))$ in the notation above. Then $\mathrm{Cen}_{T(Y,X)}(G)$ is isomorphic to $\mathrm{Aut}(Y,\varphi,F)$ (Section (0.C)). In particular, if $T(Y,X)$ is a primitive (e.g. doubly transitive) representation, and G is not a cyclic group of prime degree, then $\mathrm{Aut}(Y,\varphi,F) = \{\mathrm{Id.}\}$.

Proof. Let $y = y^{(1)}$ be a primitive generator of $F(Y)/F(X)$; $y^{(1)},\dots,y^{(n)}$ the conjugates of y over $F(X)$. If $\beta \in \mathrm{Aut}(Y,\varphi,F)$, then β gives a field automorphism of $F(X)(y^{(1)})$ which is determined by a polynomial $g(y) \in F(X)[y]$. In fact, we may take $g(y) \in F(X)[y]$ where $g(y)$ is the unique polynomial of degree at most n-1 such that $g(y^{(1)}) = \beta(y^{(1)})$. Therefore, the automorphisms of $F(X)(y^{(1)})$ can be identified with $N(G(1))/G(1)$. From Lemma (2.1), this identifies $\mathrm{Aut}(Y,\varphi,F)$ with $\mathrm{Cen}_{T(Y,X)}(G)$ (the proof gives a natural identification).

Suppose $T(Y,X)$ is a primitive representation and G is not a cyclic group of prime degree. Then there are no proper groups between $G(1)$ and G, and $N(G(1)) = G(1)$. From Lemma 2.1, $\mathrm{Aut}(Y,\varphi,F) = \{\mathrm{Id.}\}$. ■

Of prime concern is the exact sequence of groups:

$$1 \to G(\widehat{F(Y)}/\widehat{\overline{F}}(X)) \to G(\widehat{F(Y)}/F(X)) \xrightarrow{\text{rest.}} G(\hat{\overline{F}}/F) \to 1 \tag{2.2}$$

where rest. denotes the restriction of automorphisms of $F(Y)$ to F. Rest. is surjective in (2.2) because $\overline{F} \cap F(Y) = F$.

The middle term (respectively, the first term) of (2.2) is called the arithmetic monodromy (respectively, the geometric monodromy) group of the extension $F(Y)/F(X)$. Let $\mathcal{Y}_1,\dots,\mathcal{Y}_r$ be the places of $F(X)$ ramified in $F(Y)$. We fix the integer i. Let $\mathfrak{p}_i$ be a place of $\widehat{F(Y)}$ over the place $\mathcal{Y}_i$, and let $D(\mathfrak{p}_i)$ (respectively, $I(\mathfrak{p}_i)$) be the decomposition group (respectively, the inertial group) of $\mathfrak{p}_i/\mathcal{Y}_i$. If $\tau \in G(\widehat{F(Y)}/F(X))$ then we denote by $\tau(\mathfrak{p}_i)$ the places of $\widehat{F(Y)}$ obtained from:

$$\widehat{F(Y)} \xrightarrow{\tau^{-1}} \widehat{F(Y)} \xrightarrow{\mathfrak{p}_i} \overline{F} \cup \{\infty\} .$$

Then we have $\tau \cdot D(p_i) \cdot \tau^{-1}$ (respectively, $\tau \cdot I(p_i) \cdot \tau^{-1}$) equal to $D(\tau(p_i))$ (respectively, $I(\tau(p_i))$).

Let $n = [F(Y):F(X)]$. We identify $G(\widehat{F(Y)}/F(X))$ with its image in S_n under $T(Y,X)$. Let $G = G(\widehat{F(Y)}/\hat{F}(X))$; let $N_{S_n}(G)$ be the normalizer of G in S_n and ; let $F(\mathcal{Y}_i)$ denote the field generated (over F) by the values of (inhomogeneous) coordinates of the point on X corresponding to $\mathcal{Y}_i$. Then we have:

(2.3) $G(\hat{F}/\hat{F} \cap F(\mathcal{Y}_i))$ is a quotient group of $D(p_i)/I(p_i)$.

Let $I(Y,X)$ be the group of automorphisms of G obtained by inner action of $N_{S_n}(G)$ on G. We obtained a canonical map: $N_{S_n}(G) \xrightarrow{\psi} I(Y,X)$. Notice that ψ is injective if $Cen_{T(Y,X)}(G) = \{Id.\}$ (or $Aut(Y,\varphi) = \{Id.\}$ from Lemma 2.2).

Proposition 2. In the notation above, $G(\hat{F}/\hat{F} \cap F(\mathcal{Y}_i))$ can be identified with a quotient of a subgroup of $N_{S_n}(I(p_i))/I(p_i)$. Suppose, in addition, that

(2.4) G has no center.

Then, $G(\widehat{F(Y)}/F(X))$ can be identified with a subgroup of $I(Y,X)$. Equivalently, ψ applied to $G(\widehat{F(Y)}/F(X))$ is injective.

Proof. Since $D(p_i)$ is a subgroup of $N_{S_n}(I(p_i))$ the first part of the proposition follows from (2.3).

Let $\hat{Y} \xrightarrow{\hat{\varphi}} X$ be a cover of absolutely irreducible curves over $\hat{F}$ such that $\hat{F}(\hat{Y})/\hat{F}(X)$ is isomorphic (as an extension of fields) to $\widehat{F(Y)}/\hat{F}(X)$. Let H be the subset of elements $\tau \in G(\hat{F}/F)$ such that τ is the restriction of an element $\hat{\tau} \in G(\widehat{F(Y)}/F(X))$ with the following property: there exists $\gamma \in G(\widehat{F(Y)}/\hat{F}(X))$ with

(2.5) $\gamma \cdot \sigma \cdot \gamma^{-1} = \hat{\tau}^{-1} \cdot \sigma \cdot \hat{\tau}$ for all $\sigma \in G(\widehat{F(Y)}/\hat{F}(X))$.

The existence of γ does not depend on the choice of $\hat{\tau}$, and from (2.4), γ is unique for a given choice of $\hat{\tau}$. It is obvious that H is a

subgroup of $G(\hat{F}/F)$. The conclusion of the proposition follows if we show that $H = \{\mathrm{Id.}\}$.

To show this we let F° be the fixed field of H. We show that there is a Galois cover $Y^\circ \xrightarrow{\varphi^\circ} X$ (of projective non-singular curves) such that:

(2.6) a) Y° and φ° are defined over F°;

b) there exists $Y^\circ \xrightarrow{\Phi^\circ} Y$ with $\varphi \cdot \Phi^\circ = \varphi^\circ$; and

c) $Y^\circ \otimes \hat{F} \xrightarrow{\varphi^\circ \otimes \mathrm{Id.}} X$ is isomorphic (as a cover by $\Phi \otimes \mathrm{Id.}$) to $\hat{Y} \to X$.

Therefore, $F^\circ(Y) \subset F^\circ(Y^\circ) \subset \widehat{F(Y)}$, and $F^\circ(Y^\circ)/F^\circ(X)$ is a Galois extension containing $F^\circ(Y)$. However, since $\widehat{F(Y)}$ is the Galois closure of $F^\circ(Y)/F^\circ(X)$, we have: $F^\circ(Y) = \widehat{F(Y)}$; or $F^\circ = \hat{F}$; or $H = \{\mathrm{Id.}\}$.

We have reduced the proposition to establishing the conditions of expression (2.6).

Again let $\tau \in H$. Let $\hat{y}$ be a primitive generator of $\widehat{F(Y)}/F(X)$ (i.e., $\widehat{F(Y)} = F(X)(\hat{y})$). Let $s(\underset{\sim}{x}, \hat{y})$ be a generic point of $\hat{Y}$, where $s(\underset{\sim}{x}, \hat{y})$ denotes a tuple of rational functions in the coordinates of a generic point $\underset{\sim}{x}$ of X and $\hat{y}$. As above, $\hat{\tau}$ is an element of $G(\widehat{F(Y)}/F(X))$ whose restriction to $\hat{F}$ is τ. Each $\sigma \in G(\widehat{F(Y)}/F(X))$ is represented by $g_\sigma(y) \in F(X)[y]$ so that $\sigma(\hat{y}) = g_\sigma(\hat{y})$. Apply τ to the covers $\hat{Y} \xrightarrow{\hat{\Phi}} Y \xrightarrow{\varphi} X$ to obtain $\hat{Y}^\tau \xrightarrow{\hat{\Phi}^\tau} Y \xrightarrow{\varphi} X$. Then, $s(\underset{\sim}{x}, \hat{\tau}(\hat{y}))$ is a generic point of $\hat{Y}^\tau$.

For $\sigma \in G(\widehat{F(Y)}/\hat{F}(X))$ let $\sigma^* : \hat{Y} \to \hat{Y}$ be the morphism such that σ^* applied to the generic point $s(\underset{\sim}{x}, \hat{y})$ is $s(\underset{\sim}{x}, g_\sigma(\hat{y}))$. Similarly, let $\hat{\tau}^* : \hat{Y} \to \hat{Y}^\tau$ be the morphism such that $\hat{\tau}^*(s(\underset{\sim}{x}, \hat{y})) = s(\underset{\sim}{x}, \hat{\tau}(\hat{y}))$. Then $(\sigma^*)^\tau : \hat{Y}^\tau \to \hat{Y}^\tau$ maps the generic point $s(\underset{\sim}{x}, \hat{\tau}(\hat{y}))$ to $s(\underset{\sim}{x}, g_\sigma(\hat{\tau}(\hat{y})))$. Therefore, (2.5) translates to

$$(2.7) \qquad (\hat{\tau}^*)^{-1} \cdot (\sigma^*)^\tau \cdot \hat{\tau}^* = \gamma^* \cdot \sigma^* \cdot (\gamma^*)^{-1}.$$

Let $\hat{\tau}^* \cdot \gamma^* = \theta_\tau^*$, so $\theta_\tau^* : \hat{Y} \to \hat{Y}^\tau$ and

$$(2.8) \qquad (\theta_\tau^*)^{-1} \cdot (\sigma^*)^\tau \cdot \theta_\tau^* = \sigma^*.$$

From the uniqueness of θ^*_τ (which comes from (2.4)) we obtain the

cocycle condition: $(\theta^*_{\tau_1})^{\tau_2} \cdot \theta^*_{\tau_2} = \theta^*_{\tau_1 \cdot \tau_2}$ for $\tau_1, \tau_2 \in H$.

From Weil's cocycle criteria for reducing the field of definition of a variety ([We]) there exists Y^o and φ^o satisfying (2.6) a), b) and c). However, it does not immediately follow that Y^o is a Galois cover of X. Let

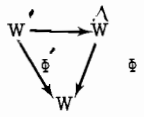
$$\psi : \begin{array}{ccc} Y^o & \longrightarrow & \hat{Y} \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

be the birational map (defined over $\hat{F}$) given by (2.6)c) such that $\psi^\tau \cdot \psi^{-1} = \theta^*_\tau$. Then for $\sigma^* \in \mathrm{Aut}(\hat{Y},\hat{\varphi})$ we obtain an automorphism $\psi^{-1} \cdot \sigma^* \cdot \psi \in \mathrm{Aut}(Y^o,\varphi^o)$. We check, using condition (2.8) that $\psi^{-1} \cdot \sigma^* \cdot \psi$ is transformed into itself by the action of $G(\hat{F}/F^o)$. The cycle $\psi^{-1} \cdot \sigma^* \cdot \psi$ is, therefore, defined over F^o ([We,2; p.15, theorem 3]). In characteristic zero, this can be seen by a trivial average process applied to the polynomials defining the ideal of the cycle $\psi^{-1} \cdot \sigma^* \cdot \psi$ in its ambient projective space. $\mathrm{Aut}(\hat{Y},\hat{\varphi})$ is isomorphic to $\mathrm{Aut}(Y^o,\varphi^o,F^o)$, and $Y^o \xrightarrow{\varphi^o} X$ is a Galois cover. This establishes our proposition as indicated above. ■

We note that in the special case that all automorphisms of G are inner and T(Y, X) is the regular representation of G, a part of Proposition 2 is due to Shimura and Shih [Shih].

We make some comments on the process of going to the Galois closure for the fibers of a smooth family of curves covering a given curve X. We say that an algebraic set W is an F-variety if: W is defined over F, and; W is not the union of two non-empty algebraic sets defined over F. Let $W \xrightarrow{\varphi} V$ be a separable cover of (normal) F-varieties.

Lemma 2.3. *There exists a unique Galois cover $\hat{W} \xrightarrow{\hat{\varphi}} V$ of F-varieties having the following properties: $\hat{W} \xrightarrow{\Phi} W$ is a cover of F-varieties; $\hat{\varphi} = \varphi \cdot \Phi$; if $W' \xrightarrow{\Phi'} W$ is a cover of F-varieties such that $W' \xrightarrow{\varphi \cdot \Phi'} V$ is a Galois cover, then there exists a unique diagram,*



such that this induces the inclusion of $F(\hat{W})$ into $F(W')$.

Proof. Apply the argument of [Mum; p. 396-397] to the inclusion of $F(W)$ into $\widehat{F(W)}$ (the Galois closure of $F(W)/F(V)$). Then $\hat{W}$ is the normalization of W in $\widehat{F(W)}$. ∎

Let $\mathfrak{Z}$ be a proper and smooth family of irreducible curves covering a fixed curve X, defined over F. That is, $\mathfrak{Z}$ consists of: $\mathcal{Y} \xrightarrow{\Phi} \mathcal{O} \times X \xrightarrow{pr_1} \mathcal{O}$; $\xrightarrow{pr_2} X$

$\mathcal{Y}$ and $\mathcal{O}$ are normal varieties; $\mathcal{Y}$, Φ, and $\mathcal{O}$ are defined over F; $pr_1 \cdot \Phi$ is smooth and $\mathcal{Y}_{\underline{p}} \xrightarrow{pr_2 \cdot \Phi} X$ is a cover of connected, non-singular, projective curves for $\underline{p} \in \mathcal{O}$.

Warning!! Although $\mathcal{Y}_{\underline{p}}$, $pr_2 \cdot \Phi$, and X are defined over $F(\underline{p})$, it is possible that they are defined over a field properly contained in $F(\underline{p})$. When we form the fiber of Φ over $\underline{p}$, in actuality we obtain $\mathcal{Y}_{\underline{p}} \xrightarrow{\Phi_{\underline{p}}} \underline{p} \times X$; a diagram whose minimal field of definition is $F(\underline{p})$. This point arises in a crucial way in Section 5 where we are concerned with $\mathcal{Y}_{\underline{p}} \to X$ induced from projection of $\underline{p} \times X$ to X.

Definition: Let $\mathfrak{Z}$ be a family as above. Let η be a generic point of $\mathcal{O}$. So $F(\eta)$ is isomorphic to $F(\mathcal{O})$. Let $\hat{F}(\mathcal{O})$ be the algebraic closure of $F(\mathcal{O})$ in $\widehat{F(\mathcal{Y}_\eta)}$ (the Galois closure of $F(\mathcal{Y}_\eta)/F(\eta \times X)$. We call $\hat{F}(\mathcal{O})$ the extension of constants field for the family $\mathfrak{Z}$. Let $\hat{F}_{fix}(\mathcal{O})$ (the fixed component of the extension of constants) be the field $\overline{F} \cap \hat{F}(\mathcal{O})$.

One of the central problems related to the subject matter of this article is the determination of the extension of constants field for the Hurwitz families described in Sections 3 and 4 (see [Fr and L; Chap. VII] or [Fr, 1]). Section 3 of [Fr,1] contains a reasonably definitive conjecture on an explicit description of the extension of constant fields.

Section 3. Families of Covers of $\mathbb{P}^1$: Hurwitz Families and Symmetrized Hurwitz Families

In this section the ground field is $\mathbb{C}$. Consider a cover $Y \xrightarrow{\varphi} \mathbb{P}^1$ of non-singular, projective curves, where $u(1)^{(o)},\dots,u(r)^{(o)} \in \mathbb{P}^1$ is a collection of points containing the branch points of φ, and $\sigma(1),\dots,\sigma(r)$ are a description of the branch cycles of φ (Section (1.B)). We remind that $\sigma(i)$ is a generator of the inertial group for some prime $\mathfrak{p}$ of $\hat{\mathbb{C}}(Y)$ (Galois closure of $\mathbb{C}(Y)/\mathbb{C}(X)$) over $u(i)^{(o)}$, $i = 1,\dots,r$. Let n be deg (φ) and let $\mathfrak{u}^{(o)} = (u_1^{(o)},\dots,u_r^{(o)})$. We describe three objects related to the cover $Y \xrightarrow{\varphi} \mathbb{P}^1$:

(3.1)a) $\mathcal{H}(Y,\varphi;r)$, Parameter space for deformations of $Y \xrightarrow{\varphi} \mathbb{P}^1$ (or Hurwitz parameter space);

b) $\mathfrak{I}^{\mathrm{symm}}(Y,\varphi;r)$, a symmetrized Hurwitz family, and

c) $\mathfrak{I}(Y,\varphi;r,\mathfrak{u}^{(o)})$, a Hurwitz family.

Most of the remainder of this section is consecrated to the description of these objects by their relevant properties (constructions appear in Section 4). The reader may benefit from example 2 where the cases $r = 2$ and $r = 3$ are worked out in detail. Unfortunately, even when the families (3.1)b) and c) exist, they may not be unique. However, as we show, a simple Cech cohomology theory classifies these. Hurwitz considered (3.1)a) and b) in the case of simple branching [Hu] and [Fu]; (see example 1). For $n > 2$, S_n is doubly transitive. Since the monodromy group of a simple cover is S_n (see example 1) $\mathrm{Aut}(Y,\varphi) = \{\mathrm{Id.}\}$ (Lemma 2.2). From this will follow the existence and uniqueness of (3.1)b) and (3.1)c).

Let A be a Zariski open subset of $\mathbb{P}^1(\mathbb{C})$. Let U_{A^r} be the collection of r unordered, distinct points of A. Then U_{A^r} can be regarded as a functor in A. We give another description of U_{A^r}. Let: $\Delta(A)$ be the diagonal in $A \times A$; $\pi_i : \underbrace{A \times A \times \dots \times A}_{r \text{ times}} \to A$ the projection onto the i-th factor;

$\Delta(i,j:A) = (\pi_i \times \pi_j)^{-1}(\Delta(A))$, and,

$$U_A^r \overset{\text{def}}{=} \underbrace{A \times A \times \ldots \times A}_{r \text{ times}} - \bigcup_{\substack{i<j \\ i=1,j=1}}^{i=r,j=r} \Delta(i,j:A).$$

The symmetric group S_r acts on U_A^r by permuting the coordinates, and $U_{A^r} = U_A^r/S_r$.

