Proceedings of Symposia in Pure Mathematics
Volume 37, 1980

EXPOSITION ON AN ARITHMETIC-GROUP THEORETIC CONNECTION VIA RIEMANN'S EXISTENCE THEOREM

M. FRIED[1]

There is a triumph for the group theory that is applied to the examples of this paper (Examples 1 and 2 of §1.A, §1.B and §3). Starting with an infinite collection of arithmetic questions parametrized (for example) by the degrees of certain polynomials involved in the phrasing of the problem, we apply theorems of Burnside, Feit, Schur, Scott, Wagner, Wielandt, et al. to conclude a list of solutions that has a reasonable finitistic description. I selected these examples partly to illustrate this remarkable circumstance; a circumstance commensurate (as the Schur problems will show) with the finitistic description in [**Maz**] of the **Q**-rational points on the *complete set* of modular curves $\{Y_0(n)\}_{n=1}^{\infty}$. Uncovering a simple explanation for this surprising phenomenon, which occurs repeatedly in the examples of [**Fr, 0**], remains one of the unsolved problems in this area joining group theory to arithmetic.

This paper focuses on two examples from the motivational section [**Fr, 0,** §7] of my partially completed book. As examples of diophantine geometry problems they are archetypal of those that can be rephrased in terms of *arithmetic monodromy groups*, and illustrative of those whose solutions apparently demand an open eye to rich connections with many diverse areas of mathematics. In format we follow, for each of the problems, the outline of the 4 stages that appear in §1.A. In scope we will be long on the first 3 stages: introduction of Riemann's existence theorem; arithmetic monodromy interpretation; and illustration of the special type of permutation group theory that arises so naturally in this area. The classical Riemann's existence theorem tells us a prescription (§0.A) for asserting the *existence* of ramified covers of the Riemann sphere having degree n and explicit points of branching. The final list of covers results from the combinatorial expedient of computing some equivalence classes of

---

1980 *Mathematics Subject Classification.* Primary 14H25, 14H30.

[1]The author was funded by NSF Grant No. MCS-78-02669. We would also like to thank Horst Zimmer for his comments and careful reading of the manuscript.

homomorphisms of a group F (in this case, a free group on r generators modulo one relation; r being the number of branch points of the cover being considered) into the symmetric group on n letters, S_n.

There are problems that arise in applying Riemann's existence theorem. First, it is just an *existence* theorem; it does not explicitly produce algebraic equations for these covers. Secondly, it does not directly give us information about arithmetic monodromy groups of these covers. The examples of this paper suggest the direction that is taken in [**Fr, 0**, §§6, 9] to remedy these deficiences. In the end, much of this delicate arithmetic information can be obtained, in generalization to the original Riemann's existence theorem, by computing equivalence classes of permutation representations of certain finitely presented groups. Artin's braid group, the Hurwitz monodromy group, and many of the other classical combinatorial groups arise and present us with representation theory problems. Suggested reading order: §1 (follow Schur's problem) → §0.A → §0.C → §3 → rest of paper.

Table of Contents

0. Directions on a Riemann surface.

0.A. *Riemann's existence theorem.* We consider a compact Riemann surface $\mathcal{S}$ with a "sphere of reference", a situation that is not well represented by a picture in $\mathbf{R}^3$. We identify $\mathbf{P}^1$ (projective 1-space over the complex numbers) with the one-point compactification $\mathbf{C} \cup \{\infty\}$ of the complex plane. By a sphere of reference we mean a surjective complex analytic map $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ presenting $\mathcal{S}$ as a degree n ramified cover of $\mathbf{P}^1$. Let $D(\varphi) \overset{\text{def}}{=} \{$branch points of φ; points $z \in \mathbf{P}^1$ such that $|\varphi^{-1}(z)|$ is less than $n\}$. Now consider the properties of such a map φ.

For each $z \in \mathbf{P}^1$ let N_z be a small "disc" neighborhood of z, and consider $\mathcal{S}|_{N_z} \xrightarrow{\varphi} N_z$, the restriction of φ over N_z.

For $z \notin D(\varphi)$, N_z can be selected so that φ naturally presents $\mathcal{S}|_{N_z}$ as isomorphic to n copies of N_z. For $z \in D(\varphi)$ we choose N_z so that

$$\mathcal{S}|_{N_z} - \{\varphi^{-1}(z)\} \xrightarrow{\varphi} N_z - \{z\} \text{ is an unramified cover.} \tag{0.1}$$

The fundamental group of a punctured disc is naturally isomorphic to $\mathbf{Z}$ by choosing as a generator a "circle" about z in the counterclockwise direction.

DEFINITION 0.1. Let $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}$ be three connected manifolds and let $\mathcal{R}_i \xrightarrow{\psi_i} \mathcal{R}$, $i = 1, 2$, be an unramified covering morphism. We say that $\mathcal{R}_1 \to \mathcal{R}$ and $\mathcal{R}_2 \to \mathcal{R}$ are *equivalent* (as covers of $\mathcal{R}$) if there exists a (not necessarily unique) homeomorphism ψ: $\mathcal{R}_1 \to \mathcal{R}_2$ such that $\psi_2 \circ \psi = \psi_1$. From the theory of the fundamental group we know that equivalence classes of *connected* covers of $\mathcal{R}$ are in one-one correspondence with conjugacy classes of subgroups of $\pi^1(\mathcal{R}, z_0) \overset{\text{def}}{=}$ the fundamental group generated by the homotopy classes of paths on $\mathcal{R}$ based at the point z_0.

In expression (0.1) write $\mathcal{S}|_{N_z} - \{\varphi^{-1}(z)\}$ as a disjoint union of connected components $\cup_{i=1}^{t} M_i$ where t is equal to $|\varphi^{-1}(z)|$. Then, up to equivalence (as a cover of $N_z - z$) M_i is uniquely determined by the degree of the restriction of φ to M_i. Indeed, if $z = 0$, and N_0 is a small disc about the origin in $\mathbf{C}$, then the cover of degree e is represented by

$$M' = \{(\omega, z) \in \mathbf{C} \times \mathbf{C} | \omega^e = z\}|_{N_0 - \{0\}} \xrightarrow{\text{proj. on } z} N_0 - \{0\}.$$

Thus, corresponding to φ we have two pieces of data:

(0.2) (a) the collection of points $D(\varphi)$ in $\mathbf{P}^1$; and

(b) for each $z \in D(\varphi)$ the collection of integers (some repeated) given by the degrees of the connected components of $\mathcal{S}|_{N_z}$ as covers of N_z (as above).

For each $z \in D(\varphi)$ let $\sigma(z)$ be a symbol of the form $(s_1)(s_2) \cdots (s_t)$ where $s_1, \ldots, s_t$ are the integers associated to z by (0.2)(b). Since $\Sigma_{i=1}^{t} s_i = n$, it is customary to leave out of this symbol those integers s_i for which $s_i = 1$. We define the index of $\sigma(z)$ (denoted by $\text{ind}(\sigma(z))$) to be the integer $\Sigma_{i=1}^{t}(s_i - 1)$. In terms of these quantities the *Riemann-Hurwitz* formula becomes

(0.3) $2(n + g - 1) = \Sigma_{z \in D(\varphi)} \text{ind}(\sigma(z))$ where $g = g(\mathcal{S})$ is the *genus* of $\mathcal{S}$ (the number of handles in a description of $\mathcal{S}$ as a sphere with handles; the number of linearly independent holomorphic differentials on $\mathcal{S}$; etc.).

Now let $z_0(\varphi)$ be a preselected base point, not in the support of $D(\varphi) = \{z_1, \ldots, z_r\}$. Let $\{P_1, \ldots, P_n\}$ be a naming of the points of the fiber $\varphi^{-1}(z_0(\varphi))$. The fundamental group $\pi^1(\mathbf{P}^1 - \{z_1, \ldots, z_r\}, z_0(\varphi))$ is a free group on r generators, which we denote by $\Sigma_1, \ldots, \Sigma_r$, modulo the one relation $\Sigma_1 \cdots \Sigma_r = \text{Id}$, where Id denotes the identity in this group. In Figure 1 the paths $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are representatives of the homotopy classes of paths that give generators $\Sigma_1, \ldots, \Sigma_r$.

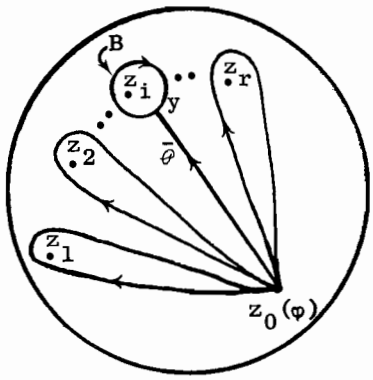


FIGURE 1. Generating paths on an r-punctured sphere

The paths $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are (excluding their beginning and endpoints): nonintersecting; oriented, in order, clockwise around $z_0(\varphi)$; and $\mathcal{P}_i$ is homotopic to the path $\bar{\mathcal{P}} \circ B \circ \bar{\mathcal{P}}^{-1}$ where B, the boundary of a "small" disc neighborhood of z_i, starts and ends at y.

Note that the path $\mathcal{P}_1 \circ \mathcal{P}_2 \circ \cdots \circ \mathcal{P}_r$ is homotopic to the identity by going around the "back" of the sphere.

For each degree n cover $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ with branch points among the set $\{z_1, \ldots, z_r\}$ we associate to each Σ_i (as above) a permutation σ_i of the points $\{P_1, \ldots, P_n\}$ in the fiber above $z_0(\varphi)$ in the following way. The effect of σ_i applied to P_k is P_l where: P_l is the endpoint of the unique path on $\mathcal{S}$ lying over $\mathcal{P}_i$ and starting at P_k. For convenience we change $\{P_1, \ldots, P_n\}$ to $\{1, 2, \ldots, n\}$ so that we may regard σ_i as being contained in S_n. Thus we obtain a homomorphism $\pi^1(\mathbf{P}^1 - \{z_1, \ldots, z_r\}, z_0) \to S_n$.

DEFINITION 0.2. We call the ordered r-tuple $(\sigma_1, \ldots, \sigma_r) = \boldsymbol{\sigma}$ *a description of the branch cycles of the cover* $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ *with respect to the base point* $z_0(\varphi)$ *and the collection of paths* $\mathcal{P}_1, \ldots, \mathcal{P}_r$. If we reorder the points $P_1, \ldots, P_n$ by permuting the subscripts via $\tau \in S_n$, a new computation of the branch cycles will yield $(\sigma_1', \ldots, \sigma_r')$ where $\sigma_i' = \tau^{-1} \cdot \sigma_i \cdot \tau$, $i = 1, \ldots, r$. We say that $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ are *equivalent*. If we write σ_i as a product of disjoint cycles in S_n, then the lengths of these disjoint cycles are the same as the integers that appear in the symbol $\sigma(z_i)$ following expression (0.2).

Conversely, for a given homomorphism of $\pi^1(\mathbf{P}^1 - \{z_1, \ldots, z_r\}, z_0)$ into S_n we may consider the images of $\Sigma_1, \ldots, \Sigma_r$ (denoted $\sigma_1, \ldots, \sigma_r$) as the branch cycles of a cover $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ computed with respect to the paths $\mathcal{P}_1, \ldots, \mathcal{P}_r$. Indeed, from fundamental group theory, we obtain a cover $X \xrightarrow{\varphi'} \mathbf{P}^1 - \{z_1, \ldots, z_r\}$. We compactify X to give $\mathcal{S} = \mathcal{S}(\varphi)$ by making a relative compactification of $(\varphi')^{-1}(D_{z_i}^0)$ where D_{z_i} is a disc neighborhood of z_i on $\mathbf{P}^1$ and $D_{z_i}^0 = D_{z_i} - \{z_i\}$. The upshot of all this is:

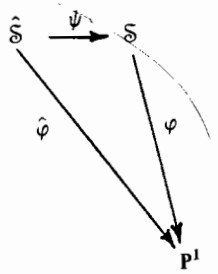
RIEMANN'S EXISTENCE THEOREM. *Given paths* $\mathcal{P}_1, \ldots, \mathcal{P}_r$ *as described in Figure* 1, *there is a one-one correspondence between equivalence classes of*

(0.4)(a) *connected covers* $\mathcal{S}(\varphi) \to \mathbf{P}^1$ *of degree* n; *and*

(b) r-*tuples* $(\sigma_1, \ldots, \sigma_r) \in (S_n)^r$ *such that* $\sigma_1 \cdots \sigma_r = \mathrm{Id}$, *and* $\sigma_1, \ldots, \sigma_r$ *generate a transitive subgroup of* S_n.

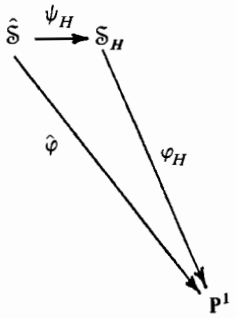
The group $G(\sigma)$ generated by $\sigma_1, \ldots, \sigma_r$ is called the *geometric monodromy group* of the cover $\mathcal{S} \to \mathbf{P}^1$. Let $\mathrm{Aut}(\mathcal{S}, \varphi)$ be the group of analytic isomorphisms $\alpha\colon \mathcal{S} \to \mathcal{S}$ for which $\varphi \circ \alpha = \varphi$. The cover $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ is said to be *Galois* if the order of the group $\mathrm{Aut}(\mathcal{S}, \varphi)$ is n (i.e., it is as big as it can be). For any cover $\mathcal{S} \xrightarrow{\varphi} \mathbf{P}^1$ there exists a unique minimal Galois cover $\hat{\mathcal{S}} \xrightarrow{\hat{\varphi}} \mathbf{P}^1$ fitting in a commutative diagram (the *Galois closure diagram*)

(0.5)(a)



The group $\mathrm{Aut}(\hat{\mathcal{S}}, \hat{\varphi})$ is isomorphic to $G(\sigma)$, but it is most canonically identified with the elements of S_N that centralize the image of $G(\sigma)$ in its right regular representation. Here N is the order of $G(\sigma)$. For any subgroup H of $\mathrm{Aut}(\hat{\mathcal{S}}, \hat{\varphi})$ (or, by a slight abuse, of $G(\sigma)$), the classical Galois correspondence produces for us a diagram

(0.5)(b)



where the cover $\hat{\mathcal{S}} \to \mathcal{S}_H$ is Galois with group isomorphic to H.

Let T_H be the permutation representation of $G(\sigma)$ given by multiplication on the right cosets of H in $G(\sigma)$. Then $(T_H(\sigma_1), \ldots, T_H(\sigma_r))$ gives us a description of the branch cycles for the cover $\mathcal{S}_H \xrightarrow{\varphi_H} \mathbf{P}^1$.

0.B. *Neighborhoods of a cover*; *Artin braid group*; *Hurwitz monodromy group*. Let $\mathcal{S}^{(0)} \xrightarrow{\varphi^{(0)}} \mathbf{P}^1$ be an n-sheeted cover of the Riemann sphere, as described in §0.A, where the branch points of $\varphi^{(0)}$ are $z_1^{(0)}, \ldots, z_r^{(0)}$. Notationally we denote the cover by the pair $(\mathcal{S}^{(0)}, \varphi^{(0)})$.

DEFINITION 0.3. *A neighborhood* $(\mathcal{T}, \Phi, \mathcal{P})$ *of* $(\mathcal{S}^{(0)}, \varphi^{(0)})$ *over* $\mathcal{P}$ consists of the data

$$\begin{array}{ccccc} \mathcal{T} & \xrightarrow{\Phi} & \mathcal{P} \times \mathbf{P}^1 & \xrightarrow{\mathrm{pr}_1} & \mathcal{P} \\ & & & \searrow^{\mathrm{pr}_2} & \\ & & & & \mathbf{P}^1 \end{array} \tag{0.6}$$

and a specified point $\mathfrak{p}^{(0)} \in \mathcal{P}$ where

(a) Φ is a proper map of degree n;

(b) $\mathcal{T}$ and $\mathcal{P}$ are complex connected manifolds;

(c) for each $\mathfrak{p} \in \mathcal{P}$, $\mathrm{pr}_2 \circ \Phi$ presents the fiber $\mathcal{T}_{\mathfrak{p}} \overset{\text{def}}{=} (\mathrm{pr}_1 \circ \Phi)^{-1}(\mathfrak{p})$ as an n-sheeted cover of $\mathbf{P}^1$ having exactly r branch points; and

(d) the covers $\mathcal{T}_{\mathfrak{p}^{(0)}} \to \mathbf{P}^1$ and $\mathcal{S}^{(0)} \xrightarrow{\varphi^{(0)}} \mathbf{P}^1$ are equivalent as covers of $\mathbf{P}^1$ (the natural extension of Definition 0.1).

We consider a few comments on *fiber products*. Let X, Y, Z be three sets; f: $X \to Z$, g: $Y \to Z$ any functions. Then the fiber product of X and Y over Z is the set $X \times_Z Y = \{(x, y) | f(x) = g(y)\} \subseteq X \times Y$. If X, Y, Z are complex (or algebraic) sets, and the functions f and g are induced by complex (or algebraic) morphisms, then $X \times_Z Y$ has the structure of a complex (or algebraic) set and the natural maps pr_X: $Y \to X$ and pr_Y: $X \times_Z Y \to Y$ are induced by complex (or algebraic) morphisms.