Let $\mathcal{O}(r)$ be the collection of pairs consisting of: the isomorphism class of a cover of $\mathbb{P}^1$, and; a collection of r distinct points containing the branch points of this cover. We put a topology on $\mathcal{O}(r)$ (complex topology) as follows. Regard $\underset{\sim}{p},\underset{\sim}{p}' \in \mathcal{O}(r)$ as "close" if $\underset{\sim}{p}$ (respectively $\underset{\sim}{p}'$) is represented by $Y \xrightarrow{\varphi} \mathbb{P}^1$ (respectively $Y' \xrightarrow{\varphi'} \mathbb{P}^1$) where: the associated r points of φ and φ' are "close", and Y is a C^∞ trivial deformation of Y' through covers of $\mathbb{P}^1$ by a "small" deformation of the branch points. In Section 4 we will show that $\mathcal{O}(r)$ is a complex manifold. Let $\mathcal{O}(Y,\varphi;r)$ be the connected component of $\mathcal{O}(r)$ containing the isomorphism class corresponding to $Y \xrightarrow{\varphi} \mathbb{P}^1$. Also, by associating to $\underset{\sim}{p} \in \mathcal{O}(r)$ the unordered collection of r points in the second coordinate of $\underset{\sim}{p}$ we obtain a map $\mathcal{O}(Y,\varphi;r) \to U_{\mathbb{P}^r}$. In Section 4 we endow $\mathcal{O}(Y,\varphi;r)$ with the unique structure that will make this map an unramified cover. Fulton [Fu] calls $\mathcal{O}(Y,\varphi;r)$ (in the simple branching case, anyway) the Hurwitz scheme (over $\mathbb{C}$). However, since all significant computations must consider the total family of covers, we prefer our naming system. Fulton's motivation is to represent a certain functor (isomorphism classes of simple branched covers of $\mathbb{P}^1$) and therefore in his situation $\mathcal{O}(Y,\varphi;r)$ is the set of complex points of a representing scheme for this functor. Let $G \subset S_n$ be a transitive subgroup of S_n for which $\text{Cen}_{S_n}(G)$ (the centralizer of G in S_n) is the identity group. Let $\mathcal{O}(G,r)$ be the collection of triples $(Y,\varphi,\underset{\sim}{u})$ where: $Y \xrightarrow{\varphi} \mathbb{P}^1$ is a cover of projective non-singular curves with monodromy group G, and $\underset{\sim}{u} = (u(1),\ldots,u(r))$ is a collection of r points of $\mathbb{P}^1$ containing the branch points of φ. Since $\text{Cen}_{S_n}(G) = \{\text{Id.}\}$, Lemma 2.2 shows that $\text{Aut}(Y,\varphi) = \{\text{Id.}\}$. In this case the considerations of [Fu] are applicable. In particular, the total family (3.1)b) has good reduction (smooth and proper) to those positive characteristics which do not divide the

order of G. In the general case, however, when $\mathrm{Cen}_{S_n}(G) \neq \{\mathrm{Id.}\}$ the universal property for (3.1)b) must be more subtly phrased: and even with this rephrasing, existence of (3.1)b) is a more delicate property.

We ask that (3.1)b) have the following properties:

(3.2)a) $\mathcal{J}^{\mathrm{symm}}(Y,\varphi;r) \xrightarrow{\Phi^{\mathrm{symm}}} \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$

is a cover of complex algebraic varieties, and;

b) for $\underline{p} \in \mathcal{O}(Y,\varphi;r)$ the fiber $(\mathcal{J}^{\mathrm{symm}}(Y,\varphi;r))_{\underline{p}} \xrightarrow{\mathrm{pr}_2 \circ \Phi^{\mathrm{symm}}} \mathbb{P}^1$ is a cover of non-singular projective curves representing the isomorphism class $\underline{p}$.

Due to the presence of automorphisms in the fibers, $\mathcal{J}^{\mathrm{symm}}(Y,\varphi;r)$ is not expected to be unique. However, if such a structure exists (satisfying (3.2)a) and b) it is versal for the étale topology. We explain this for our situation.

Let $\mathcal{Y} \to \mathcal{O}' \times \mathbb{P}^1$ be a connected, proper, smooth family of curves covering $\mathbb{P}^1$ as in the discussion following Lemma 2.3. Suppose for $\underline{p} \in \mathcal{O}'$, $Y_{\underline{p}} \to \mathbb{P}^1$ is in the isomorphism class of $\underline{p}^* \in \mathcal{O}(Y,\varphi;r)$. Then there exists: a neighborhood U of $\underline{p}$ (in the complex topology, or the etale topology), and; a unique map $U \xrightarrow{\Psi} \mathcal{O}(Y,\varphi;r)$ such that $\mathcal{Y}|_U \to U \times \mathbb{P}^1$ is isomorphic (as a cover) to

$$U \times_{\mathcal{O}(Y,\varphi;r)} \mathcal{J}^{\mathrm{symm}}(Y,\varphi;r) \to U \times \mathbb{P}^1.$$

Assume that $\mathcal{J}^{\mathrm{symm}}(Y,\varphi;r)$ exists (has properties (3.2)a) and b)). We describe a sheaf of groups $\mathrm{AUT}(Y,\varphi;r)$ on $\mathcal{O}(Y,\varphi;r)$. If U is an open set of $\mathcal{O}(Y,\varphi;r)$ in the complex topology, (it does not suffice to consider the Zariski topology) then $\mathrm{AUT}(Y,\varphi;r)(U)$ is the group consisting of automorphisms

$$\alpha : \mathcal{J}^{\mathrm{symm}}(Y,\varphi;r)|_U \to \mathcal{J}^{\mathrm{symm}}(Y,\varphi;r)|_U$$

(commutative triangle: both maps over $U \times \mathbb{P}^1$).

For an open set $V \subset U$, $\mathrm{AUT}(Y,\varphi;r)(U) \xrightarrow{\mathrm{rest.}\ (V,U)} \mathrm{AUT}(Y,\varphi;r)(V)$ is the

restriction of an automorphism. This presheaf is obviously a sheaf. It is now a standard computation to show that the elements of the Cech cohomology set $H^1(\mathcal{O}(Y,\varphi;r), \mathrm{AUT}(Y,\varphi;r))$ are in 1-1 correspondence with the isomorphism classes of covers $\mathfrak{Z} \to \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$ having the properties (3.2)a) and b) (with $\mathfrak{Z}^{symm}(Y,\varphi;r)$ replaced by $\mathfrak{Z}$).

Even for the most general applications (that we have considered) it is not the existence but rather the stable existence of symmetrized Hurwitz families that is so crucial. That is, we regard r branch points as r+s branch points by adding s branch points (arbitrarily) to the considerations above. Then we ask if $\mathfrak{Z}^{symm}(Y,\varphi;r+s)$, satisfying (3.2)a) and b) with r replaced by r+s, exists for s large.

Since it is difficult to work directly with the objects (3.1)b), we consider Hurwitz families $\mathfrak{Z}(Y,\varphi;r,\underset{\sim}{u}^{(0)})$ in the constructions of Section 4.A. We describe these now in the case when $\mathfrak{Z}^{symm}(Y,\varphi;r)$ exists.

All objects satisfying (3.2)b) are "twistings"; $\mathcal{J}^{symm}(Y,\varphi;r)(\psi)$ of $\mathcal{J}^{symm}$ for $\psi \in H^1(\mathcal{O}(Y,\varphi;r), \mathrm{AUT})$. We explain this. Since $\mathcal{J}^{symm}$ is versal for the complex (resp. etale) topology, any object satisfying (3.2)b) is locally (on the base $\mathcal{O}(Y,\varphi;r)$) isomorphic to $\mathcal{J}^{symm}(Y,\varphi;r)$ restricted to an open set of the base. Since AUT is the sheaf of local automorphisms of $\mathcal{J}^{symm}$ over $\mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$ we can now apply the well-known dictionary between twisted forms of $\mathcal{J}^{symm}(Y,\varphi;r)$ and elements of $H^1(\mathcal{J}^{symm},\varphi;r)$, AUT).

We have canonical maps: $\mathcal{O}(Y,\varphi;r) \xrightarrow{\pi} U_{\mathbb{P}^r}$ and $U^r_{\mathbb{P}} \to U_{\mathbb{P}^r}$, so we may form $\mathcal{Y} = \mathcal{J}^{symm}(Y,\varphi;r) \times_{U_{\mathbb{P}^r}} U^r_{\mathbb{P}}$. The direct image sheaf π_* (AUT) acts on π_* ($\mathcal{J}^{symm}$) regarded as family of covers $\mathbb{P}^1$ over the parameter space $U_{\mathbb{P}^r}$. Thus, if we pull back π_*(AUT) to $U^r_{\mathbb{P}}$ a direct factor of this sheaf of groups acts effectively on a connected component of the pull-back of $\pi_*(\mathcal{J}^{symm})$ to $U^r_{\mathbb{P}}$. The twistings of $\mathcal{J}$ by elements of the first cohomology set with coefficients in this sheaf give the structures of type (3.1)c). Our main constructions consider first the existence of $\mathcal{J}(Y,\varphi;r,\underset{\sim}{u}^{(o)})$ (see the definition at the beginning of Section 4). Under certain conditions we may then proceed to the construction of $\mathcal{J}^{symm}(Y,\varphi;r)$, which unfortunately does not always exist even when $\mathcal{J}(Y,\varphi;r,\underset{\sim}{u}^{(o)})$ does exist.

Example 2. Hurwitz Families and Symmetrized Hurwitz Families in the case r=2 or 3.

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover of projective, non-singular curves equipped with an ordered triple of points of $\mathbb{P}^1$, containing among them the branch points of φ. For simplicity we assume these designated points are $u(1)^{(0)} = 0$, $u(2)^{(0)} = 1$, $u(3)^{(0)} = \infty$. First we show that Hurwitz families always exist in this case. Again, for simplicity, assume that Y is a non-singular curve in $\mathbb{P}^2(\mathbb{C})$. Then Y may be represented as the points on: $f(x,y,z) = 0$ where f is a homogeneous polynomial in the homogeneous coordinates x, y, z for $\mathbb{P}^2(\mathbb{C})$, and φ is given by projection on the x, z coordinates. Let u(1), z(1); u(2), z(2); u(3), z(3) be pairs of homogeneous coordinates for 3 copies of $\mathbb{P}^1$. Consider:

$$(3.3)\qquad ((z(3)\cdot x - z\cdot u(3))(z(1)\cdot u(2) - z(2)\cdot u(1))^n f\left(X, \frac{y}{z(3)\cdot x - z\cdot u(3)}, \frac{z}{z(3)\cdot x - z\cdot u(3)}\right)$$

where $X = \left(\frac{z(1)\cdot x - z\cdot u(1)}{z(3)\cdot x - z\cdot u(3)}\right)$ $\left(\frac{u(2)\cdot z(3) - u(3)\cdot z(2)}{z(1)\cdot u(2) - 3(2)\cdot u(1)}\right)$ and deg f = deg φ = n.

where deg f = deg φ = n. We call this the family generated by $Y \xrightarrow{\varphi} \mathbb{P}^1$.

From expression (3.3) we obtain:

$\mathfrak{J} = \mathfrak{J}(Y, \varphi; r, (o, 1, \infty)) \xrightarrow{\Phi} U^3_{\mathbb{P}} \times \mathbb{P}^1$ where, for $\underset{\sim}{p} \in U^3_{\mathbb{P}}$ the fiber $(\mathfrak{J}(Y, \varphi; r, (0, 1, \infty)))_{\underset{\sim}{p}}$ is the expression (3.3) with $\frac{u(1)}{z(1)}$, $\frac{u(2)}{z(2)}$, and $\frac{u(3)}{z(3)}$ replaced by the (respective) coordinates of $\underset{\sim}{p}$. This is a Hurwitz family as can be seen by the characterization in Section 4. The main point is that $\mathfrak{J}$ is a connected manifold covering $U^3_{\mathbb{P}} \times \mathbb{P}^1$ such that the connected components of the fiber $\mathfrak{J}_{\underset{\sim}{p}}$ (for $\underset{\sim}{p} \in U^3_{\mathbb{P}}$) are pairwise non-isomorphic as covers of $\mathbb{P}^1$. In this case, each fiber has exactly one connected component, so this condition is trivially satisfied. As long as we have (3.3) in front of us, let's make an observation on the completion of $\mathfrak{J}$ in its ambient projective space. As we will observe in Section 4, $\mathfrak{J}$ has a completion to a unique normal, projective variety $\mathfrak{J}^*$, fibered over $(\mathbb{P}^1)^r$ (where r=3 in this example). It is easy to deduce that $\mathfrak{J}^*(Y, \varphi; r, (0,1,\infty))$ has 'very' degenerate fibers over the branch locus of $\Phi^* : \mathfrak{J}^* \to (\mathbb{P}^1)^3 \times \mathbb{P}^1$. In fact,

let $(\sigma(1),\sigma(2),\sigma(3))$ be a description of the branch cycles (corresponding respectively to the points $0,1,\infty$) of (Y,φ). Let $v(i)$ be the number of disjoint cycles in $\sigma(i)$ (regarded as an element of S_n); $i = 1,2,3$. Over the $\frac{u(2)}{z(2)} = \frac{u(3)}{z(3)}$ locus, the fibers of $\mathfrak{Z}^*$ consist of $v(1)$ copies of $\mathbb{P}^1(\mathbb{C})$ (as covers of $\mathbb{P}^1$) joined together over the place $\frac{u(2)}{z(2)}$ on $\mathbb{P}^1$. This can be seen by an inspection of (3.3). We can similarly describe the fibers over the $\frac{u(1)}{z(1)} = \frac{u(3)}{z(3)}$ and $\frac{u(1)}{z(1)} = \frac{u(2)}{z(2)}$ loci. In other words, the fibers of $\mathfrak{Z}^*$ over the $\frac{u(2)}{z(2)} = \frac{u(3)}{z(3)}$ locus are <u>not</u> covers of $\mathbb{P}^1$ with branch cycles $(\tau(1),\tau(2))$ where $\tau(1) = \sigma(1)$ and $\tau(2) = \sigma(2)\cdot\sigma(3)$, as would be expected from 'coelescing of branch cycles'. For more on the description of the completion $\mathfrak{Z}^*$ of Hurwitz families (over the branch locus) see [Fr,2].

Now we consider the construction of a symmetrized Hurwitz family (properties (3.2)a) and b)) containing (Y,φ). For $\sigma \in S_3$, denote also by σ the morphism

$$U^3_{\mathbb{P}} \to U^3_{\mathbb{P}} \text{ where } \sigma\left(\frac{u(1)}{z(1)}, \frac{u(2)}{z(2)}, \frac{u(3)}{z(3)}\right) = \left(\frac{u((1)\sigma)}{z((1)\sigma)}, \frac{u((2)\sigma)}{z((2)\sigma)}, \frac{u((3)\sigma)}{z((3)\sigma)}\right)$$

Let $(\sigma \times \mathrm{Id})^*(\mathfrak{Z})$ be the Cartesian product in the diagram

$$\begin{array}{ccc} (\sigma \times \mathrm{Id})^*(\mathfrak{Z}) & \longrightarrow & \mathfrak{Z} \\ \downarrow{\scriptstyle \Phi'} & & \downarrow{\scriptstyle \Phi} \\ U^3_{\mathbb{P}} \times \mathbb{P}^1 & \xrightarrow{\sigma \times \mathrm{Id}.} & U^3_{\mathbb{P}} \times \mathbb{P}^1 \end{array}$$

Let H be the group consisting of elements σ of S_3 such that there is an isomorphism $\psi : (\sigma \times \mathrm{Id})^*(\mathfrak{Z}) \to \mathfrak{Z}$ with

(3.4)
$$\begin{array}{ccc} (\sigma \times \mathrm{Id}.)^*(\mathfrak{Z}) & \xrightarrow{\psi} & \mathfrak{Z} \\ & {\scriptstyle \Phi'} \searrow \quad \swarrow {\scriptstyle \Phi} & \\ & U^3_{\mathbb{P}} \times \mathbb{P}^1 & \end{array} \qquad \text{(commutative triangle).}$$

We now show that in <u>the special case of this example</u>: H is the subgroup of S_3 consisting of σ such that for $p \in U^3_{\mathbb{P}}$ there is an isomorphism

(3.5)
$$\begin{array}{ccc} & \theta_p : \mathfrak{Z}_p & \longrightarrow \mathfrak{Z}_{\sigma(p)} \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array} \qquad \text{(commutative triangle).}$$

In fact, let $\underset{\sim}{p} \in U^3_{\mathbb{P}}$, and let $\sigma \in S_3$ be such that we have the diagram (3.5). We return to the expression (3.3) to prove that this necessary condition is sufficient.

For $\underset{\sim}{p} \in U^3_{\mathbb{P}}$ let $u(1,\underset{\sim}{p}), u(2,\underset{\sim}{p}), u(3,\underset{\sim}{p})$ (respectively) be the coordinates of $\underset{\sim}{p}$. Then, for $\underset{\sim}{p},\underset{\sim}{p}' \in U^3_{\mathbb{P}}$, there exists a unique Möbius transformation, $\tau_{\underset{\sim}{p}',\underset{\sim}{p}}(u(i,\underset{\sim}{p})) = u(i,\underset{\sim}{p}')$, $i = 1,2,3$. We write this as: $\tau_{\underset{\sim}{p}',\underset{\sim}{p}}(\underset{\sim}{p}) = \underset{\sim}{p}'$. In particular,

(3.6) $U^3_{\mathbb{P}}$ is complex analytically isomorphic to $\text{Möb} \overset{\text{def}}{=} SL(2,\mathbb{C})/\{\pm I\}$.

From transport of structure (3.5) implies that there exists a commutative triangle

$$\theta_{\tau(\underset{\sim}{p})} : \mathfrak{I}_{\tau(\underset{\sim}{p})} \to \mathfrak{I}_{\tau(\sigma(\underset{\sim}{p}))}$$
$$\mathbb{P}^1$$

We choose τ such that $\tau(\underset{\sim}{p}) = (0,1,\infty)$. We apply the construction (3.3) simultaneously to the members of this commutative triangle as in (3.4) where: the family generated by $\mathfrak{I}_{\tau(\sigma(\underset{\sim}{p}))} \to \mathbb{P}^1$ is identified with $(\sigma \times \text{Id.})^*(\mathfrak{I}) \xrightarrow{\Phi'} U^3_{\mathbb{P}} \times \mathbb{P}^1$; and ψ is the isomorphism generated by $(\theta_{\tau(\underset{\sim}{p})})^{-1}$. Then by direct computation we see that for each $\underset{\sim}{p} \in U^3_{\mathbb{P}}$,

(3.7) $\text{Aut}(\mathfrak{I}_{\underset{\sim}{p}}/\mathbb{P}^1) = \text{Aut}(\mathfrak{I}/U^3_{\mathbb{P}} \times \mathbb{P}^1)$ ($\mathfrak{I}$ has a full set of automorphisms).

Let G be the group of automorphisms of $\mathfrak{I}$ such that: if $\tau \in G$, there exists $\sigma \in H$ with a commutative diagram.

$$\begin{array}{ccc} \mathfrak{I} & \xrightarrow{\tau} & \mathfrak{I} \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ U^3_{\mathbb{P}} \times \mathbb{P}^1 & \xrightarrow{\sigma \times \text{Id.}} & U^3_{\mathbb{P}} \times \mathbb{P}^1 \end{array}$$

Then we have an exact sequence

(3.8) $1 \to \text{Aut}(\mathfrak{I}/U^3_{\mathbb{P}} \times \mathbb{P}^1) \to G \xrightarrow{\beta} H \to 1$

We show that the following two statements are equivalent:

(3.9)a) the sequence (3.8) splits, and;

b) there is a symmetrized Hurwitz family

$\mathfrak{I}^{symm} \to U_{\mathbb{P}^3} \times \mathbb{P}^1$ such that $\mathfrak{I} \to U^3_{\mathbb{P}} \times \mathbb{P}^1$ is a connected component of $\mathfrak{I}^{symm} \times_{U_{\mathbb{P}^3}} U^3_{\mathbb{P}}$ (as previously).

Since $\mathcal{P}(Y,\varphi;r)$ consists of isomorphism classes of covers of $\mathbb{P}^1$ (equipped with a triple of points on $\mathbb{P}^1$ containing the branch points of the cover), we easily see that $\mathcal{P}(Y,\varphi;r)$ is isomorphic to $U^3_{\mathbb{P}}/H$. If the sequence (3.8) splits, then there exists a subgroup $\tilde{H} \subseteq G$ such that $\tilde{H} \xrightarrow{\beta} H$ is an isomorphism. Therefore, we have the quotient $\mathfrak{I}/\tilde{H} \to (U^3_{\mathbb{P}}/H) \times \mathbb{P}^1 = \mathcal{P}(Y,\varphi;r) \times \mathbb{P}^1$. From properties (3.2)a) and b) we see that $\mathfrak{I}/\tilde{H} = \mathfrak{I}^{symm}$ is, indeed, a symmetrized Hurwitz family. On the other hand, if (3.9)b) holds, then $\mathfrak{I}^{symm}$ is easily seen to be a quotient of $\mathfrak{I}$ by a group $\tilde{H} \subseteq G$ such that $\beta : \tilde{H} \to H$ is surjective.

We deduce that in the case r=3 Symmetrized Hurwitz families containing $Y \xrightarrow{\varphi} \mathbb{P}^1$ exist if (3.8) splits. In particular, this is so if $(|Aut(Y/\mathbb{P}^1)|, |H|) = 1$. (lemma of Zassenhaus and Schur; [Za]).

Two quick observations! Since $SL(2,\mathbb{C})$ is a simply connected manifold, (3.6) implies that the fundamental group of $U^3_{\mathbb{P}}$ is $\mathbb{Z}/(2)$. In the case when r=2, a Hurwitz family is represented by a cover $\mathfrak{I} \to U^2_{\mathbb{P}} \times \mathbb{P}^1$. We have $U^3_{\mathbb{P}} = U^2_{\mathbb{P}} \times \mathbb{P}^1 - \Delta(1,3) - \Delta(2,3)$. Thus, $\mathfrak{I}|_{U^3_{\mathbb{P}}} \to U^3_{\mathbb{P}}$ is an unramified cover. From the observation on the fundamental group: A Hurwitz family corresponding to a cover $Y \xrightarrow{\varphi} \mathbb{P}^1$ (with r=2) exists only in the case that $\deg(\varphi)=2$. A Hurwitz family does indeed exist in the case that $\deg(\varphi) = 2$. We present this family in projective coordinates. Let (x,z,y,y_1) be homogeneous coordinates for $\mathbb{P}^3(C)$, and let $(u(1),z(1))$ and $(u(2),z(2))$ be homogeneous coordinates for two copies of $\mathbb{P}^1$. Then if $Y \xrightarrow{\varphi} \mathbb{P}^1$ is a degree 2 cover, it is contained in the Hurwitz family (family of curves in $\mathbb{P}^3(\mathbb{C})$)

(3.10) $y^2(u(1)\cdot z-z(1)x)(u(1)z(2)-z(1)\cdot u(2))=(u(1))^2z^2(u(2)\cdot z-z(2)\cdot x)$,

$y_1^2(u(2)\cdot z-z(2)\cdot x)(u(1)\cdot z(2)-z(1)\cdot u(2))=(u(2))^2z^2(u(1)\cdot z-z(1)\cdot x)$.

We note that this family extends to a normal, projective cover $\mathcal{Y}^*$ of $(\mathbb{P}^1\times\mathbb{P}^1)\times\mathbb{P}^1$ (variables are $(u(1),z(1);u(2),z(2);x,z)$). Over the $\frac{u(1)}{z(1)}=\frac{u(2)}{z(2)}$ locus the fibers of this family are degree 1 covers of $\mathbb{P}^1$. Again this is a degenerate branch locus. From coelescing of branch points one would have expected these fibers to have been 2 copies of $\mathbb{P}^1$ joined together at a point.

In the case that $Y\xrightarrow{\varphi}\mathbb{P}^1$ is an abelian cover, Kummer theory may be applied to treat the existence of both Hurwitz families and symmetrized Hurwitz families ([Fr, 2]). This remark applies to the two branch point case above (covers are cyclic in this case). ∎

Section 4. Basic Construction of Hurwitz Families: The Hurwitz Number

(4.A) Basic Construction

We retain the notation of Section 3. For $\underset{\sim}{\alpha}=(\alpha(1),\dots,\alpha(r))$ and $\underset{\sim}{\beta}=(\beta(1),\dots,\beta(r))\in S_n^r$ we say that $\underset{\sim}{\alpha}$ is equivalent to $\underset{\sim}{\beta}$ if there exists $\gamma\in S_n$ such that $\gamma\beta(i)\gamma^{-1}=\alpha(i)$; $i=1,\dots,r$. We denote the equivalence class of $\underset{\sim}{\alpha}$ by $\mathrm{Con}(\underset{\sim}{\alpha},S_n)$. We say that $\underset{\sim}{\alpha}$ and $\underset{\sim}{\beta}$ are neighbors at the i-th coordinate if either:

(4.1)a) $\beta(i)=\alpha(i+1)$, $\beta(i)\cdot\beta(i+1)\cdot\beta(i)^{-1}=\alpha(i)$ and $\beta(j)=\alpha(j)$ for $j\neq i$ or $i+1$; or

b) $\beta(i+1)=\alpha(i)$, $(\beta(i+1))^{-1}\cdot\beta(i)\cdot\beta(i+1)=\alpha(i+1)$ and $\beta(j)=\alpha(j)$ for $j\neq i$ or $i+1$.

We say that $\underset{\sim}{\alpha}\overset{R}{}\underset{\sim}{\beta}$ if there is a sequence of neighbors, the first being α and the last being $\underset{\sim}{\beta}$. To the pair of neighbors (4.1)a) or b) we associate the element $(i\ i+1)\in S_r$. Similarly, to the relation $\underset{\sim}{\alpha}\overset{R}{}\underset{\sim}{\beta}$ we associate an element $\theta(\underset{\sim}{\alpha}\overset{R}{}\underset{\sim}{\beta})\in S_r$ by taking the product (in order) of the elements associated to each pair of neighbors in the sequence.

Definition 4.1 For $\underset{\sim}{\sigma} \in S_n^r$ we denote by: Br*($\underset{\sim}{\sigma}$) (the *-Braid Class of $\underset{\sim}{\sigma}$) the set of $\underset{\sim}{\tau} \in S_n^r$ such that

(4.2)a) $\underset{\sim}{\tau} \overset{R}{\sim} \underset{\sim}{\sigma}$, and

b) $\theta(\underset{\sim}{\tau} \overset{R}{\sim} \underset{\sim}{\sigma}) = \mathrm{Id.} \in S_r$;

Br**($\underset{\sim}{\sigma}$) the set of $\underset{\sim}{\tau} \in S_n^r$ such that only (4.2)a) is satisfied, and;

Br($\underset{\sim}{\sigma}$) (the Braid Class of $\underset{\sim}{\sigma}$), the set of $\underset{\sim}{\tau}' \in S_n^r$ such that $\mathrm{Con}(\underset{\sim}{\tau}', S_n) = \mathrm{Con}(\underset{\sim}{\tau}, S_n)$ for some $\underset{\sim}{\tau} \in$ Br**($\underset{\sim}{\sigma}$).

Definition 4.2 For $\underset{\sim}{\sigma} \in S_n^r$ we let $G(\underset{\sim}{\sigma})^*$ be the subgroup of the normalizer of $G(\underset{\sim}{\sigma})$ in S_n (Section 0.B) consisting of those elements τ such that

$$\mathrm{Con}(\tau\sigma(i)\tau^{-1}, G(\underset{\sim}{\sigma})) = \mathrm{Con}(\sigma(i), G(\underset{\sim}{\sigma})); \; i = 1, \ldots, r.$$

Definition 4.3. For $\underset{\sim}{\sigma} \in S_n^r$ we say that $\underset{\sim}{\sigma}$ is semi-complete if for each $\tau \in G(\underset{\sim}{\sigma})^*$, conjugation by τ gives an inner automorphism of $G(\underset{\sim}{\sigma})$. We say that $\underset{\sim}{\sigma}$ is complete if in addition $G(\underset{\sim}{\sigma})$ has no center.

We have a map

$G(\underset{\sim}{\sigma})^* \xrightarrow{\Psi} \mathrm{Aut}(G(\underset{\sim}{\sigma})) \overset{\mathrm{def}}{=}$ {automorphisms of the group $G(\underset{\sim}{\sigma})$}, where $\Psi(\gamma)$ is the automorphism of $G(\underset{\sim}{\sigma})$ given by conjugation by $\gamma \in G(\underset{\sim}{\sigma})^*$. Consider the condition: the sequence

(4.3) $$1 \longrightarrow \mathrm{Cen}_{S_n}(G(\underset{\sim}{\sigma})) \longrightarrow G(\underset{\sim}{\sigma})^* \xrightarrow{\Psi} \Psi(G(\underset{\sim}{\sigma})^*) \longrightarrow 1$$

splits where $\mathrm{Cen}_{S_n}(G(\sigma))$ is the centralizer of $G(\underset{\sim}{\sigma})$ in S_n.

Lemma 4.1. In the notation above, (4.3) splits if:

(4.4)a) $\underset{\sim}{\sigma}$ is complete;

b) the orders of $\mathrm{Cen}_{S_n}(G(\underset{\sim}{\sigma}))$ and $\Psi(G(\sigma)^*)$ are relatively prime, or;

c) $G(\underset{\sim}{\sigma})$ is a regular permutation group (the embedding of $G(\underset{\sim}{\sigma})$ in S_n is the regular representation of $G(\underset{\sim}{\sigma})$).

Proof. We must find a group $H \subset G(\underset{\sim}{\sigma})^*$ that is a section for ψ. In case (4.4)b) H exists by the Lemma of Zassenhaus and Schur ([Za]). In case (4.4)a) we take H to be $G(\underset{\sim}{\sigma})$, and in the Case (4.4)c) take the subgroup of $G(\underset{\sim}{\sigma})^*$ consisting of elements which fix the identity element in $G(\underset{\sim}{\sigma})$ (the letters of the regular representation are identified with the elements of $G(\underset{\sim}{\sigma})$). ■

Example 3. An example where (4.3) does not split.

Let $G = G((\mathbb{Z}/(8))^*, 8)$ be the multiplicative group of 2×2 matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ with $a \in (\mathbb{Z}/(8))^*$ (invertible integers modulo 8) and $b \in \mathbb{Z}/(8)$. Consider G embedded in S_8 by the representation of G on the integers modulo 8. It is easy to see that $G = G(\underset{\sim}{\sigma})^* = G(\underset{\sim}{\sigma})$ for $\underset{\sim}{\sigma}$ any collection of generators of G (use the characteristic subgroup generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$). If condition (4.3) holds for some group $H \subset G$, then H would have no center and we could write

$$G = H \times \mathrm{Cen}(G) \quad (\mathrm{Cen}(G) \text{ is the center of } G).$$

However, since G is a 2-group, so is H, and therefore H has a non-trivial center.

For later purposes it is important to notice that G has an outer automorphism. In fact, let

$$b_a = \begin{cases} 0 \text{ if } a = 1 \text{ or } 3 \\ 1 \text{ if } a = 5 \text{ or } 7 \end{cases}.$$

Then we define $\alpha : G \to G$ by

$\alpha\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b_a \cdot 4 + b \\ 0 & 1 \end{pmatrix}$. It is easy to check that α is not inner, and we observe that α preserves conjugacy classes. ■

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover of projective, non-singular curves, and let $\underset{\sim}{u}^{(0)}$ be an ordered r-tuple of points of $\mathbb{P}^1$ which contain among them the branch points of φ. A Hurwitz family (over $\mathbb{C}$) corresponding to the data (Y, φ) and $\underset{\sim}{u}^{(0)}$ consists of a complex manifold $\mathfrak{I}(Y, \varphi; r, \underset{\sim}{u}^{(0)})$ equipped with structure morphisms

$$\mathfrak{I}(Y, \varphi; r, \underset{\sim}{u}^{(0)}) \xrightarrow{\Phi} U^r_{\mathbb{P}} \times \mathbb{P}^1 \xrightarrow{pr_1} U^r_{\mathbb{P}} \qquad (4.5)$$

$$\xrightarrow{pr_2} \mathbb{P}^1$$

such that:

(4.6)a) $pr_1 \cdot \Phi$ is a smooth morphism;

b) for $\underset{\sim}{u} \in U^r_{\mathbb{P}^1}$, the fiber $\mathcal{Y}_{\underset{\sim}{y}}$ (of the morphism $pr_1 \cdot \Phi$) consists of a disjoint union of Riemann surfaces, presented (by restriction of $pr_2 \cdot \Phi$ to $\mathcal{Y}_{\underset{\sim}{y}}$) as branched covers of $\mathbb{P}^1$, branched over the collection of points $u(1), \ldots, u(r)$ (where $(u(1), \ldots, u(r)) = \underset{\sim}{y}$);

c) (Y, φ) is a connected component of $\mathcal{Y}_{\underset{\sim}{y}^{(0)}} \xrightarrow{pr_2 \cdot \Phi} \mathbb{P}^1$; and

d) the connected components of $\mathcal{Y}_{\underset{\sim}{y}^{(0)}}$ (as covers of $\mathbb{P}^1$) are non-isomorphic.

Let $(\sigma(1), \ldots, \sigma(r)) = \underset{\sim}{\sigma}$ be an ordered description of the branch cycles of φ; $n = \deg \varphi$.

Proposition 3. Suppose that a Hurwitz family exists (satisfying (4.5) and (4.6)). Then, the number of connected components of the fiber $\mathcal{Y}_{\underset{\sim}{y}^{(0)}}$ is given by

(4.7)
$$\frac{|Br^*(\underset{\sim}{\sigma})|}{|\{\alpha^{-1}\underset{\sim}{\sigma}\alpha \mid \alpha \in G(\underset{\sim}{\sigma})^*\} \cap Br^*(\underset{\sim}{\sigma})|}$$

If Aut $(Y, \varphi) = \{\mathrm{Id.}\}$, then Hurwitz families exist and are unique.

More generally, if condition (4.3) is satisfied (see Lemma 4.1) then Hurwitz families exist locally for the Zariski topology. That is, (4.5) and (4.6) hold with $U^r_{\mathbb{P}^1}$ replaced by some affine subset of $U^r_{\mathbb{P}^1}$ containing $\underset{\sim}{y}^{(0)}$. If, in addition $G(\underset{\sim}{\sigma})$ has no center, then Hurwitz families exist (includes the case when $\underset{\sim}{\sigma}$ is complete or when the embedding $G(\underset{\sim}{\sigma}) \subset S_n$ is the regular presentation of $G(\underset{\sim}{\sigma})$).

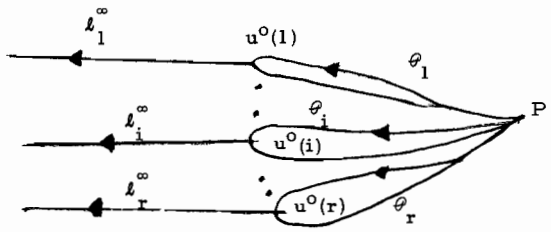
Hurwitz families always exist in the case that $r=3$ (see Example 2). In this case, as in the case that $G(\underset{\sim}{\sigma})$ is an abelian group, expression (4.7) is 1.

Proof. Let $\mathbb{A}^{\infty} = \mathbb{P}^1 - \{\infty\}$, and let $\mathbb{A}^{o} = \mathbb{P}^1 - \{0\}$. For simplicity we assme that $u^{(0)}(1), \ldots, u^{(0)}(r) \in \mathbb{A}^{\infty}$. Let $P \in \mathbb{A}^{\infty} - \{u^{(0)}(1), \ldots, u^{(0)}(r)\}$.

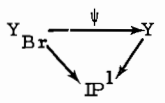
Let $\sigma(1), \ldots, \sigma(r) \in S_n$ (respectively) be a description of the branch cycles for (Y, φ) corresponding to the action of the paths $\theta_1, \ldots, \theta_r$ (respectively; as in Fig. 2), on the fiber $P_1, \ldots, P_n$ of (Y, φ) over P. A permutation θ of $P_1, \ldots, P_n$ leaves the description of the branch cycles invariant iff:

(4.8) θ is contained in $\mathrm{Cen}_{S_n}(G(\underset{\sim}{\sigma}))$, the centralizer in S_n of $G(\underset{\sim}{\sigma})$.

Figure 2.



We form oriented branch cuts $\ell_1^{\infty}, \ldots, \ell_r^{\infty}$ (parallel cuts, along the negative real axis in Figure 2, although it suffices to take any direction for which the cuts are disjoint.) Let $\mathcal{S}_n = \bigcup_{i=1}^{n} \mathbb{P}_i^1(\mathbb{C})$ where $\mathbb{P}_i^1(\mathbb{C}) = \mathbb{P}^1(\mathbb{C}), i = 1, \ldots, n$ (i.e., n disjoint copies of the sphere). Utilizing the branch cuts, construct a scissors and paste' model $Y_{Br} \xrightarrow{\varphi_{Br}} \mathbb{P}^1(\mathbb{C})$ such that the 'sheets' of φ_{Br} (corresponding to the connected components of $\mathcal{S}_n$) are permuted as $\sigma(1), \ldots, \sigma(r)$ as the paths $\theta_1, \ldots, \theta_r$ (respectively) are traversed. Thus, identifying as named, the fiber $P_1, \ldots, P_n$ of $Y \xrightarrow{\varphi} \mathbb{P}^1$ over P with the 'sheets' of $Y_{Br} \xrightarrow{\varphi_{Br}} \mathbb{P}^1$, we obtain a canonical isomorphism $\psi : Y_{Br} \to Y$ fitting in a commutative triangle



Consider the collection $T(r,n)$ of pairs:

$(\underset{\sim}{u},\underset{\sim}{\tau})$ with $\underset{\sim}{u} = (u_1,\ldots,u_r) \in U^r_{\mathbb{A}^\infty}$ and $\underset{\sim}{\tau} \in (S_n)^r$ satisfying:

$\prod_{i=1}^{r} \tau(\alpha(i)) = \mathrm{Id}$. where α is the permutation of $\{1,\ldots,r\}$ such that;

(4.9)a) $\quad \mathrm{Im}\, u_{\alpha(i)} \geq \mathrm{Im}\, u_{\alpha(i+1)}$

and b) $\quad \mathrm{Re}\, u_{\alpha(i)} > \mathrm{Re}\, u_{\alpha(i+1)}$ in the case of equality in (a).