Let $\mathbf{A}^r_R$ and $\mathbf{A}^r_C$ be two copies of affine r-space, and consider the natural map $\mathbf{A}^r_R \xrightarrow{\Psi_r} \mathbf{A}^r_C$ that sends $(x_1, \ldots, x_r)$ to the r-tuple of symmetric functions

$$(y_1, \ldots, y_r) = \left(\ldots, (-1)^i \sum_{j(1) < \cdots < j(i)} x_{j(1)} \cdots x_{j(i)}, \ldots \right).$$

The subscripts R and C stand for (resp.) Roots and Coefficients. The cover $\mathbf{A}^r_R \xrightarrow{\Psi_r} \mathbf{A}^r_C$ is called (at least by the author) the *Noether cover*; it is Galois with group S_r. The variety $\mathbf{A}^r$ can be regarded as an affine subset of both $(\mathbf{P}^1)^r$ and of $\mathbf{P}^r$: $\mathbf{A}^1 = \mathbf{P}^1 - \{\infty\}$ embeds $(\mathbf{A}^1)^r$ in $(\mathbf{P}^1)^r$; and $\mathbf{A}^r$ can be regarded as the subset of $\mathbf{P}^r$ represented by $r+1$-tuples $(y_0, y_1, \ldots, y_r)$ with $y_0 = 1$. Interestingly enough $(\mathbf{P}^1)^r$ and $\mathbf{P}^r$ are joined in a commutative diagram

$$\begin{array}{ccc} \mathbf{A}^r_R & \xrightarrow{\Psi_r} & \mathbf{A}^r_C \\ \downarrow & & \downarrow \\ (\mathbf{P}^1)^r & \xrightarrow{\overline{\Psi}_r} & \mathbf{P}^r \end{array} \tag{0.7}$$

where the vertical arrows are the respective identifications of $\mathbf{A}^r$ with subsets of $(\mathbf{P}^1)^r$ and $\mathbf{P}^r$ given above.

The true nature of this diagram is best understood by considering the set of nonzero polynomials in Z

$$P_r = \left\{ \sum_{i=0}^{r} y_i \cdot Z^i | (y_0, \ldots, y_r) \in \mathbf{C}^{r+1} - \{(0, \ldots, 0)\} \right\},$$

modulo the action of $\mathbf{C}^*$ that equivalences two polynomials if one is a nonzero multiple of the other. This set is then identified with $\mathbf{P}^r$, and the map $\overline{\Psi}_r$ maps $(x_1, \ldots, x_r)$ to $\Pi_{i=1}^r(Z - x_i)$ with the stipulation that if $x_i = \infty$, $Z - x_i$ is replaced by the constant 1. Thus $\mathbf{P}^r$ can be regarded as the quotient of $(\mathbf{P}^1)^r$ by S_r. Finally, let Δ_r be the subset of $\mathbf{A}_R^r$ consisting of the points having two or more equal coordinates, and let D_r (the *discriminant locus* of the Noether cover) be the image of Δ_r under Ψ_r. By abuse we also denote by Δ_r (resp., D_r) the closure of Δ_r (resp., D_r) in $(\mathbf{P}^1)^r$ (resp., $\mathbf{P}^r$). We regard $\mathbf{P}^r - D_r$ as the collection of *r unordered distinct points of* $\mathbf{P}^1$.

For $(\mathcal{T}, \Phi, \mathcal{P})$ a neighborhood of $(\mathcal{S}^{(0)}, \varphi^{(0)})$, there is a natural map $\Psi_{\mathcal{P}}$: $\mathcal{P} \to \mathbf{P}^r - D_r$ which associates to $\mathfrak{p} \in \mathcal{P}$ the collection of branch points of the cover $\mathcal{T}_{\mathfrak{p}} \to \mathbf{P}^1$ that appears in expression (0.6)(c). Let $q^{(0)} = \Psi_{\mathcal{P}}(\mathfrak{p}^{(0)})$ and for convenience assume that $q^{(0)} \in \mathbf{A}_C^r$. The neighborhoods of $(\mathcal{S}^{(0)}, \varphi^{(0)})$ are an important consideration in problems in which Riemann's existence theorem is applied; especially those neighborhoods $(\mathcal{T}, \Phi, \mathcal{P})$ for which the map $\Psi_{\mathcal{P}}$ is a *finite map* (i.e., proper with fibers consisting of a finite number of points). It would be very valuable if we could find a neighborhood of $(\mathcal{S}^{(0)}, \varphi^{(0)})$ for which $\mathcal{P} = \mathbf{P}^r - D_r$, but this is very rarely the case as we shall see.

The fundamental group of $\mathbf{A}_C^r - D_r = \mathbf{A}^r - D_r$, denoted $\pi^1(\mathbf{A}^r - D_r, q^{(0)})$ is called the *Artin Braid Group*. Similarly, the fundamental group $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$ is called the *Hurwitz Monodromy Group*. Let

$$G(\Sigma_1, \ldots, \Sigma_r; \Sigma_1 \ldots \Sigma_r) \overset{\text{def}}{=} G(\boldsymbol{\Sigma})$$

denote the free group on the generators $\Sigma_1, \ldots, \Sigma_r$ modulo the one relation $\Sigma_1 \ldots \Sigma_r = \mathrm{Id}$. Let $\mathrm{Aut}(G(\boldsymbol{\Sigma}))$ (resp., $\mathrm{Aut}(G(\boldsymbol{\Sigma}))/\mathrm{Inn}(G(\boldsymbol{\Sigma}))$) be the group of automorphisms (resp., automorphisms modulo inner automorphisms) of the group $G(\boldsymbol{\Sigma})$.

THEOREM ([Ar, E, 1], [Ar, E, 2], [Bo], [Ni], [Fr, 0; PROPOSITION 0.1]). *The fundamental group $\pi^1(\mathbf{A}^r - D_r, q^{(0)})$ is a subgroup of the automorphism group of the free group on $\Sigma_1, \ldots, \Sigma_r$, given by generators $\overline{Q}_1, \ldots, \overline{Q}_{r-1}$ (see* (0.8)*) subject only to the relations: $\overline{Q}_i \cdot \overline{Q}_j = \overline{Q}_j \cdot \overline{Q}_i$ for $1 \leqslant i < j \leqslant r-1$, $j \neq i+1$ or $i-1$; and $\overline{Q}_i \cdot \overline{Q}_{i+1} \cdot \overline{Q}_i = \overline{Q}_{i+1} \cdot \overline{Q}_i \cdot \overline{Q}_{i+1}$, $i = 1, \ldots, r-2$. In addition, the natural map coming from the embedding of $\mathbf{A}^r - D_r$ in $\mathbf{P}^r - D_r$ in expression* (0.7) *induces a surjective map of $\pi^1(\mathbf{A}^r - D_r, q^{(0)})$ onto $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$. The group $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$ naturally maps to $\mathrm{Aut}(G(\boldsymbol{\Sigma}))/\mathrm{Inn}(G(\boldsymbol{\Sigma}))$, and the image group is called the Mapping Class Group.*

Indeed, $\overline{Q}_i$ acts on the r-tuple $(\Sigma_1, \ldots, \Sigma_r)$ by:

$$(\boldsymbol{\Sigma})\overline{Q}_i \quad \text{is equal to} \tag{0.8}$$

$$\left(\Sigma_1, \ldots, \Sigma_{i-1}, \Sigma_i \cdot \Sigma_{i+1} \cdot \Sigma_i^{-1}, \Sigma_i, \ldots, \Sigma_r\right), \qquad i = 1, \ldots, r-1.$$

We also denote by $\overline{Q}_1, \ldots, \overline{Q}_{r-1}$ the images of $\overline{Q}_1, \ldots, \overline{Q}_{r-1}$ in $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$.

Let $\boldsymbol{\sigma}^{(0)} = (\sigma_1^{(0)}, \ldots, \sigma_r^{(0)})$ be a description of the branch cycles of the cover $\mathcal{S}^{(0)} \overset{\varphi^{(0)}}{\to} \mathbf{P}^1$ (as in §0.A). Let $\mathrm{Ni}(\boldsymbol{\sigma}^{(0)})$ (the *Nielsen classes* associated to $\boldsymbol{\sigma}^{(0)}$) be the *equivalence classes* of elements $\boldsymbol{\tau} \in (S_n)^r$ for which $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_r)$ and there

exist $\gamma \in S_n$ and $\beta \in S_r$ for which:

(0.9)(a) $G(\gamma^{-1} \cdot \tau \cdot \gamma) = G(\sigma^{(0)})$;

(b) $\tau_1 \cdot \cdots \cdot \tau_r = \mathrm{Id}$; and

(c) $\gamma^{-1} \cdot \tau_{(i)\beta} \cdot \gamma$ is conjugate to $\sigma_i^{(0)}$ in $G(\sigma)$, $i = 1, \ldots, r$.

Through expression (0.8) the group $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$ acts on $\mathrm{Ni}(\sigma^{(0)})$.

DEFINITION 0.4. The *Hurwitz number* of $\sigma^{(0)}$, denoted $\mathrm{Hur}(\sigma^{(0)})$, is the number of orbits of $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$ on $\mathrm{Ni}(\sigma^{(0)})$. The *Braid classes* associated to $\sigma^{(0)}$ consist of the elements in the orbit of $\sigma^{(0)}$, denoted $\mathrm{Br}(\sigma^{(0)})$, under the action of $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$. From the theory of the fundamental group, the transitive representation of $\pi^1(\mathbf{P}^r - D_r, q^{(0)})$ on $\mathrm{Br}(\Sigma^{(0)})$ corresponds to an equivalence class of unramified covers, denoted

$$\Psi_{\mathcal{H}}\colon \mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)}) \to \mathbf{P}^r - D_r, \tag{0.10}$$

where $\mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)})$ is called the *Hurwitz parameter space associated to* $(\mathbb{S}^{(0)}, \varphi^{(0)})$.

The space $\mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)})$ has a universal property. If $(\mathcal{T}, \Phi, \mathcal{P})$ is *any* neighborhood of $(\mathbb{S}^{(0)}, \varphi^{(0)})$, $\Psi_{\mathcal{P}}\colon \mathcal{P} \to \mathbf{P}^r - D_r$ the associated map, then there exists a commutative diagram

$$\begin{array}{ccc} \mathcal{P} & \xrightarrow{\Psi'} & \mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)}) \\ & {\scriptstyle \Psi_{\mathcal{P}}} \searrow \quad \swarrow {\scriptstyle \Psi_{\mathcal{H}}} & \\ & \mathbf{P}^r - D_r & \end{array} \tag{0.11}$$

Thus (as explained in [**Fr**, **0**, §3]) we may use $\mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)})$ as a guide in traversing the neighborhoods of the cover $(\mathbb{S}^{(0)}, \varphi^{(0)})$.

When $\mathrm{Aut}(\mathbb{S}^{(0)}, \varphi^{(0)})$ consists of only a single element then there exists a unique neighborhood $(\mathcal{T}, \Phi, \mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)}))$ of $(\mathbb{S}^{(0)}, \varphi^{(0)})$ inducing the map of expression (0.10). In the general case the existence of such a neighborhood is a delicate problem interpreted in [**Fr**, **0**, §4] as a problem about special representations of the Hurwitz monodromy group. For the exposition of this paper we do not consider the neighborhoods of $(\mathbb{S}^{(0)}, \varphi^{(0)})$ but only the space $\mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)})$. However, we should point out that we cannot do arithmetic without *coordinates* giving an *algebraic structure* on $\mathcal{H}(n, r; \mathbb{S}^{(0)}, \varphi^{(0)})$ and some of the related neighborhoods of $(\mathbb{S}^{(0)}, \varphi^{(0)})$. The problem of finding algebraic versions of Riemann's existence theorem is phrased in [**Fr**, **0**, §6] in terms of finding explicit algebraic coordinates for these spaces. Of all the quantities introduced in [**Fr**, **0**] none is so crucial as the Hurwitz number, $\mathrm{Hur}(\sigma^{(0)})$. In general $\mathrm{Hur}(\sigma^{(0)})$ is 1. Indeed, the irreducibility of many of the foundational spaces of classical algebraic geometry (e.g., the moduli space of curves of genus g) is a corollary of the Hurwitz number being one for special choices of $\sigma^{(0)}$. But it is not always one [**Fr**, **9**, §3] and this possibility is the deepest challenge to the arithmetic-algebraic theory developed to date. The investigation of the Hurwitz number of special $\sigma^{(0)}$ is an important problem in combinatorial group theory. We conclude this section with an example of utmost importance to the sequel which may help the reader with the relation of these concepts to other classical moduli spaces.

0.C. *Modular curves.* Let L be a discrete (additive) subgroup of $\mathbf{C}$ such that $E = \mathbf{C}/L$ is compact. There is an invariant $j(\mathbf{C}/L) = j(E)$ of E such that $\mathbf{C}/L_1$ and $\mathbf{C}/L$ are analytically isomorphic if and only if $j(\mathbf{C}/L_1) = j(\mathbf{C}/L)$. We regard the function j as a uniformizing function on the space of one-dimensional complex tori. This space is represented as $\mathfrak{U}/\mathrm{PSL}(2, Z)$: the quotient of the *upper half plane* by the action of the group $\mathrm{PSL}(2, Z)$ of Mobius transformations with integer coefficients.

Let $\mathfrak{p} \in E$ be a point of order n in the group $\mathbf{C}/L$; n a fixed integer. Then $\mathfrak{p}$ is represented by one of the complex numbers α/n where $\alpha \in L$ but α/m is not in L for m a divisor of n and $m > 1$. We let $\langle \mathfrak{p} \rangle$ denote the subgroup of E generated by $\mathfrak{p}$. From $\langle \mathfrak{p} \rangle$ we obtain a complex analytic map of groups:

$$E \xrightarrow{\Phi} E_1 = E/\langle \mathfrak{p} \rangle = \mathbf{C}/\langle L, \alpha/n \rangle \tag{0.12}$$

where $\langle L, \alpha/n \rangle$ denotes the group generated by L and α/n.

Denote the diagram of (0.12) by (E, Φ, E_1). Two such diagrams (E, Φ, E_1) and (E', Φ', E_1') are equivalent if there exists a commutative diagram

$$\begin{array}{ccc} E' & \xrightarrow{\Phi'} & E_1' \\ \Psi\downarrow & & \downarrow\Psi_1 \\ E & \xrightarrow{\Phi} & E_1 \end{array} \tag{0.13}$$

where Ψ and Ψ_1 are analytic group isomorphisms.

Let $Y_0(n)$ denote the equivalence classes of triples (E, Φ, E_1).

Now, it is also true that [**Ah**, Chapter 7] every complex torus $\mathbf{C}/L = E$ can be presented as a 2-sheeted cover $E \xrightarrow{\beta} \mathbf{P}^1$ branched over 4 points of $\mathbf{P}^1$, so that the origin of E lies over the place at ∞ on $\mathbf{P}^1$; and the diagram (0.12) can be extended to

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E_1 \\ \beta\downarrow & & \downarrow\beta_1 \\ \mathbf{P}^1 & \xrightarrow{\varphi} & \mathbf{P}^1 \end{array} \tag{0.14}$$

Here $\mathbf{P}^1$ is canonically presented as the quotient $E/\langle -1 \rangle$ where $\langle -1 \rangle$ is the group (of order 2) generated by the automorphism of E induced by "multiplication by -1" on $\mathbf{C}$. Since $\langle \mathfrak{p} \rangle$ is invariant under this automorphism, the diagram is commutative.

We are interested in a description of the branch cycles of the cover

(0.15) $\mathbf{P}^1 \xrightarrow{\varphi} \mathbf{P}^1$, a cover of degree n having the same branch points, $\{z_1, z_2, z_3, z_4\}$, as does $E_1 \xrightarrow{\beta_1} \mathbf{P}^1$.

Indeed, the cover $E \xrightarrow{\beta_1 \circ \Phi} \mathbf{P}^1$ is a Galois cover, and $\mathrm{Aut}(E, \beta_1 \circ \Phi)$ is generated by translation by $\mathfrak{p}$ and "multiplication by -1". We easily conclude that the cover of expression (0.15) has monodromy group isomorphic to the 2×2 matrix group $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ modulo n where $a = \pm 1$, and b is any integer modulo $n\}$. Denote this group by $A(\langle -1 \rangle, n)$. If we let $\sigma_i^{(0)}$, $i = 1, 2, 3, 4$, be a description of the

0.C. *Modular curves.* Let L be a discrete (additive) subgroup of $\mathbf{C}$ such that $E = \mathbf{C}/L$ is compact. There is an invariant $j(\mathbf{C}/L) = j(E)$ of E such that $\mathbf{C}/L_1$ and $\mathbf{C}/L$ are analytically isomorphic if and only if $j(\mathbf{C}/L_1) = j(\mathbf{C}/L)$. We regard the function j as a uniformizing function on the space of one-dimensional complex tori. This space is represented as $\mathfrak{U}/\mathrm{PSL}(2, Z)$: the quotient of the *upper half plane* by the action of the group $\mathrm{PSL}(2, Z)$ of Mobius transformations with integer coefficients.