Now repeat the previous construction for Y_{Br} with: $\underset{\sim}{u}^{(0)}$ replaced by $\underset{\sim}{u}$; $\mathcal{S}$ replaced by $\underset{\sim}{\tau}$, and; cuts $\ell_1^\infty,\ldots,\ell_r^\infty$ replaced by oriented cuts parallel to $\ell_1^\infty,\ldots,\ell_r^\infty$ emanating (respectively) from the points of the coordinates of $\underset{\sim}{u}$. In this way we obtain $Y(\underset{\sim}{u},\underset{\sim}{\tau})$. As long as equality does not occur in (4.9)a) everything is exactly as before. If, on the other hand

$$\mathrm{Im}\, u_{\alpha(i-1)} > \mathrm{Im}\, u_{\alpha(i)} = \mathrm{Im}\, u_{\alpha(i+1)} = \ldots = \mathrm{Im}\, u_{\alpha(i+k)} > \mathrm{Im}\, u_{\alpha(i+k+1)}$$

then we patch together the components of $\mathcal{S}_n$ along the pullbacks of the cuts according to the prescription:

(4.10) $\tau(\alpha(i))$ corresponds to the cut from $u_{\alpha(i)}$ to $u_{\alpha(i+1)}$;

$\tau(\alpha(i))\cdot\tau(\alpha(i+1))$ corresponds to the cut from $u_{\alpha(i+1)}$ to $u_{\alpha(i+2)}$;

$\tau(\alpha(i))\cdot\tau(\alpha(i+1))\cdots\tau(\alpha(i+k))$ corresponds to the cut from $u_{\alpha(i+k)}$ to ∞; and $\tau(\alpha(i+k+1))$ corresponds to the cut from $u_{\alpha(i+k+1)}$.

There is a natural topology on the set $T(r,n)$ which we now describe. Let $(\underset{\sim}{u},\underset{\sim}{\tau})$ and $(\underset{\sim}{u}',\underset{\sim}{\tau}') \in T(r,n)$ where $\underset{\sim}{u}'$ is contained in an ε-ball about $\underset{\sim}{u}$ in $U^r_{\mathbb{A}^\infty}$. Let φ be a path from $\underset{\sim}{u}$ to $\underset{\sim}{u}'$ entirely contained in this ε-ball. Let φ be represented by $\bar{\varphi}\colon [0,1] \longrightarrow U^r_{\mathbb{A}^\infty}$, and let $t_1 < t_2 < \ldots < t_a$ be the values $t \in [0,1]$ at which two or more of the coordinates of $\bar{\varphi}(t)$ have their imaginary parts equal. With no loss we may assume (by a slight deformation of $\bar{\varphi}$) that: there are only finitely many such points, and; excluding $i = a$ if $t_a = 1$, at most two of the coordinates of $\bar{\varphi}(t_i)$ have the same imaginary part. Let $m(i)$

and n(i) be such that: $\underset{\sim}{u}(t_i) = \bar{\varphi}(t_i)$ and; the imaginary parts of $u_{m(i)}(t_i)$ and $u_{n(i)}(t_i)$ are equal, i = 1,...,a . Assume that the real part of $u_{m(i)}(t_i)$ is less than the real part of $u_{n(i)}(t_i)$. Let $\varepsilon(i) = 1$ if the imaginary part of $u_{n(i)}(t)$ is greater than the imaginary part of $u_{m(i)}(t)$ for t less than t_i and close to t_i, and; let $\varepsilon(i) = -1$ otherwise. For each integer i = 0,...,a (i=0,...,a-1 if t_a=1) we associate an r-tuple of elements $\underset{\sim}{\tau}_i \in S_n^r$. We do this assignment by induction. For i = 0 let $\underset{\sim}{\tau}_0 = \underset{\sim}{\tau}$. Assume that we have found $\underset{\sim}{\tau}_i$. Then we let $\underset{\sim}{\tau}_{i+1} = (\tau(1)_{i+1},\ldots,\tau(r)_{i+1})$ where: $\tau(j)_i = \tau(j)_{i+1}$ for $j \neq n(i+1)$ or $m(i+1)$; if $\varepsilon(i+1) = 1$ then $\tau(n(i+1))_i = \tau(m(i+1))_{i+1}$ and $\tau(n(i+1))_i^{-1}$. $\tau(m(i+1))_i \cdot \tau(n(i+1))_i = \tau(n(i+1))_{i+1}$ and; if $\varepsilon(i+1) = -1$, then $\tau(m(i+1))_i = \tau(n(i+1))_{i+1}$ and $\tau(m(i+1))_i \cdot \tau(n(i+1))_i \cdot \tau(m(i+1))_i^{-1} = \tau(m(i+1))_{i+1}$. We let $\underset{\sim}{\tau}' = \underset{\sim}{\tau}_a$ (or $\underset{\sim}{\tau}_{a-1}$ if $t_a = 1$). Then we say that $(\underset{\sim}{u}',\underset{\sim}{\tau}')$ is contained in the ε-ball about $(\underset{\sim}{u},\underset{\sim}{\tau})$ in T(r,n). From the continuity of our previous construction there is a natural fiber space topology making $\mathcal{Y}^* = \cup\, Y(\underset{\sim}{u},\underset{\sim}{\tau})$ (union over $(\underset{\sim}{u},\underset{\sim}{\tau}) \in T(r,n)$) into a manifold.

We denote by $\mathcal{Y}_{Br}(Y,\varphi;r,\underset{\sim}{u}^{(0)})$ the connected component of $\mathcal{Y}^*$ containing Y_{Br}. Now, with $U^r_{\mathbb{P}^1}$ replaced by $U^r_{\mathbb{A}^1_\infty}$, $\mathcal{Y}_{Br}$ satisfies (4.6)a, b and c), but not (4.6)d). Two connected components of the fiber of $\mathcal{Y}_{Br}$ over $\underset{\sim}{u}^{(0)}$ are isomorphic (as covers of $\mathbb{P}^1$) iff their branch cycle descriptions are the same for some renaming of their respective fibers over the base point P. Equivalently; iff their branch cycle descriptions can be obtained, one from the other, by conjugation by some element of $G(\varphi)^*$. An examination of the construction shows that: the number of connected components of the fiber $\mathcal{Y}_{Br}$ above $\underset{\sim}{u}^{(0)}$ is given by $|Br^*(\varphi)|$; and (up to isomorphism) each of these occurs as many times as the expression in the denominator of (4.7).

Now assume that a Hurwitz family $\mathcal{Y}'$, satisfying (4.6)a), b), c) and d) does exist. Consider the restriction of $\mathcal{Y}'$ to $U^r_{\mathbb{A}^1_\infty} \times \mathbb{P}^1$ (which we again denote by $\mathcal{Y}'$). Since $\mathcal{Y}_{Br}$ and $\mathcal{Y}'$ both contain $Y \to \mathbb{P}^1$, it is easy to see that there exists a many valued map from $\mathcal{Y}_{Br}$ to $\mathcal{Y}'$ (as covers of $U^r_{\mathbb{A}^1_\infty} \times \mathbb{P}^1$). In particular, the same

set of Riemann surfaces (as covers of $\mathbb{P}^1$) occur in the fibers $(\mathfrak{I}_{Br})_{\underset{\sim}{u}(0)}$ and $\mathfrak{I}'_{\underset{\sim}{u}(0)}$. This establishes the first part of the proposition.

We now show that if condition (4.3) holds, then there exists a Hurwitz family satisfying (4.6) with $U^r_{\mathbb{P}}$ replaced by $U^r_{\mathbb{A}^\infty}$. In fact, this Hurwitz family is the quotient of $\mathfrak{I}_{Br}$ by a finite group of automorphisms $\tilde{H}$ which is isomorphic to a subgroup of the group H that appears in the proof of Lemma 4.1

Let $P(\underset{\sim}{u})$ be any continuous function on $U^r_{\mathbb{A}^\infty}$ with values in $\mathbb{A}^\infty$ such that for each $\underset{\sim}{u}$, $P(\underset{\sim}{u})$ lies to the right of all the points $u_1, \ldots, u_r \in A^\infty$ (as in Figure 2). Such a function is easy to construct. Let $P_1(\underset{\sim}{u}), \ldots, P_n(\underset{\sim}{u})$ be the points above $P(\underset{\sim}{u})$ in $\mathfrak{S}_n = \bigcup_{i=1}^{n} \mathbb{P}^1_i(\mathbb{C})$ (as in previous notation) where $P_i(\underset{\sim}{u}) \in \mathbb{P}^1_i(\mathbb{C})$ for $i = 1, \ldots, r$. Then the branch cut construction allows us to identify $P_1(\underset{\sim}{u}), \ldots, P_n(\underset{\sim}{u})$ with points in the fiber of

$$Y_{\underset{\sim}{u}} \xrightarrow{\varphi_{\underset{\sim}{u}}} \mathbb{P}^1 \quad \text{above } P(\underset{\sim}{u})$$

where $Y_{\underset{\sim}{u}}$ is any connected component of $(\mathfrak{I}_{Br})_{\underset{\sim}{u}}$. Let H' be the subset of H (as in Lemma 4.1) consisting of those $\alpha \in H$ such that $\alpha^{-1}\underset{\sim}{\sigma}\alpha \in Br^*(\underset{\sim}{\sigma})$. Note that H' is a group. Indeed, if some braiding of $\underset{\sim}{\sigma}$ gives $\alpha^{-1}\underset{\sim}{\sigma}\alpha$, and if some braiding of σ gives $\beta^{-1}\underset{\sim}{\sigma}\beta$, then this former braiding applied to $\beta^{-1}\underset{\sim}{\sigma}\beta$ will give.

$$(\beta^{-1}\cdot\alpha\cdot\beta)^{-1}\beta^{-1}\cdot\underset{\sim}{\sigma}\cdot\beta\cdot(\beta^{-1}\cdot\alpha\cdot\beta) = (\alpha\beta)^{-1}\cdot\underset{\sim}{\sigma}\cdot(\alpha\beta).$$

Thus, the composition of the two braidings gives $(\alpha\beta)^{-1}\underset{\sim}{\sigma}(\alpha\beta)$ and we have $\alpha\beta \in H'$.

Let $Y'_{\underset{\sim}{u}} \xrightarrow{\varphi'} \mathbb{P}^1$ and $Y''_{\underset{\sim}{u}} \xrightarrow{\varphi} \mathbb{P}^1$ be two connected components of the fiber of $(\mathfrak{I}_{Br})_u$ such that (as covers of $\mathbb{P}^1$), $Y_{\underset{\sim}{u}}$ and $Y''_{\underset{\sim}{u}}$ are isomorphic. Let $P'_1(\underset{\sim}{u}), \ldots, P'_n(\underset{\sim}{u})$, and $P''_1(\underset{\sim}{u}), \ldots, P''_n(\underset{\sim}{u})$ be the respective fibers of φ' and φ'' above $P(\underset{\sim}{u})$, as previously described. Then, from condition (4.3) there exists a unique element $h \in H'$ (regarded as a subgroup of S_n) such that with the renaming of the fiber $P''_1(\underset{\sim}{u}), \ldots, P''_n(\underset{\sim}{u})$ to $P'''_1(\underset{\sim}{u}), \ldots, P'''_n(\underset{\sim}{u})$ with $P'''_i(\underset{\sim}{u}) = P''_{h(i)}(\underset{\sim}{u})$ the branch cycle descriptions for $Y'_{\underset{\sim}{u}}$ and $Y''_{\underset{\sim}{u}}$ are the same. In turn, this

isomorphism extends uniquely to an automorphism (denoted $\tilde{h}$) of $\mathfrak{I}_{Br}$ as a cover of $U^r_{\mathbb{A}^\infty} \times \mathbb{P}^1$. We denote the group generated by $\tilde{h}$ for $h \in H'$ by $\tilde{H}$. The quotient of $\mathfrak{I}_{Br}$ by $\tilde{H}$ is easily seen to satisfy the conditions of (4.6).

In the case when $\mathrm{Aut}(Y, \varphi, \mathbb{C}) = \{\mathrm{Id.}\}$ the construction is easily finished. The same construction as above, with $U^r_{\mathbb{A}^\infty}$ replaced by $U^r_{\mathbb{A}^0}$ yields a Hurwitz family $\mathfrak{I}(Y, \varphi; \underset{\sim}{u}^{(0)})$ over $U^r_{\mathbb{A}^0} \times \mathbb{P}^1$. Since the fibers of the Hurwitz family over $U^r_{\mathbb{A}^0}$ and $U^r_{\mathbb{A}^\infty}$ have no automorphisms, the restriction of the two Hurwitz families to $U^r_{\mathbb{A}^0} \cap U^r_{\mathbb{A}^\infty}$ are seen to be canonically isomorphic. From [Gr and Re] the resulting manifold is a Zariski open subset of a projective algebraic variety. Since $U^r_{\mathbb{P}} - (U^r_{\mathbb{A}^0} \cup U^r_{\mathbb{A}^\infty})$ is of codimension 2 in $U^r_{\mathbb{P}}$, it is easy to see that this manifold extends to the desired structure $\mathfrak{I}$ over $U^r_{\mathbb{P}} \times \mathbb{P}^1$.

Unfortunately, the proof that the Hurwitz family exists when (4.3) holds and $G(\underset{\sim}{g})$ has no center is complicated. In particular, it requires the computation of generators and relations for the fundamental group of $U^r_{\mathbb{A}^\infty} \cap U^r_{\mathbb{A}^0}$. This argument is contained in [Fr, 2]. See the discussion of Section 4.B.

If $G(\underset{\sim}{g})$ is an abelian group, it is obvious that expression (4.7) is 1.

In the case when r=3 (3 branch point case) we constructed Hurwitz families explicitly in Example 2, and back handedly we see that (4.7) is 1. This computation may also be done directly. ∎

4.B) The Hurwitz Number and Further Observations on the Existence of Symmetrized Hurwitz Families

Let $\underset{\sim}{g} \in S_n^r$ with $\underset{\sim}{g} = (\sigma(1), \ldots, \sigma(r))$ and $\sigma(1) \cdot \sigma(2) \cdots \sigma(r) = \mathrm{Id.}$

Definition 4.4. We define the Hurwitz set of $\underset{\sim}{g}$ to be the collection $\mathcal{H}(\underset{\sim}{g})$ $\{\underset{\sim}{\tau} \in S_n^r \mid$ there exists $\underset{\sim}{\tau}' \in S_n^r$ and $\beta \in S_n$ with: $\beta^{-1} \cdot \underset{\sim}{\tau}' \cdot \beta = \underset{\sim}{\tau}$; $G(\underset{\sim}{g}) = G(\underset{\sim}{\tau}')$; $\tau'(1) \cdots \tau'(r) = \mathrm{Id.}$, and; $\mathrm{Con}(\tau'(i), G(\underset{\sim}{g})) = \mathrm{Con}(\sigma(i), G(\underset{\sim}{g}))$ for $i = 1, \ldots, r\}$. The Hurwitz number, $\mathrm{Hur}(\underset{\sim}{g})$ is the ratio $|\mathcal{H}(\underset{\sim}{g})| / |\mathcal{H}(\underset{\sim}{g}) \cap \mathrm{Br}(\underset{\sim}{g})|$. It follows easily from the constructions of Section 4.A that $\mathrm{Hur}(\underset{\sim}{g})$ is an integer.

In relation to Remark 1 and Lemma 1.1. we have:

Proposition 4. Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover of projective non-singular curves having $\underset{\sim}{\sigma} \in S_n^r$ as a description of the branch cycles of φ (as in Section 1.A). Then, Hur $(\underset{\sim}{\sigma})$ is 1 if and only if every element of the Hurwitz set of $\underset{\sim}{\sigma}$ is a description of the branch cycles of φ.

Proof. The proof of Proposition 3 shows that the elements of $Br(\underset{\sim}{\sigma})$ are exactly the descriptions of the branch cycles of covers of $\mathbb{P}^1$ which are deformations (as covers of $\mathbb{P}^1$) of $Y \xrightarrow{\varphi} \mathbb{P}^1$. Let $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ be a cover obtained by deformation of (Y, φ). Choose paths (as in Section 1.A) $\theta_1(Z), \ldots, \theta_r(Z)$ based at $P(Z) \in \mathbb{P}^1$ minus the branch points of $\varphi(Z)$ (similar to Figure 2) which yield the element $\underset{\sim}{\tau} \in Br(\underset{\sim}{\sigma})$ as a description of the branch cycles of $\varphi(Z)$. Then, by deforming the paths $\theta_1(Z), \ldots, \theta_r(Z)$ and the point $P(Z)$ continuously in the deformation of $Z \to \mathbb{P}^1$ back to $Y \to \mathbb{P}^1$ we obtain a new set of paths on $\mathbb{P}^1$ minus the branch points of $\varphi(Y)$. For these new paths we have $\underset{\sim}{\tau}$ as a description of the branch cycles for $Y \to \mathbb{P}^1$.

If $Hur(\underset{\sim}{\sigma})$ is 1, then the construction above shows that every element of the Hurwitz set of $\underset{\sim}{\sigma}$ is, indeed, a description of the branch cycles of (Y,φ) (as in Section 1.A).

Conversely, suppose that every element of the Hurwitz set is a description of the branch cycles of $\underset{\sim}{\sigma}$. Let $\underset{\sim}{\tau} \in \mathcal{H}(\underset{\sim}{\sigma})$ and let $\theta_1(\underset{\sim}{\sigma}), \ldots, \theta_r(\underset{\sim}{\sigma})$ (respectively $\theta_1(\underset{\sim}{\tau}), \ldots, \theta_r(\underset{\sim}{\tau})$) be paths (from the same point P) with which we compute $\underset{\sim}{\sigma}$ (respectively $\underset{\sim}{\tau}$) as a description of the branch cycles of (Y, φ). Then $\theta_1(\underset{\sim}{\sigma}), \ldots, \theta_r(\underset{\sim}{\sigma})$ (respectively $\theta_1(\underset{\sim}{\tau}), \ldots, \theta_r(\underset{\sim}{\tau})$) are generators of the fundamental group of $\mathbb{P}^1$ minus the branch points of φ. Therefore, by Nielson's Theorem ([Ma, K, and S; page 122, Theorem N1]) $\theta_1(\underset{\sim}{\tau}), \ldots, \theta_r(\underset{\sim}{\tau})$ are related to $\theta_1(\underset{\sim}{\sigma}), \ldots, \theta_r(\underset{\sim}{\sigma})$ by elementary Nielsen transformations. From the proof

of Proposition 3 (and inspection of the elementary Nielsen transformations) it is clear that the paths $\theta_1(\underset{\sim}{g}), \ldots, \theta_r(\underset{\sim}{g})$ are obtained from $\theta_1(\underset{\sim}{\tau}), \ldots, \theta_r(\underset{\sim}{\tau})$ by continuous deformation of $\theta_1(\underset{\sim}{\tau}), \ldots, \theta_r(\underset{\sim}{\tau})$ through the deformation of the branch points of (Y,φ) (as in the proof of Proposition 3). Therefore, by appeal to the first half of the proof, $\underset{\sim}{\tau} \in Br(\underset{\sim}{g})$, and the Hurwitz number is 1. ■

Clebsch ([Cle]) showed that the Hurwitz number is 1 in the case of simple branching (Example 1). This is the main ingredient in the classical proof of the connectedness of the coarse (non-compactified) moduli scheme of curves of genus g (first completely proved by Severi; see [Fu]).

In the remainder of this subsection we describe conditions under which symmetrized Hurwitz families exist containing the cover $Y \xrightarrow{\varphi} \mathbb{P}^1$. Of course, if $\mathrm{Aut}(Y,\varphi) = \{\mathrm{Id.}\}$ symmetrized Hurwitz families exist and are unique, as can be seen from their local existence over analytic subsets of $\mathcal{O}(Y,\varphi; r)$. Therefore we are primarily concerned with the case when $\mathrm{Aut}(Y,\varphi) \neq \{\mathrm{Id.}\}$.

We define:

$$G^{**} = \{ \tau \in S_n \mid \text{there exists } \beta \in S_r \text{ with:}$$

$$\mathrm{Con}(\tau^{-1}(\sigma(i))\cdot\tau,\ G(\underset{\sim}{g})) = \mathrm{Con}(\sigma((i)\beta),\ G(\underset{\sim}{g})) \text{ for } i = 1, \ldots, r\}.$$

We identify $\mathrm{Aut}(Y,\varphi)$ with the centralizer in S_n of $G(\underset{\sim}{g})$ (as in Section 2), so $\mathrm{Aut}(Y,\varphi)$ is contained in G^{**}. We have an exact sequence:

$$(4.11) \qquad 1 \to \mathrm{Aut}(Y,\varphi) \to G^{**} \xrightarrow{\psi} \mathrm{Aut}(G(\underset{\sim}{g})) \to 1 \text{ (similar to expression (4.3))}.$$

Let $\overline{G}^{**}$ be the $\tau \in G^{**}$ such that $\tau^{-1}\cdot\underset{\sim}{g}\cdot\tau$ is contained in $Br^{**}(\underset{\sim}{g})$. From expression (4.11) we obtain, by restriction of ψ to $\overline{G}^{**}$;

$$(4.12) \qquad 1 \to \mathrm{Aut}(Y,\varphi) \to \overline{G}^{**} \xrightarrow{\text{rest. } \psi} \mathrm{Im}(\psi) \to 1.$$

Proposition 5. Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover of non-singular curves having $\underset{\sim}{\sigma}$ as a description of its branch cycles. Assume that the sequence (4.12) splits. Then symmetrized Hurwitz families containing (Y,φ) (as described in expression (3.2)) exist locally for the Zariski topology on $\mathcal{P}(Y,\varphi;r)$ (see Proposition 3). This includes the case when (Y,φ) is complete (i.e. $\underset{\sim}{\sigma}$ is complete; definition 4.3), or when (Y,φ) is a Galois cover, or when the orders of $\psi(\bar{G}^{**})$ and $\mathrm{Aut}(Y,\varphi)$ are relatively prime.

Proof. The last statement of the proposition follows from the proof of Lemma 4.1. For the remainder of the proof we use the notation of the proof of Proposition 3. In the proof of Proposition 3 we have formed $\mathcal{T}_{Br} \xrightarrow{\Phi_{Br}} U_A^{r\,\infty} \times \mathbb{P}^1$. We formed Hurwitz families locally for the Zariski topology by showing (under the condition that the sequence (4.3) splits) that there exists a group H' acting as fiber preserving automorphisms of the cover given by Φ_{Br}. In this way we equivalenced any two connected components of a fiber of $\mathcal{T}_{Br} \xrightarrow{pr_1 \circ \Phi_{Br}} U_A^{r\,\infty}$ that were isomorphic as covers of $\mathbb{P}^1$ (by restriction of $pr_2 \circ \Phi_{Br}$ to the fiber).

Let T be the image of $U_A^{r\,\infty}$ under the canonical morphism $(\mathbb{P}^1)^r \xrightarrow{\alpha} \mathbb{P}^r$ given by the action of S_r on the coordinates of $(\mathbb{P}^1)^r$. Then T is $U_{(A^1)^r}$ in the notation at the beginning of Section 3. Let $\Phi_{Br}^{\alpha} = (\alpha \circ pr_1 \circ \Phi_{Br},\ pr_2 \circ \Phi_{Br})$ so that $\mathcal{T}_{Br} \xrightarrow{\Phi_{Br}^{\alpha}} T \times \mathbb{P}^1$ is a morphism such that: each point $\underset{\sim}{p} \in T$ has as coordinates the elementary symmetric functions in the coordinates of the branch points of the connected components of the cover $(\mathcal{T}_{Br})_{\underset{\sim}{p}} \xrightarrow{rest(pr_2 \circ \Phi_{Br}^{\alpha})} \mathbb{P}^1$.

Let H' be a section of the sequence (4.12). Analogous to the proof of Proposition 3 there is a fiber preserving action of H' on the cover given by Φ_{Br}^{α} such that: two connected components of a fiber $(\mathcal{T}_{Br})_{\underset{\sim}{p}} \xrightarrow{rest(pr_2 \circ \Phi_{Br}^{\alpha})} \mathbb{P}^1$ are equivalenced under the action of H' if and only if they are isomorphic as covers of $\mathbb{P}^1$. Consider $\mathcal{T}_{Br}/H' \xrightarrow{(\Phi_{Br}^{\alpha})^{H'}} T \times \mathbb{P}^1$. Let M be the pullback of

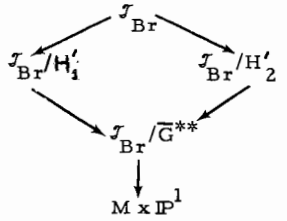
T in the natural morphism $\mathcal{O}(Y,\varphi;r) \longrightarrow \mathbb{P}^r$. Since $\mathcal{O}(Y,\varphi;r)$ is a quasi-finite and proper morphism over its image, it is a finite (in particular, affine) morphism over its image. Therefore, M is an affine subset of $\mathcal{O}(Y,\varphi;r)$. Also, we induce $\mathcal{J}_{Br}/H' \xrightarrow{\Phi} M \times \mathbb{P}^1$ by mapping the connected components of $(\mathcal{J}_{Br}/H^1)_{\underline{p}} \longrightarrow \underline{p} \times \mathbb{P}^1$ (for $p \in T$) to their respective isomorphism classes in the points of M over $\underline{p}$. Clearly, the cover Φ is a symmetrized Hurwitz family over the subset M of $\mathcal{O}(Y,\varphi;r)$.

We demonstrate the local existence of symmetrized Hurwitz families in the Zariski topology on $\mathcal{O}(Y,\varphi;r)$. For $\underline{p} \in \mathcal{O}(Y,\varphi;r)$ we replace $U^r_{\mathbb{A}^\infty}$ (therefore T and M) in the discussion above by a suitable choice of affine subset of $U^r_{\mathbb{P}}$ containing the pullback (from $U_{\mathbb{P}^r}$) of the image of $\underline{p}$ in $\mathcal{O}(Y,\varphi;r) \to U_{\mathbb{P}^r}$. ■

Since the families constructed in Proposition 4 are the key to further results on the existence of $\mathcal{J}^{symm}(Y,\varphi;r) \longrightarrow \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$ (as in expression (3.2)), we comment further on the dependence of $\mathcal{J}_{Br}/H' \xrightarrow{\Phi} M \times \mathbb{P}^1$ on the section H' (by abuse) that gives the splitting of sequence (4.12).

Let H'_1, H'_2 be two splittings of sequence (4.12). We wish to find out whether or not $\mathcal{J}_{Br}/H'_1 \xrightarrow{\Phi_1} M \times \mathbb{P}^1$ and $\mathcal{J}_{Br}/H'_2 \xrightarrow{\Phi_2} M \times \mathbb{P}^1$ are isomorphic. We have a diagram of covers:

(4.13)



From standard covering space theory:

$\mathcal{T}_{Br}/H_1' \longrightarrow \mathcal{T}_{Br}/\overline{G}^{**}$ and $\mathcal{T}_{Br}/H_2' \longrightarrow \mathcal{T}_{Br}/\overline{G}^{**}$ <u>are isomorphic as covers of</u> $\mathcal{T}_{Br}/\overline{G}^{**}$ if and only if H_1' <u>and</u> H_2' <u>are conjugate subgroups of</u> $\overline{G}^{**}$. Let $\mathcal{T}^* \longrightarrow M \times \mathbb{P}^1$ be a Galois cover of $M \times \mathbb{P}^1$ such that $\mathcal{T}^* \longrightarrow M \times \mathbb{P}^1$ factors through the cover $\mathcal{T}_{Br} \longrightarrow M \times \mathbb{P}^1$. See Lemma 2.3 for the construction of $\mathcal{T}^*$. <u>Then</u> $\mathcal{T}_{Br}/H_1' \longrightarrow M \times \mathbb{P}^1$ <u>and</u> $\mathcal{T}_{Br}/H_2' \longrightarrow M \times \mathbb{P}^1$ <u>are isomorphic as covers of</u> $M \times \mathbb{P}^1$ <u>if and only if</u> $G(\mathcal{T}^*/(\mathcal{T}_{Br}/H_1'))$ <u>is conjugate to</u> $G(\mathcal{T}^*/(\mathcal{T}_{Br}/H_2'))$ in $G(\mathcal{T}^*/M \times \mathbb{P}^1)$. Thus, it seems conceivable that H_1' and H_2' may be <u>non-conjugate</u> subgroups of $\overline{G}^{**}$ and yet $\mathcal{T}_{Br}/H_1'$ and $\mathcal{T}_{Br}/H_2'$ are isomorphic as covers of $M \times \mathbb{P}^1$.

In [Fr, 2] these constructions are used to show that under the condition that the sequence (4.12) splits, the obstruction to forming $\mathcal{T}^{symm}(Y, \varphi; r) \longrightarrow \mathcal{O}(Y, \varphi; r) \times \mathbb{P}^1$ lies in $H^2(\mathcal{O}(Y, \varphi; r), CEN(Y, \varphi))$ where: $CEN(Y, \varphi)$ is the sheaf of groups on $\mathcal{O}(Y, \varphi; r)$ such that the stalk of this sheaf at $p \in \mathcal{O}(Y, \varphi; r)$ is the center of the automorphism group of a cover $Z \longrightarrow \mathbb{P}^1$ representing p. Unfortunately, without the existence of a symmetrized Hurwitz family we cannot even be sure that there exists a sheaf $AUT(Y, \varphi)$ over $\mathcal{O}(Y, \varphi; r)$ (Section 3) such that: the stalk of this sheaf at $p \in \mathcal{O}(Y, \varphi; r)$ is the automorphism group of a cover representing p. In fact, the cohomological interpretation to the obstruction to the existence of $AUT(Y, \varphi)$ properly belongs to Giraud's theory of 'gerbes' ([Gi]). Of course, once $\mathcal{T}^{symm}(Y, \varphi; r)$ exists then we can form $AUT(Y, \varphi)$. In this case the collection of symmetrized Hurwitz families containing (Y, φ) is in one-one correspondence with the elements of the Cech Cohomology set $H^1(\mathcal{O}(Y, \varphi; r), AUT(Y, \varphi))$. In fact, it is shown in [Fr, 2] that if the sequence (4.12) splits, $AUT(Y, \varphi)$ exists. Thus, we may consider the exact sequence of 'pointed' cohomology sets:

$H^1(\mathcal{O}(Y, \varphi; r); CEN) \longrightarrow H^1(\mathcal{O}(Y, \varphi; r), CEN)$

$\longrightarrow H^1(\mathcal{O}(Y, \varphi; r), AUT/CEN) \xrightarrow{\delta} H^2(\mathcal{O}(Y, \varphi; r), CEN)$ [Gro; Prop. 5.3.1, p. 16].

There exists an explicitly computable cocycle $\theta(Y,\varphi) \in H^2(\mathcal{O}, CEN)$ such that a symmetrized Hurwitz family exists if and only if $\theta(Y,\varphi)$ is the image under δ of an element of $H^1(\mathcal{O}, AUT / CEN)$.

Section 5. The Minimal Field of Definition of Symmetrized Hurwitz Families In the Case of No Automorphisms

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover of non-singular projective curves (defined over $\mathbb{C}$) such that:

(5.1) $Aut(Y,\varphi) = \{Id.\}$ (see Section 1.4). Let $\sigma(1),\cdots,\sigma(r)$ be a description of the branch cycles of (Y,φ) with respect to orientations of neighborhoods of the branch points $u(1),\cdots,u(r)$ of φ induced from a fixed orientation of $\mathbb{P}^1$; as in Section 1.A . Let:

$$(5.2) \qquad \mathcal{T}^{symm}(Y,\varphi;r) \xrightarrow{\Phi^{symm}} \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1 \xrightarrow{pr_1} \mathcal{O}(Y,\varphi;r) \quad \xrightarrow{pr_2} \mathbb{P}^1$$

be the symmetrized Hurwitz family containing the cover $Y \xrightarrow{\varphi} \mathbb{P}^1$. We also have need for the canonical cover $\mathcal{O}(Y,\varphi;r) \xrightarrow{\psi} U_{\mathbb{P}^r}$ (as in the discussion preceeding expression (3.2)). We remind that ψ is obtained by: associate to each cover $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ the unordered collection of branch points of $\varphi(Z)$.

Consider the collection

$$\mathcal{M}(Y,\varphi;r) = (\mathcal{T}^{symm}(Y,\varphi;r),\ \Phi^{symm},\ \mathcal{O}(Y,\varphi;r), pr_1, pr_2, \psi)$$

of quasi-projective algebraic varieties. We say that a field K is a minimal field of definition of the collection $\mathcal{M}(Y,\varphi;r)$ if the following conditions are satisfied:

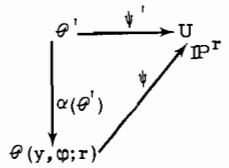
There exists a collection

$$\mathcal{M}'\{\mathcal{T}', \Phi', \mathcal{O}', pr_1', pr_2', \psi'\}$$ of quasi-projective algebraic varieties all of which are defined over K equipped with diagrams

$$(5.3a) \qquad \mathcal{T}' \xrightarrow{\Phi'} \mathcal{O}' \times \mathbb{P}^1 \xrightarrow{pr_1} \mathcal{O}' \quad \xrightarrow{pr_2} \mathbb{P}^1$$

b) $\mathcal{Q}' \xrightarrow{\psi'} U_{\mathbb{P}^r}$;

there exists isomorphisms $\alpha(\mathcal{T}')\colon \mathcal{T}' \longrightarrow \mathcal{T}^{\text{symm}}(Y,\varphi;r)$ and $\alpha(\mathcal{Q}')\colon \mathcal{Q}' \longrightarrow \mathcal{Q}(Y,\varphi;r)$, rendering an (obvious) isomorphism of the diagram (5.2) with the diagram (5.3)a) and a commutative diagram



and;

for any collection $\mathcal{M}'' = \{\mathcal{T}'', \Phi'', \mathcal{Q}'', pr_1'', pr_2'', \psi''\}$ and $\alpha(\mathcal{T}'')$, $\alpha(\mathcal{Q}'')$ as above, any field of definition of the collection $\mathcal{M}''$ contains K.

As will be seen in the proof of Theorem 5.1, it is condition (5.1) that implies the existence of a minimal field of definition of $\mathcal{M}(Y,\varphi;r)$. Theorem 5.1 is primarily concerned with the explicit computation of this field.

Let: $\{\zeta_t\}_{t\geq 1}$ be a compatible system of roots of 1; e(i) be the order of $\sigma(i)$, $i=1,\cdots,r$, and; N be the least common multiple of $e(1),\cdots,e(r)$. We identify the group $G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ with the multiplicative group $(\mathbb{Z}/(N))^*$ of invertible integers modulo N. Let $G(\mathcal{G})$ be the subgroup of S_n generated by $\sigma(1),\cdots,\sigma(r)$. For $\tau \in G(\mathcal{G})$ let $\text{Con}(\tau, G(\mathcal{G}))$ be the conjugacy class of τ in $G(\mathcal{G})$.

We define two sets:

$$\hat{M} = \Big\{ a \in (\mathbb{Z}/(N))^* \,\Big|\, \text{there exists } \beta \in S_r \text{ with } \text{Con}((\sigma(i))^a, G(\mathcal{G})) = \text{Con}(\sigma((i)\beta), G(\mathcal{G})) \text{ for } i = 1,\cdots,r \Big\}, \text{ and;}$$

$$M = \Big\{ a \in (\mathbb{Z}/(N))^* \,\Big|\, \text{there exists } \gamma \in S_n \text{ and } \beta \in S_r \text{ with } \text{Con}(\sigma(i)^a, G(\mathcal{G})) = \text{Con}(\gamma^{-1}\sigma((i)\beta)\cdot\gamma, G(\mathcal{G})) \text{ for } i = 1,\cdots,r \Big\}$$

It is easy to demonstrate that M (and therefore $\hat{M}$) is a group. Let K_M (resp. $K_{\hat{M}}$) be the fixed field of M (resp. $\hat{M}$) in $\mathbb{Q}(\zeta_N)$.

Theorem 5.1. We assume that condition (5.1) holds. Then the collection $\mathcal{M}(Y,\varphi;r)$ has a minimal field of definition which we denote by $K_{\mathcal{J}}$.

We have $K_M \subset K_{\mathcal{J}}$. In addition, if the Hurwitz number of $(\sigma(1),\cdots,\sigma(r)) = \mathcal{G}$ is 1 (see Section 4. B) we have $K_M = K_{\mathcal{J}}$.

We use the notation of Section 0. C. The field $K_{\mathcal{J}}(\theta)$ is contained in $K_{\mathcal{J}}(\mathcal{J}^{symm})$. Let $\widehat{K_{\mathcal{J}}(\mathcal{J}^{symm})}$ be the Galois closure of $K_{\mathcal{J}}(\mathcal{J}^{symm})/K_{\mathcal{J}}(\theta \times \mathbb{P}^1)$, and let $\widehat{K_{\mathcal{J}}(\theta)}$ be the algebraic closure of $K_{\mathcal{J}}(\theta)$ in $\widehat{K_{\mathcal{J}}(\mathcal{J}^{symm})}$. Then we have $K_{\widehat{M}} \subset \widehat{K_{\mathcal{J}}(\theta)}$.

Note. In the notation at the end of Section 2, $K_{\widehat{M}}$ is a portion of the fixed component of the extension of constants for the family given by (5.2). Also, it is an unsolved problem as to whether $K_M = K_{\mathcal{J}}$ when the Hurwitz number of $\mathcal{G}$ is not 1.

Proof. We consider first the collection $\mathcal{M}^{\circ}(Y,\varphi;r) = \left\{\mathcal{J}^{symm}, \Psi^{symm}, \overline{pr}_1, \overline{pr}_2\right\}$ where:

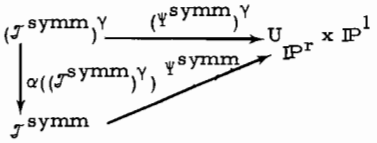
(5.4)a) $\mathcal{J}^{symm} \xrightarrow{\Psi^{symm}} U \underset{\mathbb{P}^r}{\times} \mathbb{P}^1 \xrightarrow[\overline{pr}_2]{\overline{pr}_1} U \xrightarrow{\mathbb{P}^r} \mathbb{P}^1$ and;

b) $\Psi^{symm} = (\psi \circ pr_1 \circ \Phi^{symm},\ pr_2 \circ \Phi^{symm})$.

Our first task is to show that the collection $\mathcal{M}^{\circ}(Y,\varphi;r)$ has all the properties attributed to $\mathcal{M}(Y,\varphi;r)$ in the statement of the theorem.

Let $K \subset \mathbb{C}$ be a field of finite type over $\mathbb{Q}$ containing a field of definition for each member of the collection $\mathcal{M}^{\circ}(Y,\varphi;r)$. An argument based on the proof of Lemma 1.2 allows us to assume: $[K:\mathbb{Q}] < \infty$. We also assume that $K/\mathbb{Q}$ is Galois.