Let $\mathfrak{p} \in E$ be a point of order n in the group $\mathbf{C}/L$; n a fixed integer. Then $\mathfrak{p}$ is represented by one of the complex numbers α/n where $\alpha \in L$ but α/m is not in L for m a divisor of n and $m > 1$. We let $\langle \mathfrak{p} \rangle$ denote the subgroup of E generated by $\mathfrak{p}$. From $\langle \mathfrak{p} \rangle$ we obtain a complex analytic map of groups:

$$E \xrightarrow{\Phi} E_1 = E/\langle \mathfrak{p} \rangle = \mathbf{C}/\langle L, \alpha/n \rangle \tag{0.12}$$

where $\langle L, \alpha/n \rangle$ denotes the group generated by L and α/n.

Denote the diagram of (0.12) by (E, Φ, E_1). Two such diagrams (E, Φ, E_1) and (E', Φ', E_1') are equivalent if there exists a commutative diagram

$$\begin{array}{ccc} E' & \xrightarrow{\Phi'} & E_1' \\ \Psi\downarrow & & \downarrow\Psi_1 \\ E & \xrightarrow{\Phi} & E_1 \end{array} \tag{0.13}$$

where Ψ and Ψ_1 are analytic group isomorphisms.

Let $Y_0(n)$ denote the equivalence classes of triples (E, Φ, E_1).

Now, it is also true that [**Ah**, Chapter 7] every complex torus $\mathbf{C}/L = E$ can be presented as a 2-sheeted cover $E \xrightarrow{\beta} \mathbf{P}^1$ branched over 4 points of $\mathbf{P}^1$, so that the origin of E lies over the place at ∞ on $\mathbf{P}^1$; and the diagram (0.12) can be extended to

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E_1 \\ \beta\downarrow & & \downarrow\beta_1 \\ \mathbf{P}^1 & \xrightarrow{\varphi} & \mathbf{P}^1 \end{array} \tag{0.14}$$

Here $\mathbf{P}^1$ is canonically presented as the quotient $E/\langle -1 \rangle$ where $\langle -1 \rangle$ is the group (of order 2) generated by the automorphism of E induced by "multiplication by -1" on $\mathbf{C}$. Since $\langle \mathfrak{p} \rangle$ is invariant under this automorphism, the diagram is commutative.

We are interested in a description of the branch cycles of the cover

(0.15) $\mathbf{P}^1 \xrightarrow{\varphi} \mathbf{P}^1$, a cover of degree n having the same branch points, $\{z_1, z_2, z_3, z_4\}$, as does $E_1 \xrightarrow{\beta_1} \mathbf{P}^1$.

Indeed, the cover $E \xrightarrow{\beta_1 \circ \Phi} \mathbf{P}^1$ is a Galois cover, and $\mathrm{Aut}(E, \beta_1 \circ \Phi)$ is generated by translation by $\mathfrak{p}$ and "multiplication by -1". We easily conclude that the cover of expression (0.15) has monodromy group isomorphic to the 2×2 matrix group $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ modulo n where $a = \pm 1$, and b is any integer modulo $n\}$. Denote this group by $A(\langle -1 \rangle, n)$. If we let $\sigma_i^{(0)}$, $i = 1, 2, 3, 4$, be a description of the

Because of the importance of the modular curve $Y_0(n)$, this example should dispel any notion that the Hurwitz families are "simple" when we consider covers of $\mathbf{P}^1$ by other copies of $\mathbf{P}^1$. Even though the map $\Psi_{\mathfrak{IC}}$ is unramified, the cover $Y_0(n) \to \mathfrak{U}/\mathrm{PSL}(2, \mathbf{Z})$ is ramified over the points of $\mathfrak{U}/\mathrm{PSL}(2, \mathbf{Z})$ that correspond to the two isomorphism classes of elliptic curves that have nontrivial automorphisms different from that induced by "multiplication by -1" on $\mathbf{C}$ (see the Kummer-Ritt functions of §2.C). Let $q \in \mathbf{P}^4 - D_4$ be a point such that $\Theta_n(q)$ is *not* one of these two special points on $\mathfrak{U}/\mathrm{PSL}(2, \mathbf{Z})$. Then the fiber of $\Psi_{\mathfrak{IC}}$ over q is mapped in a one-one way by Λ_n. Since Λ_n is a fiber preserving map between complex manifold covers of a surjective map of complex manifolds, Λ_n is an open map. The curve $Y_0(n)$ is irreducible, and therefore from the diagram (0.17) we easily deduce that the Hurwitz number is 1 in this case. The irreducibility of $Y_0(n)$ in this case follows from the description of $Y_0(n)$ as a *homogeneous space*; $Y_0(n) \simeq \mathfrak{U}/\Gamma_0(n)$ where $\Gamma_0(n)$ is the subgroup of $\mathrm{PSL}(2, \mathbf{Z})$ whose elements are represented by matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $ad - bc = 1$ and $c \equiv 0$ modulo n.

1. The four stages and elementary arithmetic monodromy.

1.A. *Outline of the four stages and two examples of Stage* I *considerations.* The remainder of this paper concentrates on applying the ideas and notations of the four stages listed below to the Examples 1 and 2. In this subsection the examples merely illustrate the formulation of the type of problems that fit in our Stage I format. The examples are continued in §1.B, in accordance with Stage II considerations, where they are rephrased entirely in terms of elementary arithmetic monodromy. Finally, utilizing the Stage III considerations of §2, the examples are treated (with a complete exposition) as partially solved problems by an analysis of the Stage IV considerations in §3.

Stage I. *The Diophantine problem data.* We start with a number field M (a finite extension of $\mathbf{Q}$) with ring of integers R, and a diagram

$$\mathcal{C}' \xrightarrow{\Psi} \mathcal{C} \xrightarrow{\Phi} \mathcal{P}. \tag{1.1}$$

The spaces $\mathcal{C}'$, $\mathcal{C}$, and $\mathcal{P}$ are algebraic varieties; $\mathcal{P}$ is regarded as a *parameter space*; and for a point $\mathfrak{p} \in \mathcal{P}$, the fiber $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ represents one *algebraic curve*, possibly a singular affine curve, *covering another*. Also, we are given a *diophantine question D* which can be asked of any one of the curve coverings $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ in the family, for $\mathfrak{p}$ an M-rational point of $\mathcal{P}$. The reader is welcome to take $M = \mathbf{Q}$, $R = \mathbf{Z}$ if that should ease the burden of these formulations.

EXAMPLE 1. *The Schur problem for rational functions.* Let $f(y) \in M(y)$ be a rational function; $f(y) = f_1(y)/f_2(y)$ where $f_1, f_2 \in R[y]$ are relatively prime polynomials. The degree of f is defined to be the maximum of the degrees of f_1 and f_2. For $\mathfrak{m}$ a maximal prime ideal of R, the quotient $R/\mathfrak{m}$ is a finite field. So long as some of the coefficients of $f_2(x)$ do not lie in $\mathfrak{m}$, we may consider f as a mapping on $R/\mathfrak{m} \cup \{\infty\}$. We denote by $f \bmod \mathfrak{m}$ the rational function obtained by regarding the coefficients of f as being in $R/\mathfrak{m}$. Here $\{\infty\}$ designates the point at ∞ on the affine line; $f(\infty) = 0$ if $\deg(f_2 \bmod \mathfrak{m}) > \deg(f_1 \bmod \mathfrak{m})$; $f(\infty) = \infty$ if $\deg(f_1 \bmod \mathfrak{m}) > \deg(f_2 \bmod \mathfrak{m})$; and $f(\infty) = a/b$ if $\deg(f_2 \bmod \mathfrak{m}) = \deg(f_1 \bmod \mathfrak{m})$ and a and b are (resp.) the leading coefficients

of f_1 mod $\mathfrak{m}$ and f_2 mod $\mathfrak{m}$. Quickly stated, the Schur problem is the problem of finding those rational functions f which give a one-one (and therefore onto) map on $R/\mathfrak{m} \dot{\cup} \{\infty\}$ for *infinitely many primes* $\mathfrak{m}$. In order to fit this into the Stage I considerations we consider only those rational functions having a fixed degree equal to some integer n.

Let $\mathcal{C}'$ consist of the collection of affine algebraic curves, in the two variables x and y, of the form $f_1(y) - x \cdot f_2(y) = 0$ where f_1, f_2 are as above with $\max(\deg(f_1), \deg(f_2)) = n$. For $\mathcal{P}$ we take an open subset of affine $2 \cdot (n+1)$-space whose coordinates correspond to the coefficients of the pairs of polynomials represented by f_1 and f_2. For $\mathfrak{p} \in \mathcal{P}$, the cover $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ consists of the curve $\mathcal{C}'_{\mathfrak{p}}$ (given by $f_1(y; \mathfrak{p}) - x \cdot f_2(y; \mathfrak{p}) = 0$) mapped to the x-line (the curve $\mathcal{C}_{\mathfrak{p}}$) via the natural projection that takes a point (x, y) on $\mathcal{C}'_{\mathfrak{p}}$ to its x-coordinate. The diophantine question D: for an M-rational point $\mathfrak{p} \in \mathcal{P}$, do there exist *infinitely* many prime ideals $\mathfrak{m}$ of R for which the rational function $f_1(y; \mathfrak{p})/f_2(y; \mathfrak{p})$ gives a one-one map on $R/\mathfrak{m} \dot{\cup} \{\infty\}$? Equivalently, if $\bar{\mathcal{C}}'_{\mathfrak{p}}$ mod $\mathfrak{m}$ (resp., $\bar{\mathcal{C}}'_{\mathfrak{p}}$ mod $\mathfrak{m}$) is the completion in projective 2-space of the reduction of $\mathcal{C}'_{\mathfrak{p}}$ (resp., $\mathcal{C}_{\mathfrak{p}}$) modulo $\mathfrak{m}$, then we are asking that each $R/\mathfrak{m}$-rational point of $\bar{\mathcal{C}}'_{\mathfrak{p}}$ mod $\mathfrak{m}$ lies over exactly one $R/\mathfrak{m}$-rational point of $\bar{\mathcal{C}}_{\mathfrak{p}}$ mod $\mathfrak{m}$. Primarily we use the formulation that

$$\mathcal{V}_f(R/\mathfrak{m} \dot{\cup} \{\infty\}) \overset{\text{def}}{=} \{x_0 \in R/\mathfrak{m} \dot{\cup} \{\infty\} | \\ f(y_0) = x_0 \text{ for some } y_0 \in R/\mathfrak{m} \dot{\cup} \{\infty\}\}$$

is equal to $R/\mathfrak{m} \dot{\cup} \{\infty\}$ for infinitely many primes $\mathfrak{m}$.

EXAMPLE 2. *Explicit aspects of Hilbert's Irreducibility Theorem.* We continue notations from above. Let $f(x, y) \in M[x, y]$ be an irreducible polynomial. Let $\mathcal{R}_f(R)$ be the set $\{x_0 \in R | f(x_0, y)$ is reducible, as a polynomial in $M[y]\}$. One version of Hilbert's irreducibility theorem states that the complement of $\mathcal{R}_f(R)$ *in* R is infinite. In §1.B we have an arithmetic monodromy tool that allows us to consider the prospect of realizing groups as Galois groups over $\mathbf{Q}(x)$. We reserve our strongest inspection for the "simple" case when $f(x, y) = f(y) - x$ for some polynomial $f \in R[y]$. Let $\mathcal{V}_f(R) = \{x_0 \in R | f(y_0) = x_0$ for some $y_0 \in M\}$. Clearly $\mathcal{V}_f(R) \subset \mathcal{R}_f(R)$. We seek here the "theory" of the set $\mathcal{R}_f(R) - \mathcal{V}_f(R)$, denoted by $\mathcal{S}_f(R)$; when is $\mathcal{S}_f(R)$ a finite set? It is an understatement to say that the group theory involved in this problem (both solved and unsolved aspects) seems to be quite deep. We leave to the reader the analogous Stage I formulation, as it is quite similar to Example 1.

Stage II. *Translation into elementary arithmetic monodromy data.* If we are lucky, the diophantine question D of Stage I has an equivalent formulation in terms of *arithmetic monodromy groups*. That is, for $\mathfrak{p} \in \mathcal{P}$, let $M_{\mathfrak{p}}$ be the field generated by the coordinates of $\mathfrak{p}$ over M, and let $M_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})$ (resp., $M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})$) be the field of $M_{\mathfrak{p}}$-rational functions on $\mathcal{C}_{\mathfrak{p}}$ (resp., $\mathcal{C}'_{\mathfrak{p}}$). Then $M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})$ is a field extension of $M_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})$. Let $\widehat{M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})}$ be the Galois closure of the field extension $M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})/M_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})$ and let $\hat{M}_{\mathfrak{p}}$ be the algebraic closure of $M_{\mathfrak{p}}$ in $\widehat{M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})}$.

Then the *arithmetic monodromy* (resp., *geometric monodromy*) group is

$$\hat{G}_{\mathfrak{p}} \overset{\text{def}}{=} G(\widehat{M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})}/M_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})),$$

the Galois group of $\widehat{M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})}/M_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}})$ (resp., $G_{\mathfrak{p}} = G(\widehat{M_{\mathfrak{p}}(\mathcal{C}'_{\mathfrak{p}})}/\hat{M}_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{p}}))$). Again, if we are lucky, there is a statement D_G about groups such that this statement holds for $\hat{G}_{\mathfrak{p}}$ if and only if D holds for the cover $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$.

After looking at the translation of Examples 1 and 2 into arithmetic monodromy in §1.B, you might ask: how do we know which diophantine problems can be translated into arithmetic monodromy statements? You might especially ask this when you realize that this is the very step which allows us to bring to bear the powerful results on permutation groups without which there would be few definitive solutions to the types of problems presented in Examples 1 and 2. A proper answer would require a considerably more advanced exposition on the idea of *decomposition groups* (see §1.B), the idea of a *Galois stratification* as in **[FrS]**, and parts of the answer would still be conjectural.

Stage III. *Analysis of the geometric data.* Our analysis here switches to the geometric monodromy group. We turn to group theory in order to attempt a classification of the groups $G_{\mathfrak{p}}$ that satisfy the conditions resulting from Stage II. The conditions on the group $G_{\mathfrak{p}}$ are quite precise (see, for example, Proposition 2.1) coming from use of the Riemann existence theorem. They are usually phrased as conditions on a permutation representation and certain selected generators, the *branch cycles* of §0.A.

At this point we (mentally) carve the parameter space $\mathcal{P}$ of expression (1.1) into a union of disjoint pieces, $\mathcal{P} = \dot{\bigcup}_{i=1}^{t} X_i$ whereby the geometric monodromy conditions are constant along each X_i, $i = 1, \ldots, t$. Indeed, assuming that each of the curves $\mathcal{C}_{\mathfrak{p}}$ in Stage I is of genus 0 (which we *do* assume for the sake of simplicity) X_i is equipped with a natural map $X_i \overset{\Psi_i}{\to} \mathcal{H}_i$ to one of the Hurwitz parameter spaces of expression (0.10). The map Ψ_i attests to a description of the branch cycles for the cover $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ (as in Stage I) for $\mathfrak{p} \in X_i$. Assuming the success of our group theory considerations we may determine a subset S of $\{1, 2, \ldots, t\}$ such that the cover $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ satisfies the geometric monodromy conditions for $\mathfrak{p} \in \mathcal{P}$ if and only if $\mathfrak{p} \in \dot{\bigcup}_{i \in S} X_i$.

Stage IV. *Diophantine solution data.* Now, continuing the notation from Stage III, we consider separately each of the X_i's for $i \in S$. We change notation, so that X_i becomes X equipped with a map $X \overset{\Psi}{\to} \mathcal{H}$ to one of the Hurwitz parameter spaces. We say that X provides a *positive solution to the diophantine problem* D if there exists $\mathfrak{p} \in X$ such that $\mathfrak{p}$ is M-rational and if the arithmetic monodromy group $\hat{G}_{\mathfrak{p}}$ corresponding to the fiber at $\mathfrak{p}$ satisfies the condition given by D_G in Stage II. *Explicitly* deciding which of the irreducible components X_i, $i \in S$ provide positive solutions to D is the most difficult part of the whole program. The methods (still partly conjectural) by which this final step can be achieved include the results of **[Fr, 1]**, **[Fr, 2]** and **[Fr, 0, §9]**. It is these that we regard as an arithmetic form of Riemann's existence theorem, and they proceed through a delicate analysis of the fields of definition of $\mathcal{H}$ and the various neighborhoods attached to $\mathcal{H}$.

One last point. The question of whether or not X provides a positive solution to the diophantine problem D is sometimes overly subtle and outside the province of present day technique. For example, in considering the solution to Example 1 we will see that we return to the question of M-rational points on

modular curves for part of the answer. In the case that $M = \mathbf{Q}$ we *could* complete the answer to our original problem quite nicely since [**Maz**] shows that most modular curves have very few $\mathbf{Q}$-rational points. However, there are several things wrong with concluding at this point. Most Hurwitz parameter spaces do not fit into diagrams related to modular curves; and secondly, if we consider a field $M \neq \mathbf{Q}$ we do not have [**Maz**] to call upon (*yet*, anyway; see [**Frey**]). A third point is this; sometimes we are not so very interested in a fixed field M. Therefore there is a natural way out of this diophantine impasse in the case where the statement D is first considered over a field M, but for which there is a natural interpretation of D over every finite extension L of M (denote such an interpretation by $D(L)$). We say that the pair $(\mathfrak{p}, L)$ satisfies D if $\mathfrak{p} \in \mathcal{P}$ is an L-rational point of $\mathcal{P}$, and if $\mathcal{C}'_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}}$ has the desired property over L. With X as above, we say that the *solutions to D are arithmetically dense in X* if the set $X_D \overset{\text{def}}{=} \{\mathfrak{p} \in X |$ there exists L containing M with $(\mathfrak{p}, L)$ satisfies $D(L)\}$, is Zariski dense in X.

1.B. *The Čebotarev theorems and the Hilbert-Siegel theorem with application to the Schur problem and Hilbert's theorem.* Ah, if only it were possible to expose the tools of arithmetic monodromy in a complete way in a short space. Since the theorems we state here are very generally applicable to diophantine problems, for the reader inexperienced with algebraic number theory, they are best regarded as a machine whose readout is an arithmetic monodromy analysis of the diophantine properties of an irreducible curve $f(x, y) \in M[x, y]$ (see [**Fr, 0,** §8]).

We start with the arithmetic monodromy interpretation of the theorems of [**S**]. Suppose that W is a projective curve, and $W \overset{\varphi}{\to} \mathbf{P}^1$ is a cover with W and φ defined over a number field M having ring of integers R. Suppose also that x is a uniformizing variable for $\mathbf{P}^1$ and there exist infinitely many M-rational places $\mathfrak{p} \in W$ for which $x(\varphi(\mathfrak{p}))$ is in R. Then W is itself isomorphic to $\mathbf{P}^1$, and if y is a uniformizing variable for this copy of $\mathbf{P}^1$, φ is given by a rational function $f(y) = x$ for which there are at most *two* places (values of y) lying above the place $x = \infty$.

Thus, the branch cycle for the cover $W \overset{\varphi}{\to} \mathbf{P}^1$ corresponding to the place at ∞ is either an n-cycle or the product of two disjoint cycles of length s and $n - s$, respectively, where the degree of φ is n. In addition, if R has only finitely many units (e.g., $R = \mathbf{Z}$) then this branch cycle is either an n-cycle or a product of two disjoint $n/2$-cycles.

Let $f(x, y) \in \mathbf{Z}[x, y]$ be an absolutely irreducible polynomial over $\mathbf{Q}$ (i.e., irreducible over $\bar{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$). Let Ω_f be the splitting field $f(x, y)$ over the field of $\mathbf{Q}(x)$, and let $G = G(\Omega_f/\mathbf{Q}(x))$. For $x_0 \in \mathbf{Q}$ let $\Omega_{f(x_0)}$ be the splitting field of $f(x_0, y)$ over $\mathbf{Q}$. Then $G(\Omega_{f(x_0)}/\mathbf{Q})$ is naturally identified with a conjugacy class of subgroups of G, so long as x_0 is not one of the branch points $x_1, \ldots, x_r = \infty$ of the cover of the x-sphere coming from the projection of (x, y) satisfying $f(x, y) = 0$ to the x-sphere. For H a subgroup of G we consider $\mathfrak{R}(H, \mathbf{Z}) = \{x_0 \in \mathbf{Z} | G(\Omega_{f(x_0)}/\mathbf{Q})$ is conjugate in G to $H\}$. We let T_H: $G \to S_{n(H)}$ be the representation of G obtained from the action on the $n(H)$ right cosets of H. Let $\sigma_1, \ldots, \sigma_r$ be a description of the branch cycles of the cover

above, corresponding, respectively, with the points $x_1, \ldots, x_r$. Then, generalizing [S] we have

THEOREM 1.1 ([Fr, 0, §8.3]; *use last comments of* §0.A). *A necessary condition that* $\mathfrak{R}(H, \mathbf{Z})$ *be infinite is that*

(1.1)(a) $\Sigma_{i=1}^{r} \operatorname{ind}(T_H(\sigma(i))) = 2(n(H) - 1)$, *and*

(b) $T_H(\sigma(r))$ *is either an* $n(H)$*-cycle or a product of two disjoint* $n(H)/2$*-cycles.*

The case when $H = G$ is the theorem of [Hi]. The question of sufficiency in Theorem 1.1 is considered in [Fr, 0, §8.6].

Now we turn to the Čebotarev theorems. Let $f(x, y) \in R[x, y]$; let $\mathfrak{m}$ be a prime ideal of R; let $x_0 \in R/\mathfrak{m}$; and let $\Omega_{f(x_0),\mathfrak{m}}$ be the splitting field of $f(x_0, y)$ over $R/\mathfrak{m}$. Then, there exists an explicitly computable nonzero polynomial $g(x) \in R[x]$ (possibly a constant) such that if $g(x_0) \not\equiv 0 \mod \mathfrak{m}$, then $G(\Omega_{f(x_0),\mathfrak{m}}/(R/\mathfrak{m}))$ is identified with a conjugacy class of cyclic subgroups of $G(\Omega_f/M(x))$. Indeed, there is a canonical conjugacy class, denoted $\langle \sigma(\mathfrak{m}, x_0) \rangle$, in $G(\Omega_f/M(x))$ for which the subgroups of $G(\Omega_f/M(x))$ associated to $G(\Omega_{f(x_0),\mathfrak{m}}/(R/\mathfrak{m}))$ are generated, respectively, by the elements of $\langle \sigma(\mathfrak{m}, x_0) \rangle$. In addition, for $(\mathfrak{m}, x_0)$ for which $g(x_0) \not\equiv 0 \mod \mathfrak{m}$,

(1.2) the number of points (x_0, y_0) with coordinates in $R/\mathfrak{m} \dot{\cup} \{\infty\}$ is equal to the number of disjoint cycles of length 1 in $T_H(\sigma(\mathfrak{m}, x_0))$ where H is $G(\Omega_f/M(x, y))$.

Let $\hat{M}$ be the algebraic closure of M in Ω_f. *The restriction of* $\langle \sigma(\mathfrak{m}, x_0) \rangle$, *it turns out, does not depend on* x_0; therefore we let $\langle \sigma(\mathfrak{m}) \rangle$ be the resulting conjugacy class of $G(\hat{M}/M)$. Theorem 1.2 is an arithmetic monodromy combination of the classical Čebotarev density theorem of [Ce] and the Riemann hypothesis for curves over finite fields (see [Bom] and [W]).

THEOREM 1.2 ([Fr, 5, PROPOSITION 2]). *There is a constant* C (*dependent only on the degree of* f *in* x *and* y) *with the following property. Let* $|R/\mathfrak{m}|$ *be larger than* C, *and let* τ *be any element of* $G(\Omega_f/M(x))$ *whose restriction to* $\hat{M}$ *is* $\sigma(\mathfrak{m})$. *Then there exist at least* $c_\tau \cdot |R/\mathfrak{m}|$ *values of* $x_0 \in R/\mathfrak{m}$ *for which* τ *is in the class of* $\langle \sigma(\mathfrak{m}, x_0) \rangle$, *where* $c_\tau > 0$ *is not dependent on* $\mathfrak{m}$. *In addition, for any* $\bar{\tau} \in G(\hat{M}/M)$, *there exist infinitely many prime ideals* $\mathfrak{m}$ *for which* $\bar{\tau}$ *is in the class of* $\langle \sigma(\mathfrak{m}) \rangle$.

When we apply Theorems 1.1 and 1.2 to our examples, they present a common feature: the arithmetic hypotheses of the example are translated into a search for reducible members of a family of curves.

EXAMPLE 1 (*continued*). *Arithmetic monodromy interpretation of the Schur problem.* Recall that we have fixed an integer n, and we seek the rational functions of degree n for which

$$\mathcal{V}_f(R/\mathfrak{m} \dot{\cup} \{\infty\}) = R/\mathfrak{m} \dot{\cup} \{\infty\} \text{ for infinitely many prime ideals } \mathfrak{m} \text{ of } R. \tag{1.3}$$

By applying (1.2) to the case where (1.3) holds, we conclude that for each $x_0 \in R/\mathfrak{m}$, for which $g(x_0) \not\equiv 0 \mod \mathfrak{m}$ (notation as above), $\sigma(\mathfrak{m}, x_0)$ fixes

exactly *one* of the zeros $y_1, \ldots, y_n$ of $f(y) - x = 0$. By applying Theorem 1.2 we conclude that for $|R/\mathfrak{m}|$ large and $\mathfrak{m}$ satisfying (1.3), if τ is an element of $G(M(y_1, \ldots, y_n)/M(x))$ whose restriction to $\hat{M}$ is $\sigma(\mathfrak{m})$, then the coset

(1.4) $G(M(y_1, \ldots, y_n)/\hat{M}(x)) \cdot \tau$ consists only of elements that fix exactly one of $y_1, \ldots, y_n$.

If τ itself fixes y_1, by considering the elements of $G(M(y_1, \ldots, y_n)/\hat{M}(y_1)) \cdot \tau$ we easily conclude that expression (1.4) is equivalent to

(1.5) each orbit of $G(M(y_1, \ldots, y_n)/\hat{M}^{(\bar{\tau})}(y_1))$ on $y_2, \ldots, y_n$ breaks up into strictly *smaller* orbits under the action of $G(M(y_1, \ldots, y_n)/\hat{M}(y_1))$ where $\bar{\tau} = \sigma(\mathfrak{m})$ and $\hat{M}^{(\bar{\tau})}$ is the fixed field of $\bar{\tau}$ in $\hat{M}$.

By a piece of arithmetic magic **[Fr, 4]**, (1.5) is actually equivalent to (1.3), even if $|R/\mathfrak{m}|$ is *not* large. We are not, of course, suggesting that (1.5) is a simple statement: it merely leads to an accurate arithmetic monodromy interpretation that does not involve a statement about an infinite number of (possibly unknowable) primes.

Schur's original conjecture in **[Sch, 1]** (see **[Fr, 3]**) was that if f is a *polynomial* satisfying expression (1.3) then f must be a functional composition of linear polynomials and the classical polynomials given by

(1.6)(a) y^n (nth degree *cyclic polynomial*); and

(b) $T_n(y) = 2^{-n-1}\{(y + (y^2 + 4)^{1/2})^n + (y - (y^2 + 4)^{1/2})^n\}$ (nth degree *Chebychev polynomial*).

We epitomize the ad hoc nature of the subject matter around the time of the original Schur conjecture by comparing expression (1.5) with an elementary proof that compositions of linear, cyclic, and Chebychev polynomials (of degree relatively prime to 6) give one-one mappings on $\mathbf{Z}/(p)$ for infinitely many primes p. This argument **[Fr, 3,** Lemma 13] was worked out by Davenport and myself the summer before he died. It has therefore a certain sentimental value even if it may not be entirely new.

If $h(y) = y^n$, $h(y)$ clearly gives a one-one map on $Z/(p)$ if $(p - 1, n) = 1$ because the multiplicative group of nonzero elements of $\mathbf{Z}/(p)$ is a cyclic group of order $p - 1$. Let $T_n(y)$ be the nth Chebychev polynomial. There is an easily derived, and far more useful, expression for $T_n(y)$. If we let $2z = y + (y^2 - 4)^{1/2}$, then $T_n(y) = (z^n + z^{-n})/2$ where $y = (z + z^{-1})/2$. If y is an element of $\mathbf{Z}/(p)$ associate to y one of the solutions z (it makes no difference which) of $y = (z + z^{-1})/2$. All such z lie in the unique quadratic extension $\mathbf{F}(p^2)$ of $\mathbf{Z}/(p)$. If y_1, y_2 represent distinct elements of $\mathbf{Z}/(p)$ for which $T_n(y_1) = T_n(y_2)$, then either $z_1^n = z_2^n$ or $z_1^n = z_2^{-n}$ since we have $z_1^n + z_1^{-n} = z_2^n + z_2^{-n}$. The multiplicative group $\mathbf{F}(p^2) - \{0\}$ is cyclic and of order $p^2 - 1$. If $(n, p^2 - 1) = 1$, then either $z_1 = z_2$ or $z_1 = z_2^{-1}$. In either case $y_1 = y_2$ contrary to our assumption; and $T_n(y)$ is one-one as a mapping on $\mathbf{Z}(p)$. Let $h(x) = h_1(h_2(\ldots(h_r(x))\ldots))$ be a composition of linear, cyclic and Chebychev polynomials of respective degrees $n_1, \ldots, n_r$ for which $(6, N) = 1$ where $n_1 \ldots n_r = N$. Thus, from the above argument we have only to show that there exist infinitely many primes p for which $(N, p^2 - 1) = 1$. However, by Dirichlet's theorem there are infinitely many primes in the arithmetic progression $\{jN + 2 | j \in \mathbf{Z}\}$ because $(N, 2) = 1$. Also

$$(jN + 2 - 1)(jN + 2 + 1) = (jN + 1)(jN + 3)$$

is relatively prime to N since $(N, 3) = 1$, and the argument is complete.

Finally, we conclude from expression (1.5) that $G(M(y_1, \ldots, y_n)/\hat{M}(y_1))$ is *not* transitive on $y_2, \ldots, y_n$, or

(1.7) $(f_1(y) \cdot f_2(z) - f_1(z) \cdot f_2(y))/(y - z)$ is a reducible polynomial in the variables y and z where $f_1, f_2 \in \mathbf{C}[y]$ are relatively prime polynomials for which $f = f_1/f_2$.

EXAMPLE 2 (*continued*). *Explicit aspects of Hilbert's theorem.* For $f(x, y) \in \mathbf{Q}[x, y]$ an irreducible polynomial, we are led to consider the behavior for large N of the set $\mathcal{R}_f(\mathbf{Z}, N) = \{x_0 \in \mathbf{Z} | f(x_0, y)$ is reducible over M and $|x_0| < N\}$. As a consequence of Theorem 1.1 we show that there exist constants $c_1, c_2 > 0$, and an integer l for which

(1.8)(a) $c_2 \cdot N^{1/l} < |\mathcal{R}_f(\mathbf{Z}, N)| < c_1 \cdot N^{1/l}$, and $l > 1$; or

(b) $c_2 \cdot (\log(N))^l < |\mathcal{R}_f(\mathbf{Z}, N)| < c_1 \cdot (\log(N))^l$; or

(c) $|\mathcal{R}_f(\mathbf{Z}, N)|$ is bounded as a function of N.

Indeed, let H_i, $i = 1, \ldots, t$, run over the subgroups of $G(\Omega_f/\mathbf{Q}(x))$ for which H_i is *not* transitive on $y_1, \ldots, y_n$, the zeros of $f(x, y)$; the fixed field of H_i in Ω_f is of the form $\mathbf{Q}(t_i)$ for an element $t_i \in \Omega_f$; and there exists $g_i \in \mathbf{Q}(z)$ for which $g_i(t_i) = x$ where either

(1.9)(a) g_i is a polynomial; or

(b) g_i is the ratio of two polynomials of equal degree with the denominator a power of an irreducible quadratic polynomial over $\mathbf{Q}$.

If $\mathcal{V}_{g_i}(\mathbf{Z}) = \{x_0 \in \mathbf{Z} | g_i(z) = x_0$ has a solution in $\mathbf{Q}\}$, then Theorem 1.1 concludes that

(1.10) $R_f(\mathbf{Z}) \subset (\bigcup_{i=1}^{t} \mathcal{V}_{g_i}(\mathbf{Z})) \cup \bar{V}$ where $\bar{V}$ is a finite set.

It is now easy to conclude expression (1.8) (see [**Lev**]) and that

(1.11) $f(g_i(z), y)$ is reducible as a rational function in two variables, $i = 1, \ldots, t$.

We say that $\mathcal{R}_f(\mathbf{Z})$ has *exponential* (resp., *logarithmic*) density if (1.8)(b) (resp., (1.8)(a)) holds.

2. Group theory and Stage III considerations. Literary motivation for this section is contained in [**Ca, 1**], [**Kan**], [**Sc, 1**]–[**Sc, 3**] and many of the applications and results are in [**DLSc, 1**], [**DLSc, 2**], [**DSc**], [**E**], [**Fr, 3**], [**Fr, 5**]–[**Fr, 8**], [**FrSc**], [**FrSm**], [**Mc**], and [**Tv**]. The problem: considering the *reducibility* of $h(z, y) \in \mathbf{C}[z, y]$ where $h(z, y)$ has "*variables separated*". That is,

$$h(z, y) = h_1(y) \cdot g_2(z) - g_1(z) \cdot h_2(y) \tag{2.1}$$

where h_1, h_2 (and g_1, g_2) are relatively prime pairs of polynomials in $\mathbf{C}[y]$ (resp., $\mathbf{C}[z]$).

Of special importance is the case when $h_2(y) = 1 = g_2(y)$, so that we are considering the reducibility of $h(z, y) = h(y) - g(z)$. The impact of group theory appears in our use of [**Bu**], [**F, 1**], [**F, 2**], [**Sco**], [**Sch**], [**Wa**], and [**Wie, 1**]. Each of the subsections contains explicit problems stated entirely in group theoretic terms.

2.A. *Group theory and geometric monodromy as applied to the reducibility of variables separated polynomials.* We start with an ordered pair of positive integers (n, m) and we let $\mathcal{R}(n, m)$ denote the ordered pairs of rational functions in $\mathbf{C}(y)$ of respective degrees n and m:

$\mathcal{R}(n, m) = \{(h_1(y), h_2(y); g_1(y), g_2(y)) | h_1, h_2, g_1, g_2 \in \mathbf{C}[y]$, and $\max(\deg(h_1), \deg(h_2)) = n$, $\max(\deg(g_1), \deg(g_2)) = m$ and h_1 and h_2 (resp., g_1 and g_2) are relatively prime$\}$.