For $\gamma \in G(K/\mathbb{Q})$ we define $\mathcal{M}^{\circ}(Y,\varphi;r)^{\gamma} = \left\{(\mathcal{J}^{symm})^{\gamma}, (\Psi^{symm})^{\gamma}, \overline{pr}_1^{\gamma}, \overline{pr}_2^{\gamma}\right\}$ to be transform of the collection $\mathcal{M}^{\circ}(Y,\varphi;r)$ under γ. We say that $\mathcal{M}^{\circ}(Y,\varphi;r)^{\gamma}$ is isomorphic to $\mathcal{M}^{\circ}(Y,\varphi;r)$ if there is an isomorphism $\alpha((\mathcal{J}^{symm})^{\gamma})$ rendering commutative the diagram:

(5.5)


Let H be the subgroup of $G(K/\bar{\varphi})$ consisting of those γ for which $\mathcal{M}^0(Y,\varphi;r)^{\gamma}$ is isomorphic to $\mathcal{M}^0(Y,\varphi;r)$. Let $K_{\mathcal{T}}$ be the fixed field in K of H. So far we have not used the fact that $Aut(Y,\varphi) = \{Id.\}$. We call $K_{\mathcal{T}}$ the field of moduli of the collection $\mathcal{M}^0(Y,\varphi;r)$, in analogy with [Sh and Ta; pp. 32-35]. This concept will be used again in comments in Section 6 (example 8).

Since we assume $Aut(Y,\varphi) = \{Id.\}$, we see that if $\mathcal{M}^0(Y,\varphi;r)^{\gamma}$ and $\mathcal{M}^0(Y,\varphi;r)$ are isomorphic, there is a unique isomorphism $\alpha((\mathcal{T}^{symm})^{\gamma})$ making (5.5) commutative. Therefore, from [We] we may assume that $K_{\mathcal{T}}$ is a minimal field of definition of $\mathcal{M}^0(Y,\varphi;r)$ (in analogy with the definition preceding the statement of this theorem).

We refer to our next computation as:

The Branch Cycle Argument.

An approximation to this was used earlier in [Fr, 3] and in [Shih].

Let $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ be a cover (non-singular and projective) defined over a number field L, with: a description of its branch cycles given by $\sigma(1,Z),\cdots,\sigma(r,Z)$, corresponding respectively to branch points $u(1,Z),\cdots,u(r,Z)$. In analogy with previous notation consider: $e(1,Z),\cdots,e(r,Z)$; N(Z); L(Z), $\widehat{L(Z)}$, and; the algebraic closure of L in $\widehat{L(Z)}$, denoted $\hat{L}$ if no confusion will occur. Let x be a uniformizing parameter for $\mathbb{P}^1$.

Consider the automorphism $\bar{\sigma}(i)$ of $\bar{\varphi}(((x - u(i,Z))^{1/e(i,Z)}))$ which is the identity on $\bar{\varphi}$ and maps $(x - u(i,Z))^{1/e(i,Z)}$ to $\zeta_{e(i,Z)} \cdot (x - u(i,Z))^{1/e(i,Z)}$. We remind that $x - u(i,Z)$ is replaced by $1/x$ when $u(i,Z) = \infty$. We have the embedding, via Puiseux expansions

(5.6) $$\widehat{L(Z)} \xrightarrow{\widehat{\psi(i,Z)}} \bar{\varphi}(((x - u(i,Z))^{1/e(i,Z)})),\ i = 1,\cdots,r$$

where $\sigma(i,Z)$ is the restriction to $\widehat{L(Z)}$ of $\bar{\sigma}(i)$.

For any other embedding (fixed on $L(x)$)

$$\widehat{L(Z)} \xrightarrow{\widehat{\psi'(i,Z)}} \overline{\varphi} \quad (((x - u(i,Z))^{1/e(i,Z)}))$$

$\overline{\sigma}(i)$ restricts to some element of $\mathrm{Con}(\sigma(i,Z), G(\widehat{L(Z)}/L(\mathbb{P}^1)))$. If $\widehat{\psi'(i,Z)}$ is fixed on $\hat{L}$ then the restriction of $\overline{\sigma}(i)$ is in $\mathrm{Con}(\sigma(i,Z), G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))$.

Suppose now that $G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))$ is isomorphic to $G(\widehat{\mathbb{C}(Y)}/\mathbb{C}(\mathbb{P}^1))$, and suppose also that in this isomorphism $\sigma(i,Z) \in \mathrm{Con}(\sigma(i), G(\widehat{\mathbb{C}(Y)}/\mathbb{C}(\mathbb{P}^1))$. In particular, from the computations of Section 4, this holds for all covers in the family given by expression (5.2). We now show that $K_M \subset L$ (see statement of the theorem).

Suppose, in fact, that $K_M \not\subset L$. Then, there exists $\omega \in G(\overline{\varphi}/\varphi)$ such that ω is fixed on L, but ω is not fixed on K_M. Thus, the restriction of ω to $\varphi(\zeta_N)$ corresponds to $a(\omega) \in (\mathbb{Z}/(N))^*$ such that: there does not exist a $\beta \in S_r$ and a $\gamma \in S_n$ with

$$\mathrm{Con}(\sigma(i)^{-a(\omega)}, G(\underset{\sim}{\sigma})) = \mathrm{Con}(\gamma^{-1} \cdot \sigma((i)\beta) \cdot \gamma, G(\underset{\sim}{\sigma})) \text{ for all } i = 1, \cdots, r. \tag{5.7}$$

Let ω^* be an element of $G(\widehat{L(Z)}/L(\mathbb{P}^1))$ whose restriction to $\hat{L}$ is equal to ω restricted to $\hat{L}$. We extend ω to $\overline{\varphi}((x - u(i,Z))^{1/e(i,Z)}))$ by:
$\omega(\sum_k a_k(x - u(i,Z))^{k/e(i,Z)}) = \sum_k \omega(a_n)(x - u(j,Z))^{k/e(j,Z)}$ where $\omega(u(i,Z)) = u(j,Z)$. Note that we automatically have $e(i,Z) = e(j,Z)$.

Thus we obtain:

$$\widehat{L(Z)} \xrightarrow{\omega \circ \widehat{\psi(i,Z)}} \overline{\varphi}((x - u(j,Z))^{1/e(j,Z)}) \,. \tag{5.8}$$

For $\alpha \in \widehat{L(Z)}$ we compute the restriction of $\overline{\sigma}(j)$ to α as:
$\widehat{\psi(i,Z)}^{-1} \circ \omega^{-1} \circ \overline{\sigma}(j) \circ \omega \circ \widehat{\psi(i,Z)}$. By direct computation on the Puiseux expansion $\widehat{\psi(i,Z)}(\alpha)$ we see that this is the same as $\widehat{\psi(i,Z)}^{-1} \circ \overline{\sigma(i)}^{-a(\omega)} \circ \widehat{\psi(i,Z)}$, which is $\sigma(i)^{-a(\omega)}$. Since $\widehat{\psi(i,Z)}^{-1} \circ \omega^{-1} \circ \overline{\sigma}(j) \circ \omega \circ \widehat{\psi(i,Z)}$ is the identity on $\hat{L}$ (when applied to $\widehat{L(Z)}$), this is in $\mathrm{Con}(\sigma(j), G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1)))$, or

$$\mathrm{Con}(\sigma(i)^{-a(\omega)}, G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))) = \mathrm{Con}(\omega^{*-1} \cdot \sigma(j) \circ \omega^*, G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))). \tag{5.9}$$

However, with the aforementioned identification of $G(\mathfrak{L})$ with $G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))$, etc., expression (5.9) contradicts (5.7). Therefore $K_M \subset L$.

Now we show that $K_{\hat{M}} \subseteq \hat{L}$. If we assume that $K_{\hat{M}} \not\subseteq \hat{L}$ and proceed as above, we end up with the expression;

$$\mathrm{Con}(\sigma(i)^{-a(\omega)},\ G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))) = \mathrm{Con}(\sigma(j),\ G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))$$

where j is defined by $\omega(u(i, Z)) = u(j, Z)$. Again, this is a contradiction (from the definitions of $K_{\hat{M}}$ and $a(\omega)$).

We need an addition to the branch cycle argument to describe what happens when we apply $\omega \in G(\overline{\varphi}/\varphi)$ to $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ when ω is not the identity on L.

Let L^ω be the image of L under ω. Let $Z^\omega \xrightarrow{\varphi(Z)^\omega} \mathbb{P}^1$ be the transform of $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ by ω. By operating on the coefficients of the Puiseux expansions, as above, we obtain:

$$\omega : \overline{\varphi}((\,(x - u(i, Z))^{1/e(i,Z)}\,)) \longrightarrow \overline{\varphi}((\,(x - \omega(u(i, Z))^{1/e(i,Z)}\,)).$$

We define $\hat{\omega}$ so as to make the following diagram commutative:

$$\begin{array}{ccc} \widehat{L(Z)} & \xrightarrow{\psi(\widehat{i, Z})} & \overline{\varphi}((\,(x - u(i, Z))^{1/e(i,Z)}\,)) \\ \downarrow \hat{\omega} & & \downarrow \omega \\ \widehat{L^\omega(Z^\omega)} & \xrightarrow{\psi(\widehat{i, Z})^\omega} & \overline{\varphi}((\,(x - \omega(u(i,Z)))^{1/e(i,Z)}\,)) \end{array}$$

From $\hat{\omega}$ we obtain an isomorphism between the group $G(\widehat{L(Z)}/L(\mathbb{P}^1))$ and $G(\widehat{L^\omega(Z^\omega)}/L^\omega(\mathbb{P}^1))$ given by: $\sigma \longrightarrow \hat{\omega} \cdot \sigma \cdot \hat{\omega}^{-1} \overset{\text{def}}{=} \sigma^\omega$ for $\sigma \in G(\widehat{L(Z)}/L(\mathbb{P}^1))$. Also, if σ is fixed on $\hat{L}$, then $\hat{\omega} \cdot \sigma \cdot \hat{\omega}^{-1}$ is fixed on $\hat{L}^\omega$, so we have an isomorphism of $G(\widehat{L(Z)}/\hat{L}(\mathbb{P}^1))$ and $G(\widehat{L^\omega(Z^\omega)}/\hat{L}^\omega(\mathbb{P}^1))$.

If we identify these two groups by this isomorphism and call the resulting abstract group G, then (by an argument analogous to that above) we see that $Z^\omega \xrightarrow{\varphi(Z)^\omega} \mathbb{P}^1$ has a description of its branch cycles given by $\sigma(i, Z^\omega)$ (the branch cycle over $\omega(u(i, Z))$) where

$$\sigma(i, Z^\omega) \in \mathrm{Con}(\sigma(i, Z)^{-a(\omega)},\ G). \tag{5.10}$$

With this we conclude the computations we need from the branch cycle argument.

Finish of the proof of Theorem 5.1.

At the beginning of this proof we showed that $\mathcal{M}^0(Y,\varphi;r)$ has a minimal field of definition, designated $K_{\mathcal{J}}$. We finish the proof in steps.

Step 1. We show $K_{\mathcal{J}}$ is a minimal field of definition of the collection $\mathcal{M}(Y,\varphi;r)$.

Again using the proof of Lemma 1.2 we may assume that $\mathcal{M}(Y,\varphi;r)$ is defined over a finite extension of $\mathbb{Q}$ and, for $\gamma \in G(\bar{\mathbb{Q}}/\mathbb{Q})$ we may consider $\mathcal{M}(Y,\varphi;r)^{\gamma}$ (the transform of the collection $\mathcal{M}(Y,\varphi;r)$). Consider $\gamma \in G(\bar{\mathbb{Q}}/K_{\mathcal{J}})$. Apply γ to:

$$(5.11)a) \qquad \mathcal{J}^{\text{symm}}(Y,\varphi;r) \xrightarrow{\Phi^{\text{symm}}} \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1 \xrightarrow{\psi \times \text{Id.}} U_{\mathbb{P}^r} \times \mathbb{P}^1$$

to obtain

$$(5.11)b) \qquad \mathcal{J}^{\text{symm}}(Y,\varphi;r) \xrightarrow{(\Phi^{\text{symm}})^{\gamma}} \mathcal{O}(Y,\varphi;r)^{\gamma} \times \mathbb{P}^1 \xrightarrow{\psi^{\gamma} \times \text{Id.}} U_{\mathbb{P}^r} \times \mathbb{P}^1.$$

For $\underset{\sim}{p} \in \mathcal{O}(Y,\varphi;r)$, there is a unique point in $\mathcal{O}(Y,\varphi;r)^{\gamma}$ (denoted $\alpha(\gamma)(\underset{\sim}{p}) \in \mathcal{O}(Y,\varphi;r)^{\gamma}$) over $\psi(\underset{\sim}{p})$ such that: $(\mathcal{J}^{\text{symm}}(Y,\varphi;r))_{\underset{\sim}{p}} \longrightarrow \underset{\sim}{p} \times \mathbb{P}^1$ is isomorphic to

$(\mathcal{J}^{\text{symm}}(Y,\varphi;r))_{\alpha(\gamma)(\underset{\sim}{p})} \longrightarrow \alpha(\gamma)(\underset{\sim}{p}) \times \mathbb{P}^1$. From the construction of Hurwitz families in Section 4, the map $\alpha(\gamma) : \mathcal{O}(Y,\varphi;r) \longrightarrow \mathcal{O}(Y,\varphi;r)^{\gamma}$ is easily shown to be an analytic isomorphism. Also, the maps $\alpha(\gamma') \circ \alpha(\gamma)^{-1} : \mathcal{O}(Y,\varphi;r)^{\gamma} \longrightarrow \mathcal{O}(Y,\varphi;r)^{\gamma'}$ (for $\gamma,\gamma' \in G(\bar{\mathbb{Q}}/K_{\mathcal{J}})$) satisfy Weil's cocycle criteria. Therefore $\mathcal{O}(Y,\varphi;r)$ can be defined over $K_{\mathcal{J}}$. It is a cumbersome, but essentially obvious calculation to show now that $\mathcal{M}(Y,\varphi;r)$ is defined over $K_{\mathcal{J}}$.

Step 2. We show $K_M \subset K_{\mathcal{J}}$ and $K_M^{\wedge} \subset \widehat{K_{\mathcal{J}}(\mathcal{O})}$.

Suppose K_M is not contained in $K_{\mathcal{J}}$, so that $[K_M \cdot K_{\mathcal{J}} : K_{\mathcal{J}}] > 1$. Then from Hilbert's Irreducibility Theorem there exists a point $\underset{\sim}{p} \in \mathcal{O}$, algebraic over $K_{\mathcal{J}}$, such that $K_{\mathcal{J}}(\underset{\sim}{p})$ is disjoint from $K_M \cdot K_{\mathcal{J}}$ over $K_{\mathcal{J}}$. Therefore

$$(5.12) \qquad (\mathcal{J}^{\text{symm}}(Y,\varphi;r))_{\underset{\sim}{p}} \xrightarrow{\text{restriction of } pr_2 \circ \Phi^{\text{symm}}} \mathbb{P}^1$$

is a cover defined over $K_{\mathcal{T}}(\underset{\sim}{p})$. This contradicts the part of the Branch Cycle Argument which showed that any field of definition of (5.12) contains K_M.

A calculation similar to this using Lemma 2.3 can be used to show that $K_M^{\wedge} \subset K_{\mathcal{T}}(\theta)$.

Step 3. When the Hurwitz Number is 1, $K_M = K_{\mathcal{T}}$.

Suppose $K_{\mathcal{T}} \not\supset K_M$. Then there exists $\gamma \in G(\bar{\Phi}/K_M)$ such that γ is not fixed on $K_{\mathcal{T}}$. Let $\underset{\sim}{p} \in \theta(Y,\varphi;r)$ be algebraic over $K_{\mathcal{T}}$. We apply γ to the diagram.

(5.13)a)
$$\begin{array}{ccc} (\mathcal{T}^{\text{symm}}(Y,\varphi;r))_{\underset{\sim}{p}} & \hookrightarrow & \mathcal{T}^{\text{symm}}(Y,\varphi;r) \\ \downarrow & & \downarrow \\ \underset{\sim}{p} \times \mathbb{P}^1 & \hookrightarrow & \theta(Y,\varphi;r) \times \mathbb{P}^1 \end{array}$$

to obtain

(5.13)b)
$$\begin{array}{ccc} ((\mathcal{T}^{\text{symm}}(Y,\varphi;r)^{\gamma})_{\gamma(\underset{\sim}{p})} & \hookrightarrow & (\mathcal{T}^{\text{symm}}(Y,\varphi;r)^{\gamma} \\ \downarrow & & \downarrow \\ \gamma(\underset{\sim}{p}) \times \mathbb{P}^1 & \hookrightarrow & \theta(Y,\varphi;r)^{\gamma} \times \mathbb{P}^1 \end{array}$$

However, the last calculation of the Branch Cycle Argument tells us that if $\sigma(1),\cdots,\sigma(r)$ are a description of the branch cycles of the cover in the left vertical in the diagram (5.13)a), then $\tau(1),\cdots,\tau(r)$ is a description of the branch cycles in the cover in the left vertical of diagram (5.13)b), where: $\tau(1),\cdots,\tau(r)$ generates $G(\mathcal{Y})$, and, $\tau(i)$ is conjugate to $\sigma(i)$ in $G(\mathcal{Y})$ for $i = 1,\cdots,r$. Since the Hurwitz number is 1 this implies that the cover of the left vertical in diagram (5.13)b) actually appears as a fiber in the family

(5.14) $$\mathcal{T}^{\text{symm}}(Y,\varphi r) \longrightarrow \theta(Y,\varphi;r) \times \mathbb{P}^1 .$$

From the uniqueness of the Symmetrized Hurwitz family containing the cover of the left vertical of diagram (5.13)b) (under condition (5.1)) this implies

that the cover $(\mathcal{T}^{\text{symm}}(Y,\varphi;r))^{\gamma} \xrightarrow{(\Phi^{\text{symm}})^{\gamma}} \mathcal{O}(Y,\varphi;r)^{\gamma} \times \mathbb{P}^1$ is isomorphic to the cover (5.14). Since γ is not fixed on $K_{\mathcal{T}}$ this contradicts the properties we have proven for $K_{\mathcal{T}}$ (it is a field of moduli for $\mathcal{M}(Y,\varphi;r)$). With this contradiction we conclude the proof of Theorem 5.1. ■

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover (as in the beginning of this section) with a description of its branch cycles given by $\sigma(1),\cdots,\sigma(r)$. We do not assume that $\text{Aut}(Y,\varphi) = \{\text{Id.}\}$.

Corollary 5.2 Let L be any field of definition of (Y,φ). Then $K_M \subset L$. Let $\hat{L}$ be the algebraic closure of L in $\widehat{L(Y)}$ (the Galois closure of $L(Y)/L(\mathbb{P}^1)$). Then $K_M \subset \hat{L}$.

Proof. This was proved in the Branch Cycle Argument part of the proof of Theorem 5.1. ■

As a part of Theorem 5.1 we immediately obtain

Corollary 5.3 Assume in addition to the hypotheses of Corollary 5.2 that $\text{Aut}(Y,\varphi) = \{\text{Id.}\}$ and, the Hurwitz number of $\sigma(1),\cdots,\sigma(r)$ is 1. Then the Hurwitz Parameter space (Hurwitz scheme) $\mathcal{O}(Y,\varphi;r)$ is defined over K_M.

Note: There are simple examples (eg. the three Branch point case) to show that the cover $\mathcal{O}(Y,\varphi;r) \xrightarrow{\Psi} U_{\mathbb{P}^r}$ may be defined over a field strictly contained in K_M. However, since $\text{Aut}(\mathcal{O}(Y,\varphi;r),\Psi)$ is usually not the identity group, it can be a difficult problem to directly compute the 'correct' field of definition of $(\mathcal{O}(Y,\varphi;r),\Psi)$.

Corollary 5.4 Assume that (Y,φ) satisfies the hypotheses of Corollary 5.3. Let $K(\mathcal{C})$ be the intersection of all fields of definition of all pairs $(Z,\varphi(Z))$ where $Z \xrightarrow{\varphi(Z)} \mathbb{P}^1$ has a description of its branch cycles given by $\sigma(1),\cdots,\sigma(r)$. Then $K(\mathcal{C}) = K_M$.

Proof. For $\underline{p} \in \mathcal{O}(Y,\varphi;r)$, the cover $\mathcal{T}^{symm}(Y,\varphi;r) \longrightarrow \underline{p} \times \mathbb{P}^1$ (obtained from the fiber over $\underline{p}$ of $\mathcal{T}^{symm}(Y,\varphi;r) \to \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$) is defined over $K_M(\underline{p})$. From Hilbert's irreducibility theorem applied to $\mathcal{O}(Y,\varphi;r) \xrightarrow{\Psi} U_{\mathbb{P}^r}$ the field $\bigcap_{\underline{p} \in \mathcal{O}(Y,\varphi;r)} K_M(\underline{p}) = K_M$. ∎

Let G be a finite group, and let L be a number field. We now discuss some important problems.

Problem 5.5 Show that there exists $Y \xrightarrow{\varphi(Y)} \mathbb{P}^1$ such that: (Y,φ) is defined over a number field K ; $G(\hat{Y}/\hat{K}(\mathbb{P}^1)) = G$, and; $\hat{K}$ is disjoint from L over $\mathbb{Q}$.

Consider a group G with a faithful transitive representation $T : G \longrightarrow S_n$ with:

(5.15) $N(G(1))/G(1) = \{Id.\}$ (notation of Lemma 2.1)

Suppose we could show that:

(5.16)a) even if the Hurwitz number of $(Y,\varphi(Y))$ is not 1, then $\mathcal{M}(Y,\varphi;r)$ (see above) is defined over K_M, and;

b) for $\sigma(1),\cdots,\sigma(r)$ (a description of the branch cycles of (Y,φ) including all conjugacy classes of G, then $\widetilde{K_M(\mathcal{T}^{symm}(Y,\varphi;r))}$ (Galois closure of the cover $\mathcal{T}^{symm}(Y,\varphi;r) \longrightarrow \mathcal{O}(Y,\varphi;r) \times \mathbb{P}^1$) has its absolute constants equal to $\hat{K}_M$.

Under these conditions we can choose $\sigma(1),\cdots,\sigma(r)$ so that for each integer a there exists $\beta \in S_r$ such that:

$Con(\sigma(i)^a, G(\mathcal{Q})) = Con(\sigma((i)\beta), G(\mathcal{Q}))$ for $i = 1,\cdots,r$ (discussion before Theorem 5.1). Then $K_{\hat{M}} = \mathbb{Q}$, and by the assumption of (5.16)b) and an application of Hilbert's Irreducibility Theorem (as in the proof of Corollary 5.3) we can affirm a positive solution to Problem 5.5 for (G, T) satisfying (5.15). However, there is no special reason at this time to believe either (5.16)a) or b).

It is an extremely important problem to consider groups G equipped with a faithful transitive representation T for which (5.15) does not hold. In order

to consider this problem it is necessary to consider covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ equipped with the extra structure coming from a characteristic subgroup H of $\mathrm{Aut}(Y,\varphi)$ Suppose we are given two such structures $(Y_1,\varphi_1,\ H(Y_1,\varphi_1),\ S(Y_1))$ and $(Y_2,\varphi_2,H(Y_2,\varphi_2),\ S(Y_2))$ where: $S(Y_i) : H(Y_i,\varphi_i) \to H$ is an isomorphism of $H(Y_i,\varphi_i)$ with the abstract group H. We say that these two structures are isomorphic if there exists an analytic isomorphism $\alpha : Y_1 \to Y_2$ with:

$\alpha : Y_1 \to Y_2$ is commutative, and;

$\varphi(Y_1)$ $\searrow$ $\swarrow$ $\varphi(Y_2)$

$\mathbb{P}^1$

$$\alpha^{-1} \circ S(Y_2)^{-1}(g) \circ \alpha = S(Y_1)^{-1}(g) \quad \text{for all } g \in H.$$

The construction of moduli schemes and total families analogous to the construction of $\mathcal{P}(Y,\varphi;r)$ and $\mathcal{T}^{\mathrm{symm}}(Y,\varphi;r)$ is considered in [Fr, 2]. The search for the fields of definition of these new objects is a contribution to the extension of the results of this section to the more general case. Unfortunately, when the center of $\mathrm{Aut}(Y,\varphi)$ is <u>not</u> the identity there are great difficulties which require consideration of still further structure utilizing the Jacobian variety of Y.

<u>Section 6. Examples: A_n; Mathieu group of degree 11; Elementary Groups; Hurwitz Monodromy Representation (the Projective Symplectic group).</u>

This Section consists of an historical discussion followed by a sequence of examples that are placed here to (hopefully) illuminate the theory of the preceding sections. We start with a more modern treatment of the examples in [Hi] by discussing Hilbert's method of realizing A_n as a Galois group over $\mathbb{Q}$ (as the Galois group of a regular extension of $\mathbb{Q}(x)$). This example is sufficiently rich to reveal several aspects of our results. At the same time it can be read independently of the remainder of the paper; a fact which may recommend it to the reader who needs help with some of the concepts

of Sections 2 and 5. Let H be a group. In the examples we will use the phrase "we have solved the one-variable problem for H over K". This means: we have found a Galois regular extension L of $K(\mathbb{P}^1)$ such that $G(L/K(\mathbb{P}^1)) \simeq H$.

We start with the natural map: $\gamma : \mathbb{A}^n \to \mathbb{A}^n$ by $(x_1, \ldots, x_n) \to (\varepsilon_1(\underset{\sim}{x}), \ldots, \varepsilon_n(\underset{\sim}{x}))$ where $\varepsilon_i(\underset{\sim}{x})$ is the i-th elementary symmetric function in $x_1, \ldots, x_n$. Then γ presents $\mathbb{A}^n$ as a quotient of $\mathbb{A}^n$ be the action of S_n: permutation of the coordinates of $\mathbb{A}^n$ by the rule

$$(6.1) \qquad (x_i)\sigma = x_{(i)\sigma} \quad \text{for } i = 1, \ldots, n, \ \sigma \in S_n.$$

The morphism γ extends to a morphism

$$\bar{\gamma} : \underbrace{\mathbb{P}^1 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1}_{n \text{ times}} \to \mathbb{P}^n.$$

The Hurwitz Monodromy group may be defined as the fundamental group of the complement of the branch locus of $\bar{\gamma}$ in $\mathbb{P}^n$. It is through the use of Hurwitz families and symmetrized Hurwitz families that explicit permutation representations of the Hurwitz monodromy group are most easily understood.

We may regard γ as the map that associates to an ordered n-tuple of roots $x_1, \ldots, x_n$ of a polynomial $\prod_{i=1}^{n}(z - x_i) = f(z)$ the coefficients of f(z). Thus, by applying Hilbert's irreducibility theorem to $-\gamma$ we immediately obtain: there exists a monic polynomial of degree n, $f(z) \in \mathbb{Z}[z]$, such that the splitting field Ω_f of f(z) over Φ satisfies $G(\Omega_f/\Phi) \simeq S_n$.

Example 4. The alternating group of Degree n.

There are many different ways to find covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ such that: (Y, φ) is defined over Φ; $\deg(\varphi) = n$, and; the geometric monodromy group, $G(\widehat{\bar{\Phi}(Y)}/\bar{\Phi}(\mathbb{P}^1))$ is S_n. Therefore $G(\widehat{\Phi(Y)}/\Phi(\mathbb{P}^1))$ is also S_n, and $\widehat{\Phi(Y)}$ is a regular Galois extension of $\Phi(\mathbb{P}^1)$ having Galois group S_n. We mention the most general way we know to effect a construction of such pairs (Y, φ). Let Y be any curve defined over Φ. In [Fr and Ja] it is shown that there

exists φ so that $Y \xrightarrow{\varphi} \mathbb{P}^1$ is a simple branched cover (see example 1) defined over $\mathbb{Q}$ so long as $n = \deg(\varphi) \geq 2g + 1$ where $g = g(Y)$ is the genus of Y. Thus (Y, φ) satisfies the conditions above.

To achieve a construction for the alternating group we start with a construction of S_n by use of covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ with branch points $u(1,Y)$, $u(2,Y)$, $u(3,Y)$ having a description of its branch cycles given (respectively) by $\sigma(1,Y) = (12)$, $\sigma(2,Y) = (134\cdots n)$, $\sigma(3,Y) = (12\cdots n)^{-1}$. Clearly, $\sigma(i,Y)$, $i = 1,2,3$ generate S_n. Suppose $\tau(1)$, $\tau(2)$, $\tau(3)$ are in S_n and $\tau(1)$ is a 2-cycle, $\tau(2)$ is an $(n-1)$-cycle and $\tau(3)$ is an n-cycle such that the product of $\tau(1)$, $\tau(2)$, and $\tau(3)$ is the identity. Then it is easy to demonstrate that there exists $\alpha \in S_n$ such that: $\sigma(i,Y) = \alpha^{-1} \circ \tau(i) \circ \alpha$ for $i = 1,2,3$. Let $K = \mathbb{Q}(u(1,Y), u(2,Y), u(3,Y))$ be the field generated by $u(i,Y)$, $i = 1,2,3$. If $\beta \in G(\mathbb{C}/K)$ then $Y^{\beta} \xrightarrow{\varphi^{\beta}} \mathbb{P}^1$ has the same branch points and description of its branch cycles as does $Y \xrightarrow{\varphi} \mathbb{P}^1$. Thus the two covers are isomorphic by Riemann's existence theorem; by a unique isomorphism from Lemma 2.1. Therefore, Weil's cocycle criteria ([We]) implies that (Y, φ) can be defined over K. From now on we assume $u(i,Y) \in \mathbb{Q}$, $i = 1,2,3$, and $K = \mathbb{Q}$.

Let A_n be the alternating group of degree n regarded as a subgroup of $G(\widehat{\mathbb{Q}(Y)}/\mathbb{Q}(\mathbb{P}^1))$. Let $\mathbb{Q}(Z)$ be the fixed field of A_n. Then $\widehat{\mathbb{Q}(Y)}$ is a Galois regular extension of $\mathbb{Q}(Z)$, with group A_n. If we show that $\mathbb{Q}(Z)$ is of genus zero with a $\mathbb{Q}$-rational place, then we have solved the one-variable problem for A_n over $\mathbb{Q}$. However $\mathbb{Q}(Z)$ is a degree 2 extension of $\mathbb{Q}(\mathbb{P}^1)$ ramified at, at most, 3 places $(u(i,Y), i = 1,2,3)$. Thus the genus of $\mathbb{Q}(Z)$ is computed to be zero by the Riemann-Hurwitz formula, and since the branch points are $\mathbb{Q}$-rational, the ramified places of $\mathbb{Q}(Z)$ must also be $\mathbb{Q}$-rational. This concludes our argument.

Nevertheless, we feel that it is worth considering this construction directly from a description of the branch cycles for $\mathbb{Q}(Y)$ over $\mathbb{Q}(Z)$.

There are two very similar cases to consider: n even and n odd. For simplicity we choose n even.

Let $\tau(1,W) = (1\,3\cdots n)$, $\tau(2,W) = (1245\cdots n)$, and $\tau(3,W) = (12\cdots n)^{-2}$. Then $\tau(1,W)$, $\tau(2,W)$, $\tau(3,W)$ are a description of the branch cycles for a cover $W \xrightarrow{\varphi(W)} \mathbb{P}^1$ with: $(W, \varphi(W))$ defined over $\mathbb{C}$, and; $G(\widehat{\mathbb{C}(W)}/\mathbb{C}(\mathbb{P}^1)) \simeq A_n$ (with the standard representation of A_n coming from the action on the right cosets of $G(\widehat{\mathbb{C}(W)}/\mathbb{C}(W))$. We denote by $u(1,W)$, $u(2,W)$, $u(3,W)$ the branch points of $\varphi(W)$ corresponding (respectively) to $\tau(1,W)$, $\tau(2,W)$, $\tau(3,W)$. The problem (already solved by trickery above) is to choose $u(1,W)$, $u(2,W)$, $u(3,W)$ in Φ so that: $(W,\varphi(W))$ is defined over Φ, and; the algebraic closure Φ of Φ in $\widehat{\Phi(W)}$ is just Φ. In order to simplify our exposition of the combinatorics we consider the case $n = 6$. In fact, the case $n \neq 6$ is sufficient to illustrate that computations on such problems as these becomes extremely cumbersome without some sophisticated trickery.

Consider all triples $(\tau(1), \tau(2), \tau(3))$ where: $\tau(i) \in A_6$, $i = 1, 2, 3$; $\tau(1)$, $\tau(2)$ are 5-cycles and $\tau(3)$ is a product of 2 disjoint 3-cycles, and; $\tau(1)\cdot\tau(2)\cdot\tau(3) = \mathrm{Id}$. We need only consider such triples up to equivalence obtained by conjugation of the triple by an element of S_6. Therefore, with no loss we may assume $\tau(1) = (13456)$, and (by conjugation of the triple by a power of $\tau(1)$) we may assume that $\tau(2)$ fixes 3, so $\tau(3)$ moves 3 to 1. Thus, the 8 possibilities for $\tau(3)$ are: (312)(456); (312)(654); (314)(256); (314)(265); (315)(246); (315)(642); (316)(245), and; (316)(542). Of these, the only ones for which $\tau(1)^{-1}\tau(3)^{-1} = \tau(2)$ is a 5-cycle are:

(6.2) a) $\tau(2) = (64215)$; $\tau(3) = (312)(456)$;

b) $\tau(2) = (61452)$; $\tau(3) = (315)(246)$;

c) $\tau(2) = (61245)$, $\tau(3) = (315)(642)$.

Of these, the cases we are interested in are those for which $\tau(1)$, $\tau(2)$, $\tau(3)$ generate the whole alternating group. There are proper doubly transitive proper subgroups of A_6. These are: $PGL(2, \mathbb{Z}/(5)) \overset{\text{def}}{=} \{$invertible transformations on $\mathbb{Z}/(5) \cup \infty$ given by $x \longrightarrow \frac{ax+b}{cx+d}$ (Möbius transformations); a, b, c, d in $\mathbb{Z}/(5)\}$; the subgroup of $PGL(2, \mathbb{Z}/(5))$ represented by transformations with $ad - bc$ a square in $\mathbb{Z}/(5)$, and; conjugates of these groups in A_6. Consider $\overline{\tau}(1) : x \longrightarrow \frac{1}{x+1}$, $\overline{\tau(2)} : x \longrightarrow x + 1$, as permutations on 0, 1, 2, 3, 4, ∞ (modulo 5) these are given by $\overline{\tau}(1) = (0134\infty)$, $\overline{\tau(2)} = (01234)$. Thus $\overline{\tau(1)} \cdot \overline{\tau(2)} = (023)(4\infty 1)$. By making, in order, the substitutions $4 \to 1$, $\infty \to 3$, $0 \to 4$, $1 \to 5$, $3 \to 6$, we see that the triple $\left(\overline{\tau(1)}, \overline{\tau(2)}, \left(\overline{\tau(1)} \cdot \overline{\tau(2)}\right)^{-1}\right)$ is equivalent to the triple of branch cycles in (6.2) b). We do not bother with cycles of (6.2)a), but restrict attention to the cycles of (6.2)c). We can check to see that the Hurwitz number of the branch cycles of (6.2) c) is 1 and that Theorem 5.1 implies that the symmetrized Hurwitz family containing covers of $\mathbb{P}^1$ with branch cycles given by (6.2) c) is defined over Φ. In addition we compute that there exists $\alpha \in S_6$ such that $\left(\alpha \cdot \tau(2) \cdot \alpha^{-1}, \alpha \cdot \tau(2)^{-1} \cdot \tau(1) \cdot \tau(2) \cdot \alpha^{-1}, \alpha \cdot \tau(3) \cdot \alpha^{-1}\right)$ and $\left(\tau(1), \tau(2), \tau(3)\right)$ are the same. Therefore (see example 2 or go back to the results of the constructions of Section 4) the Hurwitz parameter space $\mathcal{H}$ is a degree 3 cover of an open subset of $\mathbb{P}^3$, and in turn is covered by an open subset of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. Therefore $\Phi(\mathcal{H})$ is easily seen to be a purely transcendental function field over Φ, generated by the functions of u(1), u(2), u(3) (branch point parameters) which are symmetric in u(1) and u(2) (functions of u(1) + u(2), u(1) · u(2), and u(3)). Let $\underline{p} \in \mathcal{H}_\Phi$ (Φ - rational points of $\mathcal{H}$), and let $Y_{\underline{p}} \xrightarrow{\varphi_{\underline{p}}} \mathbb{P}^1$ be the fiber above $\underline{p}$ in the Hurwitz family. Then $(Y_{\underline{p}}, \varphi_{\underline{p}})$ is defined over Φ. For simplicities sake assume that $\underline{p}$ is the image of Φ-rational point of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ so that the branch points of $\varphi_{\underline{p}}$ are Φ-rational. We abuse notation and let $\hat{\varphi}_{\underline{p}}$ be

the algebraic closure of φ in $\widehat{\varphi(Y_{\underline{p}})}$ (Galois closure of $\varphi(Y_{\underline{p}}/\varphi(\mathbb{P}^1))$. If we show that $\hat{\varphi}_{\underline{p}} = \varphi$ then $G(\widehat{\varphi(Y_{\underline{p}})}/\varphi(\mathbb{P}^1)) = A_6$ and we will have directly solved the one variable problem for A_6 over φ. From the version of Hilbert's argument we know, a priori, that we indeed have $\hat{\varphi}_{\underline{p}} = \varphi$. In addition, from Proposition 2, $\hat{\varphi}_{\underline{p}}$ is in the intersection of the decomposition fields of primes of $\widehat{\varphi(Y_{\underline{p}})}$. Let L be the residue class field of one of the two primes of $Y_{\underline{p}}$ above u(3). Then we easily compute that $\hat{\varphi}_{\underline{p}}$ is contained in $L \cdot \varphi(\zeta_3) \cap \varphi(\zeta_5)$ (where ζ_n is a primitive n-th root of 1). If we show that $L = \varphi$ (or just that $L \cap \varphi(\zeta_5) = \varphi$) then $\hat{\varphi}_{\underline{p}} = \varphi$, and we are done. This is so, from the first part of the example, but we have, as yet, no direct argument for this.