If $(h_1, h_2; g_1, g_2) \in \mathcal{R}$, then h_1/h_2 and g_1/g_2 represent rational functions of respective degree n and m. For our considerations a certain subset of $\mathcal{R}(n, m)$ should be removed.

DEFINITION 2.1. Given two rational functions $h, g \in \mathbf{C}(y)$, g is said to be *composite with* h if $g = h(s(y))$ for some $s(y) \in \mathbf{C}(y)$. In the case that $s(y)$ is a linear fractional transformation we say that g and h are *linearly related*. Suppose $(h_1, h_2; g_1, g_2) \in \mathcal{R}(n, m)$ and there exists $m(y) \in \mathbf{C}(y)$ with: $\deg(m(y)) > 1$; and both h and g are composite with $m(y)$. Write $m(\bar{s}(y)) = h(y)$ and $m(\bar{\bar{s}}(y)) = g(y)$ with $\bar{s}_1(y)/\bar{s}_2(y) = \bar{s}(y)$, and $\bar{\bar{s}}_1(y)/\bar{\bar{s}}_2(y) = \bar{\bar{s}}(y)$ where $\bar{s}_1$, $\bar{s}_2$ (resp., $\bar{\bar{s}}_1$, $\bar{\bar{s}}_2$) are relatively prime polynomials. It is easily checked (use Gauss' lemma) that $\bar{s}_1(y) \cdot \bar{\bar{s}}_2(z) - \bar{\bar{s}}_1(z) \cdot \bar{s}_2(y)$ is a factor of $h(z, y) = h_1(y) \cdot g_2(z) - g_1(z) \cdot h_2(y)$. We say that $(h_1, h_2; g_1, g_2)$ *is composite with* $m(y)$. If there is *no* $m(y)$ for which $\deg(m(y)) > 1$ and $(h_1, h_2; g_1, g_2)$ is composite with $m(y)$, we say that $(h_1, h_2; g_1, g_2)$ is *not composite* (or $h(y)$ and $g(y)$ are a noncomposite pair of rational functions). *We let* $\mathcal{R}(n, m)^{\mathrm{NC}}$ *be the* $(h_1, h_2; g_1, g_2)$ in $\mathcal{R}(n, m)$ *which are not composite.*

It is clear that $\mathcal{R}(n, m)^{\mathrm{NC}}$ is naturally isomorphic is an open subset of $A^{2(n+1)+2(m+1)}$-space, by using the coefficients of the polynomials involved as variables.

Now we introduce a new variable x, and we let $\mathbf{P}^1_x$ be a copy of $\mathbf{P}^1$ for which x is a uniformizing variable. Similarly we let $\mathbf{P}^1_y$ (resp., $\mathbf{P}^1_z$) be a copy of $\mathbf{P}^1$ for which y (resp., z) is a uniformizing variable. For each $(h_1, h_2; g_1, g_2) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ we obtain maps: $\mathbf{P}^1_y \overset{\varphi(h(y))}{\to} \mathbf{P}^1_x$ (i.e., $y^0 \in \mathbf{P}^1_y \ni h(y^0) = x^0$) and $\mathbf{P}^1_z \overset{\varphi(g(z))}{\to} \mathbf{P}^1_x$. For notational convenience we sometimes use the symbol (h, g) in place of $(h_1, h_2; g_1, g_2)$. Let $\mathcal{S}(h, g)$ be the fibered product $\mathbf{P}^1_y \times_{\mathbf{P}^1_x} \mathbf{P}^1_z$ (as in §0.B). Then we have a natural map: $\mathcal{S}(h, g) \overset{\varphi(h, g)}{\to} \mathbf{P}^1_x$. The irreducible components of $\mathcal{S}(h, g)$ are in one-one correspondence with the irreducible factors of

$$h(z, y) = h_1(y) \cdot g_2(z) - g_1(z) \cdot h_2(y)$$

since the curve $h(z, y) = 0$ is easily identified with a Zariski open subset of $\mathcal{S}(h, g)$.

For $(h, g) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ we let $D(h, g)$ be the statement: $\mathcal{S}(h, g)$ is reducible. Our problem: explicitly describe the locus of points $(h, g) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ for which $D(h, g)$ is true.

Now, in order to proceed to Stage III considerations, we need to interpret $D(h, g)$ in terms of geometric monodromy groups. From the map $\mathbf{P}^1_y \overset{\varphi(h)}{\to} \mathbf{P}^1_x$ (resp., $\mathbf{P}^1_z \overset{\varphi(g)}{\to} \mathbf{P}^1_x$) we obtain an extension of fields, $\mathbf{C}(\mathbf{P}^1_y)/\mathbf{C}(\mathbf{P}^1_x)$ (resp., $\mathbf{C}(\mathbf{P}^1_z)/\mathbf{C}(\mathbf{P}^1_x)$). By using the uniformizing variables, the extension $\mathbf{C}(\mathbf{P}^1_y)/\mathbf{C}(\mathbf{P}^1_x)$ can be identified with $\mathbf{C}(y)/\mathbf{C}(x)$. We let $\widehat{\mathbf{C}(y)}$ (resp., $\widehat{\mathbf{C}(z)}$), as in §1.A, Stage II, be the Galois closure of the extension $\mathbf{C}(y)/\mathbf{C}(x)$ (resp., $\mathbf{C}(z)/\mathbf{C}(x)$). In order to be compatible with the literature, we use the following notation: $\Omega_{h-x} = \widehat{\mathbf{C}(y)}$; $\Omega_{g-x} = \widehat{\mathbf{C}(z)}$; and $\Omega_{(h,g)} = \Omega_{h-x} \cdot \Omega_{g-x}$. *The geometric monodromy group of the*

cover $\mathcal{S}(h, g) \to \mathbf{P}^1_x$ *is identified with* $G(\Omega_{(h,g)}/\mathbf{C}(x))$. This group has two permutation representations: T_h: $G(\Omega_{(h,g)}/\mathbf{C}(x)) \to S_n$ obtained from the right cosets of $G(\Omega_{(h,g)}/\mathbf{C}(y))$; and T_g: $G(\Omega_{(h,g)}/\mathbf{C}(x)) \to S_m$ obtained from the right cosets of $G(\Omega_{(h,g)}/\mathbf{C}(z))$.

Consider the statement $D(G, T_1, T_2)$, associated to triples (G, T_1, T_2) (where T_1 and T_2 are representations of the group G): T_1 and T_2 are transitive, nonequivalent permutation representations, such that $G(T_1, 1) = \{\sigma \in G | (1)T_1(\sigma) = 1\}$ is an *intransitive* group under the representation T_2: $G(T_1, 1) \to S_m$.

PROPOSITION 2.1. *The statement* $D(h, g)$ (*i.e.*, $\mathcal{S}(h, g)$ *is reducible*) *is true if and only if the statement* $D(G(\Omega_{(h,g)}/\mathbf{C}(x)), T_h, T_g)$ *is true.*

PROOF. Indeed, from the Galois correspondence, the irreducible components of $\mathcal{S}(h, g)$ are in one-one correspondence with the orbits of $G(T_h, 1)$ in the representation T_g.

Thus, in Proposition 2.1 we have completed the translation of statement $D(h, g)$ to the geometric monodromy statement $D(G, T_h, T_g)$. We can expedite the use of Riemann's existence theorem in the later stages by continuing with further Galois theoretic observations. For brevity we quote the appropriate, relatively easy, results from [**Fr, 6**] without proof.

DEFINITION 2.2. Let $h(y) \in \mathbf{C}(y)$. We say that $h(y)$ is *decomposable* if $h(y) = h^{(1)}(h^{(2)}(y))$ where $\deg(h^{(i)}(y)) > 1$ for $i = 1, 2$. If such $h^{(1)}$ and $h^{(2)}$ do not exist then $h(y)$ is *indecomposable*.

LEMMA 2.1 [**Fr, 6**, PROPOSITION 2]. *Let* $(h_1, h_2; g_1, g_2) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ *and assume that* $\mathcal{S}(h, g)$ *is reducible. Then there exist rational functions* $h^{(1)}$, $h^{(2)}$, $g^{(1)}$, $g^{(2)} \in \mathbf{C}(y)$ *with these properties*:

(2.2)(a) $h(y) = h^{(1)}(h^{(2)}(y))$, $g(y) = g^{(1)}(g^{(2)}(y))$;

(b) $\Omega_{h^{(1)}-x} = \Omega_{g^{(1)}-x} = \Omega_{(h^{(1)},g^{(1)})}$; *and*

(c) *the irreducible components of* $\mathcal{S}(h^{(1)}, g^{(1)})$ *are in one-one correspondence with the irreducible components of* $\mathcal{S}(h, g)$.

The effect of Lemma 2.1 is that, in considering the irreducibility of $\mathcal{S}(h, g)$, we may restrict consideration to those $h, g \in \mathbf{C}(y)$ for which $\Omega_{h-x} = \Omega_{g-x} = \Omega_{(h,g)}$. In this case, the representations T_h and T_g of $G(\Omega_{(h,g)}/\mathbf{C}(x))$ are both *faithful* representations. Now we quote Riemann's existence theorem in an appropriate form.

LEMMA 2.2 [**Fr, 6**, PROPOSITION 4]. *Let* G^* *be a finite group with two faithful transitive representations* T_1^* *and* T_2^*. *Suppose that* G^* *is generated by elements* $\sigma(1)^*, \ldots, \sigma(r)^*$ *for which* $\sigma(1)^* \ldots \sigma(r)^* = \mathrm{Id}$. *Let* $z_1, \ldots, z_r$ *be distinct elements of* $\mathbf{P}^1_x$. *Then* (2.3) *and* (2.4) *are equivalent.*

There exist rational functions $h(y), g(y) \in \mathbf{C}(y)$ *as follows*:

(2.3)(a) $\mathbf{P}^1_y \xrightarrow{\varphi(h)} \mathbf{P}^1_x$ *and* $\mathbf{P}^1_z \xrightarrow{\varphi(g)} \mathbf{P}^1_x$ *are ramified only over* $z_1, \ldots, z_r$;

(b) $\Omega_{h-x} = \Omega_{g-x} = \Omega_{(h,g)}$;

(c) $G(\Omega_{(h,g)}/\mathbf{C}(x)) \simeq G^*$ *and* T_h (*resp.*, T_g) *is equivalent as a permutation representation to* T_1^* (*resp.*, T_2^*); *and*

(d) $(T_1^*(\sigma(1)^*), \ldots, T_1^*(\sigma(r)^*))$ *(resp.,* $(T_2^*(\sigma(1)^*), \ldots, T_2^*(\sigma(r)^*))$*) is a description of the branch cycles for the cover* $(\mathbf{P}_y^1, \varphi(h))$ *(resp.,* $(\mathbf{P}_z^1, \varphi(g))$*).*

The Riemann-Hurwitz formula (§0.A) *takes the form.*

(2.4)(a) $\sum_{j=1}^r \operatorname{ind}(T_1^*(\sigma(j)^*)) = 2(n-1)$, *and*

(b) $\sum_{j=1}^r \operatorname{ind}(T_2^*(\sigma(j)^*)) = 2(m-1)$

where $\deg(T_1^*) = n$, $\deg(T_2^*) = m$.

In addition, if $z_r = \infty$, *then we may take* $h(y)$ *(resp.,* $g(y)$*) to be a polynomial if and only if*

(2.4)(c) $n = m$, *and* $T_1^*(\sigma(r)^*)$ *and* $T_2^*(\sigma(r)^*)$ *are both n-cycles.*

From these remarks, the *consideration of pairs* $(h, g) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ *for which* $\mathcal{S}(h, g)$ *is reducible is equivalent to the description of the Hurwitz parameter spaces* (*of* §0.*B*) $\mathcal{H}(n, r; \mathbf{P}_y^1, \varphi(h))$ *where* $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ *has a description of its branch cycles given by* $(\sigma(1)^*, \ldots, \sigma(r)^*) = \boldsymbol{\sigma}^*$ *as in Lemma* 2.2.

The case where h and g are *polynomials* and $h(y)$ is indecomposable (as in Definition 2.2) is of extraspecial concern. For the remainder of this subsection we concentrate on this case in order to focus our group theory and algebraic geometry concerns.

DEFINITION 2.3. Let F be a finite ring. A set of distinct elements $D = \{d_1, \ldots, d_k\}$ form a *difference set* of multiplicity r if the differences $\{d_i - d_j$ for $i \neq j\}$ run over all the values of $F - \{0\}$ exactly r times. If $|F| = n$ we say that we have an $\{n, k, r\}$ design. If $F = \mathbf{Z}/(n)$, then D is said to be a *cyclic difference set*. In the latter case, an element $\alpha \in \mathbf{Z}/(n)$ is said to be a *multiplier* of the difference set D if $\{\alpha \cdot d_1, \ldots, \alpha \cdot d_k\} = \{d_1 + t, \ldots, d_k + t\} = D + t$. The sets D, $D + 1, \ldots, D + t$ are the *blocks of the design.*

THEOREM 2.1. *Let* $(h, g) \in \mathcal{R}(n, m)^{\mathrm{NC}}$ *where:* $h, g \in \mathbf{C}[y]$ (*i.e., they are polynomials*); h *is indecomposable*; *and* $\mathcal{S}(h, g)$ *is reducible. There exist polynomials* $g^{(1)}, g^{(2)} \in \mathbf{C}[y]$ *such that:* $\deg(h) = \deg(g^{(1)})$; $g(z) = g^{(1)}(g^{(2)}(z))$; $\Omega_{h-x} = \Omega_{g^{(1)}-x}$; *and the irreducible components of* $\mathcal{S}(h, g)$ *are in one-one correspondence with the irreducible components of* $\mathcal{S}(h, g^{(1)})$.

Furthermore,

(2.5)(a) $g^{(1)}$ *is indecomposable*;

(b) T_h *and* $T_{g^{(1)}}$ (*representations of* $G(\Omega_{h-x}/\mathbf{C}(x))$) *are two doubly transitive representations which are inequivalent as permutation representations, but equivalent as group representations*;

(c) $\mathcal{S}(h, g^{(1)})$ *has exactly two irreducible components*;

(d) *if* X_1 *and* X_2 *are the irreducible components of* $\mathcal{S}(h, g^{(1)})$ *given in* (c), *then the degree of the map* $X_1 \overset{\varphi(h, g^{(1)})}{\to} \mathbf{P}_x^1$, *call this* k, *satisfies* $(n-1) | k(k-1)$; *and*

(e) *there exists a difference set modulo* n *of cardinality* k.

Still further: for $\boldsymbol{\sigma}^* = (\sigma(1)^*, \ldots, \sigma(r)^*)$ *a description of the branch cycles of the cover* $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ *we take* $\sigma(r)^*$ *to be the branch cycle corresponding to* $\infty \in \mathbf{P}_x^1$. *Then, since* h *is a polynomial,* $T_h(\sigma(r)^*)$ *and* $T_{g^{(1)}}(\sigma(r)^*)$ *are both n-cycles* (*identified as n-cycles of the design indicated in* (2.5)(e)). *In addition*:

(2.6)(a) r *is equal to* 3 *or* 4; *and*

(b) $\sum_{i=1}^{r-1} T_h(\sigma(i)^*) = n - 1 = \sum_{i=1}^{r-1} T_{g^{(1)}}(\sigma(i)^*)$.

OUTLINE OF PROOF [**Fr, 6**, §3 for details]. The first paragraph is a restatement of Lemma 2.1. From [**Fr, 3,** Lemma 9], since h is indecomposable, T_h is doubly transitive unless h is a *cyclic* or *Chebychev* polynomial.

If h is a cyclic or Chebychev polynomial (expression (1.6)), [**Fr, 3,** Lemma 11] shows that h and $g^{(1)}$ are linearly related (Definition 2.1) contrary to our assumption that (h, g) is in $\mathfrak{R}(n, m)^{NC}$.

For the remainder of our comments we replace $g^{(1)}$ by g, so that $\deg(h) = \deg(g)$. Let $y_1^*, \ldots, y_n^*$ (resp., $z_1^*, \ldots, z_n^*$) be the zeros of $h(y) - x$ (resp., $g(z) - x$), so that $\mathbf{C}(y_1^*, \ldots, y_n^*) = \Omega_{h-x} = \Omega_{g-x} = \mathbf{C}(z_1^*, \ldots, z_n^*)$ where we identify y_i^* with the integer i in the representation T_h. Let $y_1^*, y_{\alpha(2)}^*, \ldots, y_{\alpha(k)}^*$ be in the orbit of y_1^* under the action of $G(\Omega_{(h,g)}/\mathbf{C}(z_1^*))$. The linear representation associated with a doubly transitive representation [**H**, Theorem 16.6.15, p. 284] is the sum of the principal representation [**H**, Theorem 16.6.15, p. 284] is the sum of the principal representation and an irreducible linear representation. Thus, the subspace of relations $\{\sum a_i \cdot y_i^* = b \text{ with } a_1, \ldots, a_n, b \in \mathbf{C}\}$ is of dimension 1, generated by $(\sum_{i=1}^n y_i^*) - c$, for some constant $c \in \mathbf{C}$. In particular, $y_1^* + y_{\alpha(2)}^* + \cdots + y_{\alpha(k)}^*$ is not a constant: indeed, it is $\bar{a} \cdot z_1^* + \bar{b}$ for some $\bar{a}, \bar{b} \in \mathbf{C}$. From this we immediately deduce that the representations T_h and T_g (of $G(\Omega_{(h,g)}/\mathbf{C}(x))$) are *equivalent* as group representations, and T_g is a doubly transitive permutation representation. If g were decomposable, from Galois theory it is easily deduced that T_g would be imprimitive (there would be a proper field between $\mathbf{C}(z)$ and $\mathbf{C}(x)$). The double transitivity of T_g therefore gives (2.5)(a) and (b). It also gives (2.5)(c) by the following argument. Let $m(z, y)$ be an irreducible factor of $h(y) - g(z)$, and let $y_{\beta(1)}^*, \ldots, y_{\beta(u)}^*$ be the zeros of $m(z_1^*, y)$. Then, if the degree of $m(z_1^*, y)$ in y is k, the coefficient of y^{k-1} is of degree 1 in z_1^*, and we obtain the relation $\bar{\bar{a}} z_1^* + \bar{\bar{b}} = y_{\beta(1)}^* + \cdots + y_{\beta(u)}^*$ for some $\bar{\bar{a}}, \bar{\bar{b}} \in \mathbf{C}$. From [**H**, loc. cit.], this is one relation too many, unless (2.5)(c) holds.

Let $T_h(\sigma(r)^*) = (1\ 2 \cdots n)$, and $T_g(\sigma(r)^*) = (1\ 2 \cdots n)$, an assumption that we can make with no loss by changing T_h and T_g to equivalent permutation representations. We easily see that the conjugates of z_1^* over $\mathbf{C}(y_1^*)$ are

$$z_1^*, (z_1^*)(\sigma(r)^*)^{1-\alpha(2)}, \ldots, (z_1^*)(\sigma(r)^*)^{1-\alpha(k)}. \tag{2.7}$$

Thus, the conjugates of z_1^* over $\mathbf{C}(y_{\alpha(j)}^*)$ are of the form

$$(z_1^*)(\sigma(r)^*)^{\alpha(j)-\alpha(i)}, \qquad i = 1, \ldots, k. \tag{2.8}$$

Now assume that z_2^* is a conjugate of z_1^* over $\mathbf{C}(y_{\alpha(j)}^*)$ for t values of j. Since G is doubly transitive on $z_1^*, \ldots, z_n^*$, each z_u^*, with $u \neq 1$, is conjugate to z_1^* over $\mathbf{C}(y_{\alpha(j)}^*)$ for exactly t of the $y_{\alpha(j)}^*$. Hence $t \cdot (n-1) = k \cdot (k-1)$ and the set $\{1, \alpha(2), \ldots, \alpha(k)\}$ is a difference set modulo n. With this we conclude the results of expression (2.5).

We give a proof of (2.6)(a) in the case that $n - 1 = k \cdot (k-1)$. The remainder of expression (2.6) is given by Lemma 2.2.

Let $\{\alpha(1), \ldots, \alpha(k)\}$ be the difference set determined above, and recall that

$$az_j^* + b = y_{j+\alpha(1)}^* + \cdots + y_{j+\alpha(k)}^*, \qquad j = 1, \ldots, n.$$

Define a finite projective plane π: $\{y_1^*, \dots, y_n^*\}$ are the points and $\{z_1^*, \dots, z_n^*\}$ are the lines; with y_i^* "on" z_j^* provided $i \equiv \alpha(u) + j \pmod n$ for some $u = 1, \dots, k$. Clearly $G = G(\Omega_{h-x}/\mathbf{C}(x))$ acts as a doubly transitive group of collineations on π. It follows from a theorem of Wagner [**Wa**] that π has order $n = q^2 + q + 1$, where q is a power of a prime. Now, nonidentity collineations of projective planes can never fix 4 noncollinear points. Hence, each $\sigma \neq \mathrm{Id}$ in G fixes at most $q + 2$ of the points $\{y_1^*, \dots, y_n^*\}$. Thus $\mathrm{ind}(\sigma) \geqslant (q^2 - 1)/2$ and

$$q^2 + q = n - 1 = \sum_1^{r-1} \mathrm{ind}(\sigma(i)) \geqslant (r - 1)(q^2 - 1)/2. \tag{2.9}$$

Therefore the number $r - 1$ of finite branch points of the cover $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ is at most $2q/q - 1$. For $q = 2$, the expression $\mathrm{ind}(\sigma) \geqslant (q^2 - 1)/2$ used above should be replaced by $\mathrm{ind}(\sigma) \geqslant (q^2 - 1)/2 + \frac{1}{2}$ (since $q^2 - 1$ is odd). Thus, in this case we need an ad hoc argument that $r - 1 \leqslant 3$. For $q > 2$, $2q/q - 1$ is at most 3 (with equality only for $q = 3$, $n = 13$).

The general case of expression (2.6)(a) follows from a theorem of Feit [**F, 1,** Theorem 4] when combined with the method of proof given above.

Let $\mathcal{P}(n, m)^{\mathrm{NC}}$ be the subset of $\mathcal{R}(n, m)^{\mathrm{NC}}$ consisting of the pairs (h, g) with h and g *polynomials. From Lemma* 2.2 *we may, with no loss, assume that* $n = m$ *in investigating the polynomial pairs* (h, g) *for which* $\mathcal{S}(h, g)$ *is reducible.*

DEFINITION 2.4. Suppose that $(h, g) \in \mathcal{P}(n, n)^{\mathrm{NC}}$, and that $\mathcal{S}(h, g)$ is reducible. We say that $\mathcal{S}(h, g)$ *is newly reducible* if $\mathcal{S}(h^{(1)}, g)$ is *irreducible* for $h^{(1)}$, $h^{(2)} \in \mathbf{C}[y]$ with $h^{(1)}(h^{(2)}(y)) = h(y)$, and $\deg(h^{(1)}) < \deg(h)$.

In §2.B we state the following problem entirely in terms of group theory.

Problem 2.1. *Describe explicitly the pairs* $(h, g) \in \mathcal{P}(n, n)^{\mathrm{NC}}$ *for which*:

(a) (h, g) *is newly reducible*; *or for which*

(b) (h, g) *is reducible and* $h(y)$ *is indecomposable* (*in particular*, (h, g) *is newly reducible*).

2.B. *Newly reducible polynomial pairs*; *living up to an example of B. Birch*; *and some theorems of Feit.* In this subsection we respond in depth to Problem 2.1. Let us start slowly by considering $\mathcal{P}(n, n)^{\mathrm{NC}}$ for low values of n. For $n = 2$: there are no reducible polynomial pairs $(h, g) \in \mathcal{P}(2, 2)^{\mathrm{NC}}$, since $y^2 - z^2 - a$ is irreducible for $a \neq 0$. The same holds for $n = 3$ by applying Lemma 2.2 to a description of the branch cycles of $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ in the case $\deg(h) = 3$, and noting that $\mathcal{S}(h, g)$ reducible implies that g is composite with h. Our first real example must await $n = 4$. Indeed, for $h(y) = y^4 + 2y^2$, $g(y) = -4y^4 - 4y^2 - 1$,

$$h(y) - g(z) = (y^2 + 2yz + 2z^2 + 1)(y^2 - 2yz + 2z^2 + 1). \tag{2.10}$$

In the notation of §2.A; there are generators $\sigma(1)^*$, $\sigma(2)^*$, $\sigma(3)^*$ of $G(\Omega_{(h,g)}/\mathbf{C}(x))$ for which $T_h(\sigma(1)^*) = (1\ 3)$, $T_h(\sigma(2)^*) = (4\ 3)(2\ 1)$, and $T_h(\sigma(3)^*) = (1\ 2\ 3\ 4)^{-1}$ (resp., $T_g(\sigma(1)^*) = (1\ 2)(3\ 4)$, $T_g(\sigma(2)^*) = (4\ 2)$, and $T_g(\sigma(3)^*) = (1\ 2\ 3\ 4)^{-1}$) is a description of the branch cycles of $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ (resp., $\mathbf{P}_z^1 \overset{\varphi(g)}{\to} \mathbf{P}_x^1$).

Now consider $\mathcal{P}(5, 5)^{\mathrm{NC}}$. Since there is no difference set modulo 5, Theorem 2.1 implies that the set of $(h, g) \in \mathcal{P}(5, 5)^{\mathrm{NC}}$ for which $\mathcal{S}(h, g)$ is reducible is empty. Similarly, for $n = 6$. If $(h, g) \in \mathcal{P}(6, 6)^{\mathrm{NC}}$, and $\mathcal{S}(h, g)$ is reducible, then h must be decomposable. The monodromy group of $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$ is easy to work

out in this case, and once again we are able to say that the set of $(h, g) \in \mathcal{P}(6, 6)^{NC}$ for which $\mathcal{S}(h, g)$ is reducible is empty.

When we come to the case $n = 7$, however, we come upon B. Birch's *brute force calculation*. Let

$$h(t, y) = h(y) = y^7 - 7\lambda t \cdot y^5 + (4 - \lambda)t \cdot y^4 + (14\lambda - 35)t^2 \cdot y^3 - (8\lambda + 10)t^2 \cdot y^2 + \left[(3 - \lambda)t^2 + 7(3\lambda + 2)t^3\right] \cdot y - \tfrac{1}{3}t^3$$

where t is a parameter, $\lambda = \frac{1}{2}(1 - \sqrt{-7})$, and $\mu = \frac{1}{2}(1 + \sqrt{-7})$. Then, by taking $g(z) = -\overline{h(z)}$ (complex conjugation of the coefficients of $h(z)$), $h(y) - g(z) = \varphi_1(y, z) \cdot \varphi_2(y, z)$ with

$$\varphi_1(y, z) = y^3 - \lambda y^2 \cdot z - \mu y \cdot z^2 + z^3 - (3\lambda + 2) \cdot t \cdot y - (3\mu + 2) \cdot t \cdot z + t,$$

$$\varphi_2(y, z) = y^4 + \lambda y^3 \cdot z - y^2 \cdot z^2 + \mu \cdot y \cdot z^3 + z^4 + 2(\mu - \lambda) \cdot t \cdot y^2 + 7t \cdot y \cdot z + 2(\lambda - \mu) \cdot t \cdot z^2 + (3 - \lambda) \cdot t \cdot y + (3 - \mu) \cdot t \cdot z - 7t^2. \tag{2.11}$$

All of the $(h', g') \in \mathcal{P}(7, 7)^{NC}$ for which $\mathcal{S}(h', g')$ is reducible can be obtained from expression (2.11) by specializing t.

In **[Fr, 0,** §5.3] we show that there are *two* families of pairs of degree 13 polynomials (h, g) for which $\mathcal{S}(h, g)$ is reducible where the families are defined over the field $Q(\zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9)$.

The main point is that the coefficients of the family explicitly written out by Birch lie in a genus zero function field. As n gets large, the amount of work in computing such an example becomes catastrophic. Worse still, if the field of coefficients were not of genus zero, it is hard to image such a computation as this, even for $n = 7$, being feasible. The example with $n = 13$ also has coefficients in a genus zero field. This is shown through the theory of the Hurwitz parameter space.

Problem (Conjecture) 2.2. (*See* **[Kan]** *for a complete discussion.*) *Consider triples* (G, T_1, T_2) *where* T_1 *and* T_2 *are distinct faithful, doubly transitive permutation representations of* G *of degree* n *with these properties*:

(2.12)(a) T_1 *and* T_2 *are equivalent as representations of* G; *and there exists* $\sigma \in G$ *such that*

(b) $T_1(\sigma)$ *and* $T_2(\sigma)$ *are both* n*-cycles.*

Must one of the following be true:

(2.13)(a) G *is a group of collineations of a finite projective geometry with* T_1 *the representation of* G *on the points,* T_2 *the representation of* G *on the hyperplanes*; *or*

(b) $n = 11$?

Now we concentrate on part (b) of Problem 2.1.

THEOREM 2.2. *There exist polynomial pairs* $(h, g) \in \mathcal{P}(n, n)^{NC}$ *for which*

(2.14) h *is indecomposable (Definition* 2.2) *and* $\mathcal{S}(h, g)$ *is reducible in the case that* $n = 7$, 11, 13, 15, 21, *and* 31. *If* $n - 1 = k(k - 1)$ *where* k *is the degree of one of the irreducible components of* $\mathcal{S}(h, g)$ *over* $\mathbf{P}^1_x$, *then we must have* $n = 7$, 13, *or* 21. *If expression* (2.12) *implies expression* (2.13), *then the only possible pairs* (h, g) *for which expression* (2.14) *holds are those of degree* $n = 7$, 11, 13, 15, 21, *and* 31. *Thus, if we could answer Problem* 2.2 *affirmatively, we would have a complete answer to Problem* 2.1, *part* (b).

DISCUSSION OF PROOF. From Lemma 2.2 and Theorem 2.1 it is sufficient to give a description of the branch cycles of the cover $\mathbf{P}^1_y \overset{\varphi(h)}{\to} \mathbf{P}^1_x$. This is a tedious exercise which we have undertaken for $n = 7, 11, 13, 15, 21$, and 31. The method for doing this appears in [**Fr, 0**, §5.3]. Feit (in [**F, 2**]) has also demonstrated the existence of these branch cycles by another method.

Now assume that $n - 1 = k \cdot (k - 1)$. We return to the proof of Theorem 2.1 where we have seen that: $r' = r - 1$, the number of *finite* branch points, cannot exceed 3; and the group $G(\Omega_{(h,g)}/\mathbf{C}(x))$ is a group of collineations on a projective plane. Let $\sigma(1)^*, \ldots, \sigma(r)^*$ be a description of the branch cycles of $(\mathbf{P}^1_y, \varphi(h))$ where $\sigma(r)^*$ is an n-cycle.

Suppose a branch cycle σ^* is of order $m \geqslant 3$. Since G is a group of collineations on the projective plane π; the element σ^* carries lines to lines and hence both σ^* and $(\sigma^*)^2$ fix at most $q + 2$ point. Therefore, in the expression of σ^* as a product of cycles all but $q + 2$ of the points lie in cycles of length at least 3. Hence $\text{ind}(\sigma^*) \geqslant \frac{2}{3}(q^2 - 1)$, with equality holding only if $q + 2$ points are left fixed and σ^* is of order 3.

If $r = 2$ then h and g are both cyclic polynomials of the same degree and hence are linearly related, contrary to our assumptions [**Fr, 3**, p. 47].

If $r = 3$ and the branch cycles $\sigma(1)^*$ and $\sigma(2)^*$ are each of order 2, then h and g must be linearly related to a Chebychev polynomial [**Fr, 3**, p. 47]. Since h is indecomposable $\deg(h)$ is a prime p, and h and g are linearly related to the unique Chebychev polynomial of that prime degree having the same branch points as the cover $\mathbf{P}^1_y \overset{\varphi(h)}{\to} \mathbf{P}^1_x$.

Now suppose $r = 3$ and that $\sigma(1)^*$ has order greater than 2. Then $q^2 + q = \text{ind}(\sigma(1)^*) + \text{ind}(\sigma(2)^*) \geqslant \frac{7}{6}(q^2 - 1)$, whence $q \leqslant 7$. For $q = 7$, we must have $\text{ind}(\sigma(1)^*) = \frac{2}{3}(q^2 - 1)$ and $\text{ind}(\sigma(2)^*) = \frac{1}{2}(q^2 - 1)$. Thus, $\sigma(1)^*$ and $\sigma(2)^*$ both fix a line and so both fix the common point; contrary to $\sigma(1)^* \cdot \sigma(2)^* = (1\ 2 \cdot \cdots \cdot n)^{-1}$. The remaining possibilities $q = 2, 3$, and 4 give us the possibilities $n = 7$, 13, and 21. The case $q = 5$ (or $q^2 + q + 1 = 31$) does not yield an example ([**F**, 2]).

If $r = 4$, then $q^2 + q \geqslant \frac{3}{2}(q^2 - 1)$ whence $q \leqslant 3$ ($n = 7, 13$) and each $\sigma(i)^*$ is of order 2.

Details, and the general case (i.e., where we do not assume that $n - 1 = k(k - 1)$) can be found in [**F, 2**]. Feit has also pointed out that we do not need to know that Problem 2.2 has an affirmative answer in the case that $n \leqslant 100$ as the calculations of [**F, 2**] handle this case.

2.C. *Double degree representations; theorems of Scott and Wielandt; the irreducible components of composite pairs.* The notations of §2.B remain in force. In §2.B we investigated in great detail the irreducible components of $\mathfrak{S}(h, g)$ for $(h, g) \in \mathcal{P}(n, m)^{\text{NC}}$ and h an indecomposable polynomial; the case corresponding to many of the present applications of the theory of the irreducible factors of polynomials with separated variables. The success of that investigation provides motivation for the further study of the irreducible components of $\mathfrak{S}(h, g)$ where

(2.15) $(h, g) \in \mathcal{R}(p, m)^{\text{NC}}$ *and h is a polynomial of prime degree p.*

By the way, the case $m = p$ is as easily handled as if g were a polynomial; and so falls in §2.B considerations.