Below we state a problem for which an affirmative answer would contribute immensely to the understanding of extension of constants. In particular, as we show, it would provide the direct argument required to complete this example. ■

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover with (Y, φ) defined over F $(F \subseteq \mathbb{C})$. For simplicity of discussion only, we assume that the branch points $u(1), \ldots, u(r)$ of φ are F-rational. By use of Puiseux expansions we obtain an embedding (fixed on F)

$$\widehat{F(Y)} \xrightarrow{\widehat{\Psi(i)}} \overline{F}\left(\left((x - u(i))^{1/e(i)}\right)\right)$$

where $e(i)$ is the order of a branch cycle $\sigma(i)$ for (Y, φ) at $u(i)$. Let $\hat{F}$ be the algebraic closure of F in $\widehat{F(Y)}$ and let $\alpha \in G(\hat{F}/F)$. Denote by $\hat{\alpha}$ any extension of α to $\overline{F}\left(\left((x - u(i))^{1/e(i)}\right)\right)$ obtained by: extending α to $\overline{F}$, and; leaving $(x - u(i))^{1/e(i)}$ fixed. Now let α^* be the restriction of $\hat{\alpha}$ to $\widehat{F(Y)}$ through the embedding $\widehat{\Psi(i)}$. Of course α^* depends on the choices of $\hat{\alpha}$ and $\widehat{\Psi(i)}$. By changing $\widehat{\Psi(i)}$ we can change α^* to any conjugate of α^* in $G = G\left(\widehat{F(Y)}/\hat{F}(\mathbb{P}^1)\right)$. Let $\mathrm{Con}(\alpha, G; u(i)) \overset{\text{def.}}{=}$ union of the conjugacy classes in G of all elements α^* obtained from a fixed α.

Problem. Show that for $i \neq j$

$$\mathrm{Con}\left(\alpha, G; u(i)\right) \cap \mathrm{Con}\left(\alpha, G; u(j)\right) \text{ is non-empty.}$$

Suppose that we can find: a universal domain M (algebraically closed and containing $\overline{F}(x)$); embeddings $\Phi(i)\colon \widehat{F(Y)} \longrightarrow M$, $\Phi(j)\colon \widehat{F(Y)} \longrightarrow M$, $\psi(i)\colon \overline{F}\left((x-u(i)^{1/e(i)})\right) \longrightarrow M$, and $\psi(j)\colon \overline{F}\left((x-u(j))^{1/e(j)}\right) \longrightarrow M$, all fixed on $F(x)$, such that $\Phi(i) = \psi(i) \circ \widehat{\psi(i)}$ and $\Phi(j) = \psi(j) \circ \widehat{\psi(j)}$. Then we can extend α on $\hat{F}$ to $\hat{\alpha}$ on M such that $\hat{\alpha}$ restricted to $F\left((x - u(i))^{1/e(i)}\right)$ and $F\left((x - u(j))^{1/e(j)}\right)$ is the identify. Thus, $\hat{\alpha}$ restricted to $\widehat{F(Y)}$, via either embedding $\Phi(i)$ or $\Phi(j)$, is an element of $\mathrm{Con}\left(\alpha, G; u(i)\right) \cap \mathrm{Con}\left(\alpha, G; u(j)\right)$.

In example 4, for $i = 2$, $j = 3$ and α the nontrivial element of $G(L/\Phi)$ we easily see that elements of $\mathrm{Con}\left(\alpha, G; u(3)\right)$ are products of 3 disjoint 2-cycles, while each of the elements of $\mathrm{Con}\left(\alpha, G; u(3)\right)$ fixes a letter. Therefore Con $(\alpha, G; u(2)$ and Con $(\alpha, G; u(3))$ have no intersection. If the problem above has an affirmative answer, we conclude that $L = \Phi$. In fact, the method would then work for the alternating group of any degree.

Example 5. Mathieu Group of Degree 11.

We quote useful facts, most of which are easy exercises in [C; p. 151, 165, 263]. For the reader's convenience we retain the notation of [C]. Let $S = (x_0 x_1 \cdots x_{10})$, $T = (x_4 x_5 x_3 x_9)(x_{10} x_7 x_2 x_6)$, and $U = (x_0 x_\infty)(x_1 x_{10})(x_2 x_5)(x_3 x_7)(x_4 x_8)(x_6 x_9)$, regarded as elements of S_{12} (letters are $x_0, x_1, \ldots, x_{10}, x_\infty$). The Mathieu group of degree 12, M_{12}, is generated by S, T, and U. If G is a k-ply transitive subgroup of S_n, not containing A_n, and if $k \geq 3$, then: every permutation of G except the identity moves at least 2k-2 symbols. From this we deduce that the 5-transitive group M_{12} is of order $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$ (the stabilizer of x_1, x_2, x_3, x_4, x_5 in M_{12} is the identity subgroup). The stabilizer of x_∞ in M_{12} is M_{11}; of order $11 \cdot 10 \cdot 9 \cdot 8$. Also, S and T generate M_{11}, so $M_{11} \subset A_{11}$.

Since M_{11} is simple it is generated by its 11-sylows (or by any of its p-sylows). Let $N(<S>)$ be the normalizer of the group generated by S in M_{11}. Let x be the number of 11-sylows. By the Sylow Theorems:

$x = \dfrac{|M_{11}|}{|N(<S>)|} \equiv 1 \bmod 11$, and; $x = 12$, 45, or 144 and $|N(<S>)| = 11 \cdot h$ where $h \mid 10$. Thus, $x = 144$ and $h = 5$. We have established that

(6.3) a) $\mathrm{Con}(S, M_{11}) = \mathrm{Con}(S^j, M_{11})$ for $j \in (\mathbb{Z}/11)^*$ and $j \neq \pm 1 \bmod 11$, and;

b) $\mathrm{Con}(S, M_{11}) \neq \mathrm{Con}(S^{-1}, M_{11})$.

In addition, since the 11-sylows are all conjugate in M_{11}, every outer automorphism of M_{11} in S_{11} has a representative (modulo inner automorphisms) in $N_{S_{11}}(<S>)$ (the normalizer in S_{11} of $<S>$), which is of order $11 \cdot 10$.

Thus, $N_{S_{11}}(M_{11})$ contains M_{11} as a subgroup of index 2.

In order to find covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ with geometric monodromy group equal to M_{11} we take $\sigma(1) = S$, $\sigma(2) = T$, $\sigma(3) = T^{-1}$, $\sigma(4) = S^{-1}$. This simple example illustrates the immense computational difficulties inherent in any example (even of degree as low as 11). Since there are 144 11-sylows in M_{11}, there is obviously a tremendous amount of calculation to find all 4-tuples $\big(\tau(1), \tau(2), \tau(3), \tau(4)\big)$ of elements of M_{11} such that: $\tau(1)\cdot\tau(2)\cdot\tau(3)\cdot\tau(4) = \mathrm{Id.}$; in some order $\tau(1), \ldots, \tau(4)$ are conjugate respectively to S, T, T^{-1}, S^{-1}, and; $\tau(1), \ldots, \tau(4)$ generate M_{11}. When this list of $\tau(1), \ldots, \tau(4)$ is completed, in order to check if the Hurwitz number of $\mathcal{G}$ is 1, we must check to see that each of the allowable $\tau(1), \ldots, \tau(4)$ is obtained by braiding $\sigma(1), \ldots, \sigma(4)$ (Section 4.B).

If the Hurwitz number is 1, Theorem 5.1 shows that the diagram

$$\mathfrak{I}^{\mathrm{symm}}(\mathcal{G}) \to \mathcal{O}(\mathcal{G}) \times \mathbb{P}^1 \xrightarrow{\mathrm{pr}_1} \mathcal{O}(\mathcal{G}) \qquad \xrightarrow{\mathrm{pr}_2} \mathbb{P}^1$$

is defined over Φ. Suppose now that we are lucky enough to find a point $\underline{p} \in \theta(\sigma)$ such that

(6.4) $\underline{p}$ is Φ-rational.

Let $u(1), u(2), u(3), u(4)$ be the branch points of $Y_{\underline{p}} \xrightarrow{\varphi} \mathbb{P}^1$. Since $(Y_{\underline{p}}, \varphi_{\underline{p}})$ is defined over Φ, condition (6.3) b) (and the Branch Cycle argument) shows that $u(1)$ and $u(2)$ are conjugate elements in the quadratic subfield of $\Phi(\zeta_{11})$. Let $\hat{\Phi}_{\underline{p}}$ be the algebraic closure of Φ in $\Phi(Y_{\underline{p}})$. From Proposition 2, $\hat{\Phi}_{\underline{p}} \subset \Phi(\zeta_{11}) \cap L \cdot \Phi(i)$ where L is the field generated by the coordinates of $\wp_1, \wp_2, \wp_3, \overline{\wp}_1$, and $\overline{\wp}_2$ where $\wp_1, \wp_2, \wp_3$ are the unramified points of $Y_{\underline{p}}$ over $u(3)$, and; $\overline{\wp}_1$ and $\overline{\wp}_2$ are the two ramified places of $Y_{\underline{p}}$ over $u(3)$.

We have not bothered to make the (difficult) computation to ascertain whether or not T and T^{-1} are conjugate in M_{11} since it does not seriously effect our computation of $\hat{\Phi}_{\underline{p}}$. In fact, by an argument involving only the possible values of the degree of L over Φ we conclude that $\hat{\Phi}_{\underline{p}}$ is contained in the unique quadratic extension of Φ contained in $\Phi(\zeta_{11})$ (that is, $\Phi(\sqrt{-11})$). Thus, in order to have solved the one-variable problem for M_{11} over $\Phi(\sqrt{-11})$ (assuming that we have demonstrated that the Hurwitz number of $(\sigma(1), \sigma(2), \sigma(3), \sigma(4))$ is 1) we have only to find a Φ-rational place $\underline{p} \in \theta(\underline{g})$. One way that the existence of such a Φ-rational point can be demonstrated is to find a genus zero curve $\mathcal{C}$ in $\theta(\underline{g})$ such that $\mathcal{C}$ can be demonstrated to have a Φ-rational place. Consider the canonical covers: $(\mathbb{P}^1)^4 \xrightarrow{\alpha} \mathbb{P}^4$ and; $\theta(\underline{g}) \xrightarrow{\Psi} \mathbb{P}^4$. Let $\mathcal{C}_{u(1),u(2),u(3)}$ be the locus $\left\{\Psi^{-1} \circ \alpha\left(u(1), u(2), u(3), u\right)\right\}$ as u runs over $\mathbb{P}^1$, and $u(1), u(2), u(3)$ are fixed. The genus of a non-singular projective model of $\mathcal{C}_{u(1),u(2),u(3)}$ is easily computed by the same calculation that affects the computation of the Hurwitz number of $\theta(\underline{g})$. This curve

was used to good effect in [Fr and L; Chap. 6] and could conceivably be put to similar use here. ■

Example 6. PSp $(2\ell, \mathbb{Z}/(3))$ and the Hurwitz Monodromy Group.

Cohen in [Co] considers simple branched covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ (see Example 1) with; $\deg \varphi = 3$, and; φ has exactly $r = 2\ell + 2$ branch points. From the classical computation of Clebsch [Cle], the Hurwitz number of (Y, φ) is 1. From Corollary 5.3 the cover $\mathcal{C}(Y, \varphi; r) \xrightarrow{\Psi} U_{\mathbb{P}^r}$ is defined over $\mathbb{Q}$. The main result of [Co] is that the cover $\left(\mathcal{C}(Y, \varphi; r), \Psi\right)$ has as geometric monodromy group the group $PSp\left(2\ell, \mathbb{Z}/(3)\right)$. That is: $G\left(\overline{\mathbb{Q}}\,\widehat{(\mathcal{C}(Y, \varphi; r)}/\overline{\mathbb{Q}}(\mathbb{P}^r)\right)$ (Galois group of the Galois closure of $\overline{\mathbb{Q}}\left(\mathcal{C}(Y, \varphi; r)\right) / \overline{\mathbb{Q}}(\mathbb{P}^r)\right)$ is the projective symplectic group over the finite field $\mathbb{Z}/(3)$. Unfortunately, $PSp(2\ell, \mathbb{Z}/(3))$ has an outer automorphism (a diagonal automorphism [Ca; Chap. 11, Steinberg's Theorem]) and the best we can assert is that: $G\left(\widehat{\mathbb{Q}(\mathcal{C}(Y, \varphi; r))} / \mathbb{Q}(\mathbb{P}^r)\right)$ contains $G\left(\mathbb{Q}\widehat{(\mathcal{C}(Y, \varphi; r)}\right) / \hat{\mathbb{Q}}(\mathbb{P}^r)\right)$ as a subgroup of index 1 or 2 (that is: $[\hat{\mathbb{Q}} : \mathbb{Q}] \leq 2$ where $\hat{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}\left(\widehat{\mathcal{C}(Y, \varphi; r)}\right)$. By specialization, using Hilbert's irreducibility theorem, there exists a Galois extension M of $\hat{\mathbb{Q}}$ such that $G(M/\hat{\mathbb{Q}})$ is isomorphic to $PSp\left(2\ell, \mathbb{Z}/(3)\right)$.

Example 7. Elementary Groups.

Let $(\mathbb{Z}/(n))^*$ denote the invertible integers modulo n. For A, a subgroup of $(\mathbb{Z}/(n))^*$, let $G(A, n) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in A,\ b \in \mathbb{Z}/(n) \right\}$ be a group of 2×2 matrices under multiplication. The standard representation of this group on the integers modulo n is designated by $T(A, n)$. We identify A with the subgroup of $G(A, n)$ given by $\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in A \right\}$.

In [Fr, 1] the case where A is the subgroup generated by -1 is considered in great detail as this case arises in many interesting diophantine problems, and is, in special cases, equivalent to the consideration of modular curves of

level n. In particular, we obtain: examples where the Hurwitz parameter space has no $\mathbb{Q}$ - rational points even though it is defined over $\mathbb{Q}$, and; many interesting examples (equivalent to the theory of complex multiplication) of covers $Y \xrightarrow{\varphi} \mathbb{P}^1$ defined over a field F such that $G\left(\widehat{F(Y)} / \hat{F}(\mathbb{P}^1)\right)$ is a proper subgroup of $G\left(\widehat{F(Y)} / F(\mathbb{P}^1)\right)$. ■

Example 8. Fields of Moduli.

Let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be a cover. In the opening remarks of the proof of Theorem 5.1 we introduced the field of moduli, $K_{\mathcal{J}}$, of the collection $\mathcal{M}(Y, \varphi; r) = \left\{\mathcal{J}^{\text{symm}}(Y, \varphi; r),\ \Phi^{\text{symm}},\ \Theta(Y, \varphi; r),\ pr_1,\ pr_2,\ \Psi\right\}$. Reminder: $K_{\mathcal{J}}$ is the fixed field in $\overline{\mathbb{Q}}$ of all $\alpha \in G(\overline{\mathbb{Q}} / \mathbb{Q})$ such that $\mathcal{M}(Y, \varphi; r)^{\alpha}$ is isomorphic to $\mathcal{M}(Y, \varphi; r)$. We also showed that when (Y, φ) has no automorphisms, then the field of moduli is a field of definition of $\mathcal{M}(Y, \varphi; r)$. This is not true in general. In fact, let $Y \xrightarrow{\varphi} \mathbb{P}^1$ be such that $G\left(\overline{\mathbb{Q}}(Y) / \mathbb{Q}(\mathbb{P}^1)\right)$ is a group G having two permutation representations T_1 (coming from Y, φ) and T_2 having the following properties. The representations T_1 and T_2 are permutation inequivalent doubly transitive representations of degree n which are equivalent as group representations. Assume also that the branch cycles $\sigma(1), \ldots, \sigma(r-1)$ for (Y, φ) are of order 2, and that the one remaining branch cycle $\sigma(r)$ is an n - cycle in both representations. Then the results of [Fr 3; Theorem 2] show that the field of moduli of $\mathcal{M}(\hat{Y}, \hat{\varphi}; r)$ is not a field of definition of $\mathcal{M}(\hat{Y}, \hat{\varphi}; r)$ where $\hat{Y} \xrightarrow{\hat{\varphi}} \mathbb{P}^1$ is the Galois closure of the cover $Y \xrightarrow{\varphi} \mathbb{P}^1$. Note that the quoted results of Proposition 3 of Section 4 imply that we may form Hurwitz Families under these hypotheses. ■

References

[C] R. Carmichael, Introduction to the Theory of Groups of Finite Order, Dover Publications, 1956.

[Ca] R. W. Carter, Simple Groups of Lie Type, John Wiley and Sons, Pure and Applied Mathematics Vol. XXVIII, 1972.

[Cle] A. Clebsch, Zür theorie der Riemann' schen Fläche, Math. Ann. 6 (1972), 216-230.

[Co] D. B. Cohen, The Hurwitz Mondromy Group, Journal of Algebra 32, 501-517 (1974).

[Fr, 1] M. Fried, Galois Groups and Complex Multiplication, preprint.

[Fr & Ja] M. Fried and M. Jarden, A Stability Property of Fields of Characteristic 0, preprint.

[Fr, 2] M. Fried, Stable Existence of Hurwitz Families, preprint.

[Fr & L] M. Fried and D. J. Lewis, Solution Spaces to diophantine problems, invited talk, Bull. of Amer. Math. Soc., to appear.

[Fr, 3] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, Illinois Journal of Math. Vol. 17, No. 1, March 1973, 128-146.

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

[Gi] J. Giraud, Cohomologie non abélienne, Lecture notes, Columbia University.

[Gode] R. Godement, Topologie algébrique et theorie des faisceux, Hermann and Cie, Paris, 1958.

[Gr and Re] H. Grauert and R. Remmert, 3 papers in Comptes Rendus de L'Acadamie des Sciences, Paris Band 245 (1957), 819-822, 822-825, 918-921.

[Gro] A. Grothendieck, A General Theory of Fibre Spaces with Structure Sheaf, University of Kansas, Dept. of Mathematics, Lawrence, Kansas.

[Hi] D. Hilbert, Über die Irreduzibilitat ganzer rationaler Functionen mit ganzzahligen Koeffizienten, J. Reine Angew. Math., 110 (1892) (Ges. Abh. II, 264-286).

[Hu] A. Hurwitz, Über Riemannshe Flachen mit gegeben Verzweigungspunten, Math. Ann. 39 (1891), 1-61.

[Ko and Sp] K. Kodaira and D. C. Spencer, On deformations of complex analytic structures I, II, Ann. Math. 67 (1958), 328-466.

[Ma, K, & S] W. Magnus, A. Karrass, D. Solitar, Combinatorial Group Theory, Interscience Publishers 1966, John Wiley and Sons, Inc.

[Mum] D. Mumford, Introduction to Algebraic Geometry, Cambridge, Mass.: Harvard University Notes (1966).

[No] E. Noether, Gleichungen mit vargeschriebener Gruppe, Math. Ann., 78 (1916), 221-229.

[Sha] I. Shafarevich, Construction of fields of algebraic numbers with given solvable Galois group, (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 18 (1954), 525-578.

[Shih] K. Shih, On the Construction of Galois Extensions of Function Fields and Number Fields, Math. Ann. 207 (1974), 99-120.

[Sh and Ta] G. Shimura and Y. Taniyama, Complex Multiplication of Alebian Varieties and its Applications to Number Theory, Math. Soc. of Japan, 1961.

[Sp] G. Springer, Introduction to Riemann Surfaces, Addison-Wesley Publishing Co., Reading, Mass., 1957.

[Sw] R. Swan, Invariant rational functions and a problem of Steenrod, Inventiones Math. 7 (1969), 148-158.

[Tre] M. Tretkoff, Algebraic extensions of the field of rational functions, Comm. Pure Appl. Math. 24 (1971), 491-497.

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

[We,2] A. Weil, Foundations of Algebraic geometry, A.M.S. Colloquium Publications, Vol. XXIX, Providence, Rhode Island, 1962.

[Za] H. Zassenhaus, The Theory of Groups (2nd Ed.), Chelsea Publ., New York, N.Y., 1958.

Received: November 1975