DEFINITION 2.5. A triple (G, T_1, T_2) is called a group with *double degree representation of degree n* if these conditions holds:

(2.16)(a) T_1 is a faithful doubly transitive representation of the group G of degree n;

(b) T_2 is a faithful primitive (but not doubly transitive) representation of the group G of degree $2 \cdot n$;

(c) there exists $\sigma \in G$ such that $T_1(\sigma)$ is an n-cycle and $T_2(\sigma)$ is a product of two disjoint n-cycles; and

(d) the restriction of T_2 to $G(T_1, 1) = \{\sigma \in G \mid (1)T_1(\sigma) = 1\}$ is an intransitive group.

THEOREM 2.3. *Let p be a prime. Let $(h, g) \in \mathcal{R}(p, 2p)^{NC}$ where $h \in \mathbf{C}[y]$ (as in expression (2.15)), and $\mathcal{S}(h, g)$ is newly reducible, and the cover $\mathbf{P}_z^1 \overset{\varphi(g)}{\to} \mathbf{P}_x^1$ has exactly two points lying over the point ∞ on $\mathbf{P}_x^1$.*

Then $\Omega_{h-x} = \Omega_{g-x}$ and $(G(\Omega_{(h,g)}/\mathbf{C}(x)), T_h, T_g)$ (as in Lemma 2.2) is a group with double degree representation of degree p. If $\boldsymbol{\sigma} = (\sigma(1), \ldots, \sigma(r))$ is a description of the branch cycles of $\mathbf{P}_y^1 \overset{\varphi(h)}{\to} \mathbf{P}_x^1$, and $\sigma(r)$ corresponds to the place over ∞, then

(2.17)(a) $T_h(\sigma(r)) = (n)$ (*i.e., an n-cycle*) and $T_g(\sigma(r)) = (n)(n)$;

(b) $\sum_{i=1}^{r} \operatorname{ind}(T_h(\sigma(i))) = 2(n-1)$; *and*

(c) $\sum_{i=1}^{r} \operatorname{ind}(T_g(\sigma(i))) = 2(2n-1)$.

Conversely, if G is a group with double degree representation of degree p, (G, T_h, T_g), and generators $\boldsymbol{\sigma}$ satisfying expression (2.17), then there exists $(h, g) \in \mathcal{R}(p, 2p)^{NC}$ as above. If such a p exists, then $2p - 1$ is a square, and we have either $p = 5$ or $p > 333$.

OUTLINE OF PROOF (*see* [**Fr**, **5**, *Corollaries* 2 *and* 3]). Most of the proof follows immediately, from Lemmas 2.1 and 2.2. However, in showing that T_h is doubly transitive; and that T_g is primitive, but not doubly transitive there is some work. From [**Fr**, **3**, Lemma 9] either T_h is doubly transitive, or h is a cyclic or Chebychev polynomial. If h is a cyclic polynomial we have $\mathbf{C}(\Omega_{h-x}) = \mathbf{C}(y)$, and if h is a Chebychev polynomial then $[\mathbf{C}(\Omega_{h-x})\colon \mathbf{C}(y)] = 2$. Since g is of degree $2 \cdot p$, and g is not composite with h, each of these cases is ruled out.

The representation T_g cannot be doubly transitive, for if it were, then T_g would be a doubly transitive representation of $G(\Omega_{(h,g)}/\mathbf{C}(x))$ of degree $2 \cdot p$ having an intransitive subgroup, $G(\Omega_{(h,g)}/\mathbf{C}(y))$, of index p. Since p is less than $2 \cdot p$, it is (well) known that this is impossible. Now we show that T_g is a primitive representation.

If T_g is not primitive then there exists a group $\bar{G}$ with $\bar{G}$ properly between $G(\Omega_{(h,g)}/\mathbf{C}(x))$ and $G(\Omega_{(h,g)}/\mathbf{C}(z))$. From the fundamental theorem of Galois theory we conclude that the fixed field of $\bar{G}$ lies properly between $\mathbf{C}(x)$ and $\mathbf{C}(z)$, and $g(z) = g^{(1)}(g^{(2)}(z))$ where $\deg(g^{(i)}) > 1$, $i = 1, 2$. Since $\deg(g) = 2p$, either $\deg(g^{(1)})$ or $\deg(g^{(2)})$ is 2. This is the first crucial place where we use the assumption $\deg(h)$ is a prime. Since $\mathbf{P}_z^1 \overset{\varphi(g)}{\to} \mathbf{P}_x^1$ has 2 places lying over the place $x = \infty$, we easily deduce there are only two possibilities:

(2.18)(a) $g^{(1)}(z)$ is a polynomial of degree p; or

(b) $g^{(2)}(z)$ is a cyclic polynomial (of degree p) and the places 0 and ∞ lie over the place ∞ in the cover $\mathbf{P}^1_z \overset{\varphi(g^{(1)})}{\to} \mathbf{P}^1_x$.

In the case (2.18)(a), $\Omega_{g^{(1)}-x} \subset \Omega_{h-x}$; and since $G(\Omega_{h-x}/\mathbf{C}(y))$ has order relatively prime to p, this group cannot be transitive in the representation $T_{g^{(1)}}$. This contradicts our assumption that $\mathcal{S}(h, g)$ is *newly* reducible, and it is the second place where we use that $\deg(h)$ is a prime. In case (2.18)(b), since $\Omega_{h-x} = \Omega_{g-x}$, the characterization of Chebychev polynomials in [**Fr, 3**, Step 3 of Lemma 9] shows that h is a Chebychev polynomial. We deduce that h and g are a composite pair (as in Definition 2.1).

The fact that $2p-1$ is a square, under the hypotheses of the theorem, is a result of [**Wie, 1**]. The case $p = 5$ is treated in [**Fr, 0,** §5.4]. Finally, in [**Sco**] it is shown that a group with double degree representation p does not exist for $5 < p < 333$.

Problem 2.3. *For what integers n do there exist double degree representations* (*Definition* 2.5) *of degree n*?

From the beginning of this section we have removed from consideration the inspection of $\mathcal{S}(h, g)$ in the case that (h, g) is a *composite pair* of rational functions: there exists $m(y)$, $h^{(2)}(y)$, $g^{(2)}(y) \in \mathbf{C}(y)$ such that $\deg(m(y)) > 1$, $h(y) = m(h^{(2)}(y))$, and $g(y) = m(g^{(2)}(y))$ (as in Definition 2.1). We did this because we were investigating the irreducibility of $\mathcal{S}(h, g)$, and if (h, g) is a composite pair, then $\mathcal{S}(h, g)$ is "trivially" reducible.

However, the archetypal example in this area actually involved the simplest case of composite pairs: the case $h = g$. Therefore we conclude this subsection with an inspection of the irreducible components of $\mathcal{S}(h, h)$, for $h \in \mathbf{C}(y)$. Since $\mathcal{S}(h, h)$ is defined to be the fibered product $\mathbf{P}^1_y \times_{\mathbf{P}^1_x} \mathbf{P}^1_z$ where $\mathbf{P}^1_y \overset{\varphi(h)}{\to} \mathbf{P}^1_x$ and $\mathbf{P}^1_z \overset{\varphi(h)}{\to} \mathbf{P}^1_x$, $\mathcal{S}(h, h)$ contains a "trivial" irreducible component corresponding to the diagonal $\Delta(y, z) \subseteq \mathbf{P}^1_y \times_{\mathbf{P}^1_x} \mathbf{P}^1_z$. An open subset of $\mathcal{S}(h, h)$ is given by $h_1(z) \cdot h_2(y) - h_1(y) \cdot h_2(z) = 0$ where $h(y) = h_1(y)/h_2(y)$ with $h_1, h_2 \in \mathbf{C}[y]$. Then $y - z = 0$ corresponds to the locus of $\Delta(y, z)$. The number of irreducible components of $\mathcal{S}(h, h)$ is identified, via the fundamental theorem of Galois theory, with the orbits of $G(\Omega_{h-x}/\mathbf{C}(x))$ in the representation T_h coming from the right cosets of $G(\Omega_{h-x}/\mathbf{C}(y))$. If $h = h^{(1)}(h^{(2)}(y))$, then we automatically obtain "extra" components of $\mathcal{S}(h, h)$. For many applications we may concentrate on the case that h is an *indecomposable* rational function (Definition 2.2); or equivalently $G(\Omega_{h-x}/\mathbf{C}(x))$ is a primitive group. From Riemann's existence theorem, in a manner analogous to the previous examples of this section, *the search for indecomposable rational functions* $h(y) \in \mathbf{C}(y)$ for which $\mathcal{S}(h, h)$ has 3 or more components is equivalent to the following problem.

Problem 2.4. *Find explicitly the* 4*-tuples* (n, G, T, σ) *for which*

(2.19)(a) *T is a primitive, but not doubly transitive, permutation representation of degree n of the group G*;

(b) $\sigma = (\sigma(1), \ldots, \sigma(r))$ *are generators of G for which* $\sigma(1) \cdots \sigma(r) =$ Id;

(c) $\sum_{i=1}^{r} \operatorname{ind}(T(\sigma(i))) = 2(n-1)$.

In the case that n is a prime, or when the search is for *polynomials* $h(y)$ for which $\mathcal{S}(h, h)$ has 3 or more components, Problem 2.4 is completely solved. We now describe these results, and remark only that beyond these cases we know

very little. The next lemma combines the famous theorems of Burnside **[Bu]** and Schur **[Sch, 2]**.

LEMMA 2.3. *Let* T: $G \to S_n$ *be a primitive, but not doubly transitive, faithful representation of the group* G. *If* n *is a prime* p *then* G *is a proper subgroup of the matrix group*

$$G((\mathbf{Z}/(p))^*, p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a \in (\mathbf{Z}/(p)^*), b \in \mathbf{Z}/(p) \right\}.$$

If n *is not a prime, then* G *cannot contain an* n*-cycle in the representation* T.

THEOREM 2.4. *Let* $h(y) \in \mathbf{C}(y)$ *be such that* $\deg(h) = p$, *a prime, and* $\mathbb{S}(h, h)$ *has at least* 3 *components. Then the monodromy group* $G(\Omega_{h-x}/\mathbf{C}(x))$ *of the cover* $\mathbf{P}^1_y \xrightarrow{\varphi(h)} \mathbf{P}^1_x$ *is one of the following*:

$$\mathbf{Z}/(p); \quad \text{or} \quad G(A, p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a \in A, b \in \mathbf{Z}/(p) \right\}$$

where A *is a subgroup of* $(\mathbf{Z}/(p))^*$ *of order* 2, 3, 4, *or* 6. *Further, a description of the branch cycles of the cover* $\mathbf{P}^1_y \xrightarrow{\varphi(h)} \mathbf{P}^1_x$ *is given by* $\boldsymbol{\sigma} = (\sigma(1), \ldots, \sigma(r))$ *where*

(2.20)(a) $r = 2$, $\sigma(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma(2) = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$; *or*

(b) $r = 3$, $\sigma(i) = \left(\begin{smallmatrix} a(i) & b(i) \\ 0 & 1 \end{smallmatrix}\right)$ *with* $a(i) \in (\mathbf{Z}/(p))^*$ *is of order* 3, $i = 1, 2, 3$; *or*

(c) $r = 3$, $\sigma(i) = \left(\begin{smallmatrix} a(i) & b(i) \\ 0 & 1 \end{smallmatrix}\right)$ *with* $a(1)$ *of order* 2, $a(2)$ *of order* 3, *and* $a(3)$ *of order* 6; *or*

(d) $r = 3$, $\sigma(i) = \left(\begin{smallmatrix} a(i) & b(i) \\ 0 & 1 \end{smallmatrix}\right)$ *with* $a(1)$ *of order* 2, $a(2)$ *and* $a(3)$ *of order* 4; *or*

(e) $r = 3$, $\sigma(i) = \left(\begin{smallmatrix} a(i) & b(i) \\ 0 & 1 \end{smallmatrix}\right)$ *with* $a(1) = a(2) = -1$, $a(3) = 1$; *or*

(f) $r = 4$, $\sigma(i) = \left(\begin{smallmatrix} -1 & b(i) \\ 0 & 1 \end{smallmatrix}\right)$, $i = 1, 2, 3, 4$.

OUTLINE OF PROOF. From Lemma 2.3, since (as noted above) the monodromy group of the cover is a primitive, not doubly transitive group of prime degree, the branch cycles of the cover $\mathbf{P}^1_y \xrightarrow{\varphi(h)} \mathbf{P}^1_x$ are in $G((\mathbf{Z}/(p))^*, p)$. From expression (2.19)(c), $2(p-1) = \sum_{i=1}^{r} \operatorname{ind}(\sigma(i))$. Let the order of $\sigma(i)$ be $e(i)$. If $e(i)$ is equal to p then $\operatorname{ind}(\sigma(i)) = p - 1$. Otherwise the index of $\sigma(i)$ is easily computed to be $((p-1)/e(i)) \cdot (e(i) - 1)$. If none of the $\sigma(i)$ is of order p, then

$$2 = \Sigma_{i=1}^{r}(e(i) - 1)/e(i).$$

Combinatorics show that the possible values of $e(1), \ldots, e(r)$ correspond to the cases (2.20)(b), (c), (d), and (f). If just one of the $\sigma(i)$'s is of order p, we have (2.20)(e).

The list given in expression (2.20) needs some further elaboration: details can be found in **[Fr, 2,** §2]. The classical cyclic and Chebychev polynomials of expression (1.6) correspond to the branch cycles of expression (2.20)(a) and (2.20)(e) respectively.

Our next notation is compatible with that of §0.C. Let L be a discrete (additive) subgroup of $\mathbf{C}$ for which $E = \mathbf{C}/L$ is compact, and let $\mathfrak{p} \in \mathbf{C}/L$ be a point of order p. Let $E_1 = \mathbf{C}/\langle L, \alpha/p \rangle$ where $\alpha \in L$, and α/p represents $\mathfrak{p}$ in $\mathbf{C}/L$. We denote by $\theta(E)$ a *nontrivial* subgroup of the analytic group isomorphisms of E. For "most" E the maximal such group is of order 2, generated by "multiplication by -1" on $\mathbf{C}$. The exceptional cases are E_α (resp., E_β), the elliptic

curve, determined up to isomorphism, with 4 (resp., 6) automorphisms of the analytic group. We can form the quotient of E by $\theta(E)$, denoted $E/\theta(E)$. Then the function field $\mathbf{C}(E/\theta(E))$ is the fixed field of the action of the group $\theta(E)$ on $\mathbf{C}(E)$. We may describe $\mathbf{C}(E/\theta(E))$ quite explicitly. An affine subset of E is represented by the equation (in $\mathbf{C}^2$) $y^2 = x^3 + ax + b$. If $\theta(E)$ is of order 2, then $\mathbf{C}(E/\theta(E)) = \mathbf{C}(x)$: if $\theta(E)$ is of order 4, then $\mathbf{C}(E_\alpha/\theta(E_\alpha)) = \mathbf{C}(x^2)$; if $\theta(E)$ is of order 3, then $\mathbf{C}(E_\beta/\theta(E_\beta)) = \mathbf{C}(y)$; and if $\theta(E)$ is of order 6, then $\mathbf{C}(E_\beta/\theta(E_\beta)) = \mathbf{C}(x^3)$. In all cases $E/\theta(E) \simeq \mathbf{P}^1$, and in all cases we obtain from the natural map $E \overset{\Phi}{\to} E_1$ a commutative diagram

$$\begin{array}{ccc} E & \overset{\Phi}{\to} & E_1 \\ \mathrm{pr}(E)\downarrow & & \downarrow\mathrm{pr}(E_1) \\ E/\theta(E) & \overset{\bar{\varphi}}{\to} & E_1/\theta(E_1) \end{array} \tag{2.21}$$

where $\theta(E)$ and $\theta(E_1)$ are taken to have the same order.

By using the explicit generators listed above for $\mathbf{C}(E/\theta(E))$ as uniformizing variables for copies for $\mathbf{P}^1$, the map $\bar{\varphi}$ is uniquely associated to a rational function $h^{\bar{\varphi}}(y)$. In the literature, as far as we know, these rational functions have never received a name. We hope that our next definition violates no traditions.

DEFINITION 2.6. If a rational function $h(y) \in \mathbf{C}(y)$ corresponds to the map $\bar{\varphi}$ in a commutative diagram represented in expression (2.21), then we call $h(y)$ a *Kummer-Ritt function*. The branch cycles for cover $\mathbf{P}^1_y \overset{\varphi(h(y))}{\to} \mathbf{P}^1_x$ where $h(y)$ is a Kummer-Ritt function are given in (2.20)(b), (c), (d), and (f). Indeed, §0.C is the complete theory of Kummer-Ritt functions whose branch cycles are given by expression (2.20)(f) [**Fr**, **2**, Lemma 2.1].

3. Conclusion of the Schur problem and explicit aspects of Hilbert's theorem. Again, M is a number field, and R its ring of integers. In §1.B we left the Schur problem at the point where we had discovered that if $f \in M(y)$ gives a one-one map on $R/\mathfrak{m} \cup \{\infty\}$ for infinitely many primes $\mathfrak{m}$, then

$$(f_1(y)\cdot f_2(z) - f_1(z)\cdot f_2(y))/(y - z)$$

is a reducible polynomial in the variables y and z where $f = f_1(y)/f_2(y)$. From this point we assume that

(3.1) degree of f is a prime q.

In Theorem 2.4 we have described the branch cycles of the cover $\mathbf{P}^1_y \overset{\varphi(f)}{\to} \mathbf{P}^1_x$ associated to such an f. *We conclude that f must be a Kummer-Ritt function (Definition 2.6) of degree equal to q.* However, how (in the world!) are we to decide for which of these Kummer-Ritt functions we actually obtain pairs (M, f) for which expression (1.5) holds: how do we generalize the Davenport-Fried argument that works for cyclic and Chebychev polynomials? Here is the answer [**Fr**, **2**, Theorem 2.2 for details]! We must find M for which f is defined over M, and $\hat{M}$ (the algebraic closure of M in $M(y_1, \ldots, y_n) = \Omega_{f-x}$) is different from M. In the case that the branch cycles are given by expression (2.20)(b) or 2.20(c) (resp., expression (2.20)(d)) we may take $M = \mathbf{Q}(\sqrt{-3})$ (resp., $M = \mathbf{Q}(\sqrt{-1})$), and the result follows immediately for $q > 3$ from the main theorem of *Complex*

Multiplication ([**ShT**, p. 135] or [**Sw-D**]), since M is generated by the coordinates of q division points on the corresponding elliptic curves. In the case that the branch cycles corresponding to the cover given by f correspond to expression (2.20)(f) then the pair (M, f) may be regarded as corresponding to a point on the modular curve of level q through the analysis of §0.C. These curves are defined over $\mathbf{Q}$ (a result that goes back to [**FriKl**] and that has been generalized in many directions; see [**Fr, 0**, §9], [**ShT**], and [**Sw-D**]). Since by [**Maz**] these curves have very few $\mathbf{Q}$-rational points, for a given $q > 3$ the best result comes from the concept of *arithmetic density* as described in Stage IV of §1.A. That is, let $Y_0(q)$ be the modular curve of level q. Consider the points $\mathfrak{p} \in Y_0(q)$ for which $\mathfrak{p}$ has coordinates in $M_{\mathfrak{p}}$ and $\mathfrak{p}$ corresponds to a rational function $f_{\mathfrak{p}}$ for which the pair $(M_{\mathfrak{p}}, f_{\mathfrak{p}})$ satisfies conditions above. Then we must show that this set of points $\mathfrak{p}$ is infinite. This argument is given in [**Fr, 2,** Lemma 2.2] as an application of the curves used in [**O**] combined with Hilbert's irreducibility theorem.

Of course, there are Kummer-Ritt functions for other integers n (not just when n is a prime). If $f(y) = f_1(f_2(y))$ with $f_1, f_2 \in M(y)$, and if

$$\mathcal{V}_f(R/\mathfrak{m} \dot{\cup} \{\infty\}) = R/\mathfrak{m} \dot{\cup} \{\infty\},$$

then

$$\mathcal{V}_{f_i}(R/\mathfrak{m} \dot{\cup} \{\infty\}) = R/\mathfrak{m} \dot{\cup} \{\infty\}, \qquad i = 1, 2.$$

Therefore, in our search for rational functions f satisfying condition (1.5) we may assume that f is indecomposable over M (i.e., $G(\Omega_{f-x}/M(x))$ is a primitive group acting on $y_1, \ldots, y_n$). *Apparently*, it is possible that $f(y)$ may be indecomposable over M but *decomposable* over $\hat{M}$ (i.e., $G(\Omega_{f-x}/\hat{M}(x))$ is *not* primitive acting on $y_1 \cdots y_n$). The geometric monodromy interpretation of this problem via branch cycles (parallel to the examples of §2): describe the triples $(G, \hat{G}, \boldsymbol{\sigma})$ where

(3.2)(a) G is a normal subgroup of the primitive subgroup $\hat{G}$ of S_n;

(b) G is not primitive (but is transitive);

(c) $\boldsymbol{\sigma} = (\sigma(1), \ldots, \sigma(r)) \in (S_n)^r$ is an r-tuple of elements that generates G and satisfies $\sigma(1) \cdots \sigma(r) = \mathrm{Id}$; and

(d) $\sum_{i=1}^{r} \mathrm{ind}(\sigma(i)) = 2(n-1)$.

Condition (3.2)(d) is the Riemann-Hurwitz formula (expression (0.3)) and it guarantees that there is a rational function f such that the cover $\mathbf{P}^1_y \overset{\varphi(f)}{\to} \mathbf{P}^1_x$ has a description of its branch cycles given by $\boldsymbol{\sigma}$.

Problem 3.1 (*Primitivity problem*). *Describe the triples* $(G, \hat{G}, \boldsymbol{\sigma})$ *satisfying expression* (3.2). *Then for each such triple* $(G, \hat{G}, \boldsymbol{\sigma})$ *answer the question: does there exist a pair* (M, f) *with* $f \in M(y)$, $\boldsymbol{\sigma}$ *a description of the branch cycles of the cover* $\mathbf{P}^1_y \overset{\varphi(f)}{\to} \mathbf{P}^1_x$, *and* $G(\Omega_{f-x}/M(x)) \simeq \hat{G}$?

Problem 3.2 (*Schur problem for rational functions of composite degree*). *Describe the triples* $(G, \hat{G}, \boldsymbol{\sigma})$ *with these properties*: n *is a composite integer*;

(3.3)(a) G *is a primitive but not doubly transitive subgroup of* S_n;

(b) G *is a normal subgroup of* $\hat{G} \subseteq S_n$ *and* $\hat{G}/G$ *is a cyclic group*;

(c) *for* $G(1)$ (*resp.*, $\hat{G}(1)$) *the stabilizer of* 1 *in* G (*resp.*, $\hat{G}$) *the orbits of* $\hat{G}(1)$ *on* $2, \ldots, n$ *break up into strictly smaller orbits under the action of* $G(1)$; *and*

(d) *the r-tuple* $\sigma \in (S_n)^r$ *satisfies conditions* (3.2)(c) *and* (d).

Then for each such triple $(G, \hat{G}, \sigma)$ *answer the question: does there exist a pair* (M, f) *with* $f \in M(y)$, σ *a description of the cycles of the cover* $\mathbf{P}^1_y \overset{\varphi(f)}{\to} \mathbf{P}^1_x$, *and* $G(\Omega_{f-x}/M(x)) \simeq \hat{G}$?

By the way, Problem 3.2 is interesting even with condition (3.3)(d) removed; it leads to the notion of a cover $Y \to \mathbf{P}^1$ having the *Diophantine Covering property* [**Fr, 2**, Proposition 2.1].

Also, it is clear (to use a word that crops up a lot in [**G**]) that one of the good things about the prime degree case, given above, is the absence of *sporadic groups*. In a manner compatible with the opening comments of this introduction, we are anticipating there being, at most, finitely many triples $(G, \hat{G}, \sigma)$ that do *not* fit into a readily recognizable pattern coming (preferably) from some geometric situation. Of course there are already well-known rank 3 primitive, but not doubly transitive, groups that must be regarded as sporadic. Indeed, [**G**, p. 93], some of these figured in the production of sporadic simple groups. These most certainly do not figure in Problem 3.2. In addition, the *automorphism groups of Grassmann varieties over finite fields have not yet been inspected for their effect on Problem* 3.2.

Finally we conclude with specific aspects of Hilbert's irreduciblity theorem applied to the case where $f(x, y) = h(y) - x$ with $h(y) \in \mathbf{Q}[y]$ *indecomposable* (i.e., h cannot be written as a functional composition of two other polynomials, both of degree greater than 1)). From expression (1.10) we easily conclude that

$$\mathcal{R}_{h-x}(\mathbf{Z}) = \mathcal{V}_h(\mathbf{Z}) \cup \left(\bigcup_{i=1}^{t} \mathcal{V}_{g_i}(\mathbf{Z}) \right) \cup \overline{V} \tag{3.4}$$

where $g_1, \ldots, g_t$ are *indecomposable rational* functions satisfying expression (1.9)(b), and $\overline{V}$ is a finite set.

We conclude that g_i in expression (3.4) cannot satisfy (1.9)(a) in consequence of the hypothesis $M = \mathbf{Q}$ ([**Fr, 6**] or the first corollary to the main theorem of [**Fr, 0**, §9.1]).

In particular $\mathcal{R}_{h-x}(\mathbf{Z}) - \mathcal{V}_h(\mathbf{Z}) \overset{\text{def}}{=} \mathcal{S}_h(\mathbf{Z})$ *is of logarithmic density*. By the way, $\mathcal{S}_h(\mathbf{Z})$ may have exponential density if h is not indecomposable: take $h(y) = y^4 + y^2$ and use the factorization of expression (2.10). In addition we could consider $\mathcal{S}_h(R)$ for R the ring of integers of a general number field M. In this case $\mathcal{S}_h(R)$ may have exponential density even *if* h is indecomposable: take h of degree 7, 11, 13, 15, 21 or 31 for which we know that there are cases of reducibility of $h(y) - g(z)$ as in Theorem 2.2 (e.g., [**Fr, 0**, §5.3] or Birch's brute force calculation in expression (2.11)).

The problem of major concern: *if* h *is indecomposable, is* $\mathcal{S}_h(\mathbf{Z})$ *finite*? Theorem 2.3 applies immediately, and we conclude that $\mathcal{S}_h(\mathbf{Z})$ is finite if the degree of h is a prime p for which either $2p - 1$ is *not* a square or $5 < p < 333$. We do have one case where $\mathcal{S}_h(\mathbf{Z})$ is *not* finite: h is of degree 5. Other than this we know of no other indecomposable polynomials h for which $\mathcal{S}_h(\mathbf{Z})$ is infinite. *In order to go further we must know if there exist other examples of double degree representations as in Problem* 2.3.

Actually, if the classification of simple groups does go through as expected at the Santa Cruz Conference, then there will be a complete classification of groups with a doubly transitive representation containing an n-cycle (as told to me by Feit and Kantor). With this the last problem will be completely resolved. Again, this is fitting tribute to the role of the classification of simple groups in regard to applications. More details on this will appear in **[Fr, 0]**. See also **[F, 3**, see Theorem 1.1] and **[Wie, 2]**.

REFERENCES

[Ah] L. Ahlfors, *Complex analysis*, McGraw-Hill, New York, 1966.

[Ar, E, 1] E. Artin, *Theorie der Zöpfe*, Abh. Math. Sem. Hamburg **4** (1925), 47–72.

[Ar,E, 2] _____, *Theory of braids*, Ann. of Math. (2) **48** (1947), 101–126.

[Bo] P. Bohnenbeust, *The algebraical braid group*, Ann. of Math. (2) **48** (1947), 127–136.

[Bom] E. Bombieri, *Counting points on curves over finite fields*, Sem. Bourbaki **25** (1972/73), No. 430.

[Bu] W. Burnside, *On simply transitive groups of prime degree*, Quart. J. Math. **37** (1906), 215–222.

[Ca, 1] J. W. S. Cassels, *Factorization of polynomials in several variables*, Proc. 15th Scandinavian Congress, Oslo, 1968, Lecture Notes in Math., no. 118, Springer-Verlag, Berlin and New York, 1970, pp. 1–17.

[Ca, 2] _____, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[CaFro] J. W. S. Cassels and A. Frohlich, *Algebraic number theory*, Thompson, Washington, D. C., 1967.

[Ce] N. Čebotarev, *Bestimmung der dichtigkeiteiner menge von primzahlen, welche zu einer gegeben substitutionsklasse gehören*, Math. Ann. **95** (1926), 191–228.

[Co] S. D. Cohen, *Value sets of functions over finite fields*, Acta Arith. (to appear).

[DSc] H. Davenport and A. Schinzel, *Two problems concerning polynomials*, J. Reine Angew. Math. **214** (1964), 386–391.

[DLSc, 1] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. Oxford Ser. 2 **12** (1961), 304–312.

[DLSc, 2] _____, *Polynomials of certain special types*, Acta Arith. **9** (1964), 107–116.

[E] L. Ehrenfucht, *Kryterium absolutnez hierokladnosci wieminow*, Prace Mat. **2** (1958), 167–169.

[F, 1] W. Feit, *Automorphisms of symmetric balanced incomplete block design*, Math. Z. **118** (1970), 40–49.

[F, 2] _____, *On symmetric balanced incomplete block design with doubly transitive automorphism groups*, J. Combinatorial Theory **14** (1973), 221–247.

[F, 3] _____, *Some consequences of the classification of finite simple groups*, these PROCEEDINGS, pp. 175–181.

[Frey] G. Frey, *Rational isogonies of prime degree and nonstandard arithmetic* (preprint).

[Fr, 0] M. Fried, *Applications of Riemann's Existence Theorem to algebraic and arithmetic geometry* (in preparation).

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

[Fr, 2] _____, *Galois groups and complex multiplication*, Trans. Amer. Math. Soc. **237** (1978), 141–162.

[Fr, 3] _____, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.

[Fr, 4] _____, *On a theorem of MacCluer*, Acta Arith. **25** (1974), 122–127.

[Fr, 5] _____, *On Hilbert's irreducibility theorem*, J. Number Theory **100** (1974), 211–232.

[Fr, 6] _____, *The field of definition of function fields and a problem in the reducibility of polynomials*, Illinois J. Math. **17** (1973), 128–146.

[Fr, 7] _____, *On the diophantine equation $f(y) - x = 0$*, Acta Arith. **19** (1971), 79–87.

[Fr, 8] _____, *On a theorem of Ritt*, J. Reine Angew. Math. **224** (1974), 40–55.

[Fr, 9] _____ (with R. Biggers), *Relations between moduli spaces of covers of $\mathbf{P}^1$ and representations of the Hurwitz monodromy group* (preprint).

[FrS] M. Fried and G. Sacerdote, *Solving Diophantine problems over: all residue class fields of a number field, and all finite fields*, Ann. of Math. (2) **104** (1976), 203–233.

[FrSc] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. **21** (1972), 153–171.

[FrSm] M. Fried and J. A. Smith, *Primitive groups, Moore graphs and rational curves*, Michigan Math. J. **19** (1972), 341–346.

[G] D. Gorenstein, *The classification of finite simple groups*. I, *Simple groups and local analysis*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 43–199.

[H] M. Hall, Jr., *The theory of groups*, MacMillan, New York, 1963.

[Hi] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Functionen mit ganz zahligen Koeffizienten*, J. Reine. Angew. Math. **110** (1892), 104–129.

[Kan] W. Kantor, 2-*transitive designs*, Part 3: *Combinatorial group theory*, Proc. Advanced Study on Combinatorics at Nijenrode Castle, Breukelen, Netherlands, July 8–20, 1974, Mathematisch Centrum, Amsterdam, 1974, pp. 44–98.

[FriKl] F. Klein and R. Fricke, *Vorlesungen über die theorie der modulfunctionen* II, Leipzig, 1892.

[Lev] W. LeVeque, *On the equation* $y^m = f(x)$, Acta Arith **9** (1964), 209–219.

[Mc] C. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials*, Acta Arith. **12** (1967), 289–299.

[Maz] B. Mazur, *Rational points on modular curves*, Modular Functions of One Variable *V*, (Bonn, 1976), Lecture Notes in Math., vol. 601, Springer-Verlag, Berlin and New York, 1977, pp. 107–148.

[Ni] J. Nielsen, *Untersuchungen zur Topologie der geschlossenen Zweiseitigen Flächen*. I-III, Acta Math. **50** (1927), 189–358; **53** (1927), 1–76; **58** (1931), 87–167.

[O] A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111.

[Sc, 1] A. Schinzel, *Reducibility of polynomials of the form* $f(x) - g(y)$, Colloq. Math. **18** (1967), 213–218.

[Sc, 2] _____, *Some unsolved problems*, Mat. Bibl. **25** (1963), 63–70.

[Sc, 3] _____, *Reducibility of polynomials*, Actes Internat. Congr. Math. 1970, Vol. 1, pp. 491–496, Gauthier-Villars, Paris, 1971.

[Sch, 1] I. Schur, *Über den zussamenhang zwischen einem problem der zahlentheorie und linear satz über algebraische Functionen*. S.-B. Preuss. Akad. Wiss. Phys.–Math. Kl. (1923), 123–134.

[Sch, 2] _____, *Zur Theorie der einfach transitiven Permutations Gruppen*, S.-B. Preuss. Akad. Wiss. Phys.–Math. Kl. (1933), 598–623.

[Sco] L. Scott, *Uniprimitive permutation group*, Theory of Finite Groups, a symposium at Harvard University, Benjamin, New York, 1972, pp. 55–62.

[ShT] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties*, Math. Soc. Japan, 1961.

[S] C. L. Siegel, *Über eininge anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys–Math. Kl. **1** (1929), 14–67.

[Sw-D] H. P. F. Swinnerton-Dyer, *Applications of algebraic geometry to number theory*, Stony Brook Sympos. Number Theory, Summer 1969, Amer. Math. Soc., Providence, R. I., 1971, pp. 1–52.

[Tv] H. Tverberg, *A study in the irreducibility of polynomials*, Dept of Math., Univ. of Bergen, 1968.

[Wa] Wagner, *On collineation groups of projective spaces*. I, Math. Z. **76** (1961), 411–462.

[W] A. Weil, *Sur les courbes et les variétés qui s'endeduisent*, Hermann, Paris, 1948.

[Wie, 1] H. Wielandt, *Primitive permutation gruppen Grad* $2p$. II, Math. Z. **63** (1956).

[Wie, 2] _____, *Permutation groups through invariant relations and invariant functions*, Lectures given at the Ohio State University, Columbus, Ohio, February 25–April 3, 1969.

UNIVERSITY OF CALIFORNIA, IRVINE