TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 235, January 1978

GALOIS GROUPS AND COMPLEX MULTIPLICATION[1]

BY

MICHAEL FRIED

ABSTRACT. The Schur problem for rational functions is linked to the theory of complex multiplication and thereby solved. These considerations are viewed as a special case of a general problem, prosaically labeled the *extension of constants problem*. The relation between this paper and a letter of J. Herbrand to E. Noether (published posthumously) is speculatively summarized in a conjecture that may be regarded as an arithmetic version of Riemann's existence theorem.

0. **Introduction.** Let F be a perfect field, and $\bar{F}$ a fixed algebraic closure of F. We consider the finite Galois extensions of F that come from certain types of geometric situations. Let $W \xrightarrow{\varphi(V,W)} V$ be a cover (finite, flat morphism) of quasi-projective varieties such that W, V, and $\varphi(V, W)$ are defined over F, and W and V are absolutely irreducible. For X, a variety defined over F, we let $F(X)$ be the field of rational functions on X defined over F. Therefore, we have a field extension $F(W)$ over $F(V)$ (by abuse, $F(W)/F(V)$). If $\varphi(V, W)$ is a separable morphism, then $F(W)/F(V)$ is a finite separable extension, and we obtain

$$(0.1) \qquad 1 \to G(\widehat{F(W)}/\hat{F}(V)) \to G(\widehat{F(W)}/F(V)) \xrightarrow{\text{rest}} G(\hat{F}/F) \to 1$$

where: $\widehat{F(W)}$ is the smallest Galois extension of $F(V)$ containing $F(W)$ (the *Galois closure* of $F(W)/F(V)$); $\hat{F} = \hat{F}(W, F)$ is the algebraic closure of F in $\widehat{F(W)}$, and; rest denotes the restriction of elements of the Galois group $G(\widehat{F(W)}/F(V))$ to $\hat{F}$. We call $\hat{F}$ the *extension of constants* obtained from W/V.

The problem of the description of $G(\hat{F}/F)$ arises in several well-known problems. For example. let G be a finite group which we desire to realize as the Galois group of some Galois extension of the rational field $\mathbf{Q}$. Suppose that: $F = \mathbf{Q}$; V is a Zariski open subset of $\mathbf{P}^n$ (projective n-space); and $G(\widehat{\bar{\mathbf{Q}}(W)}/\bar{\mathbf{Q}}(V))$, the (geometric) monodromy group is equal to G (a fact that may have come to us from analytic considerations, say in the manner of [Fr, 1]). In this case the limitation theorems of [Fr, 1, §2] sometimes serve to show

Received by the editors February 23, 1976.

AMS (MOS) subject classifications (1970). Primary 10B15, 10D25, 12A55, 14D20, 14G05, 14H05, 14H10; Secondary 10M05, 14D05, 14H25, 14H30, 14K22.

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

that $\hat{\mathbf{Q}} = \mathbf{Q}$. If so we may apply Bertini's theorem and Hilbert's irreducibility theorem to show that G is realized as a Galois group over $\mathbf{Q}$.

There are many diophantine (sic!) problems where our psychological motivation is *not* to have $\hat{F}$ turn out to be F, but rather to have $G(\hat{F}/F)$ be as large as possible. The Schur problem and the theory of complex multiplication are two examples of such problems. In §2 we complete the solution of the Schur problem for rational functions (of prime degree) by noting the precise connections between these two problems (and the theory of division points of elliptic curves).

We review quickly the contents of this paper section by section.

After preliminary notation and definitions in §1, §1.A discusses Riemann's existence theorem and the description of covers of $\mathbf{P}^1$ through the use of branch cycles. We have added to the classical interpretation of branch cycles some important comments on the explicit (algebraic) computation of a description of the branch cycles of a cover. In §1.B we consider the exact conditions under which the points of a cover of $\mathbf{P}^1$ lying over branch points provide rigidifying data (i.e., the identity is the only automorphism of the cover leaving invariant each of these points).

In §2.A, after we explain carefully the original Schur problem, we consider the general Schur problem which specializes to the Schur problem for rational functions. The important results here are the translation between arithmetic (diophantine) conditions and geometric conditions concerning the arithmetic monodromy group of a cover. In §2.B, we show that, using the theory of elliptic curves, it is possible to solve the problem posed by the conditions on the arithmetic monodromy group of a cover that arises in the consideration of the Schur problem for rational functions of prime degree.

Riemann's existence theorem says that the geometric monodromy group of a cover of $\mathbf{P}^1$ is determined by branch cycle data. In §3 we consider all triples (Y, φ, F) consisting of a cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ defined over a field F such that the cover has a given (a priori) description of its branch cycles. Using previous notation, the *arithmetic monodromy group* of the cover is $G(\widehat{F(Y)}/F(\mathbf{P}^1))$. A conjecture is described that supports a precise version of the statement: the arithmetic monodromy group of the cover is determined by *branch cycle data and the residue class fields of points lying over the branch points of the cover.* Here we use the rigidifying data of §1.B to consider certain appropriate families of covers of $\mathbf{P}^1$ related to (but not the same as) Hurwitz families. The section also relates the extent to which the results of §2 are support for this conjecture.

We would like to thank Armand Brumer for his suggestions on the exposition of portions of this paper and the related results of [Fr, 1, §2]. Also, it is fairly clear that Herbrand considered problems similar to those discussed

in this paper. Since his letter to E. Noether consists of a sketchy list of private discoveries it is difficult to make a precise comparison with [He]. However, we make an attempt at the end of §1 to give a technical interpretation of his remarks. It was Marvin Tretkoff who suggested the relevance of Herbrand's letter when we first tried to expose various arithmetic versions of Riemann's existence theorem during a stay at the Institute for Advanced Study.

1. Preliminaries on covers and Riemann's existence theorem. Let $W \xrightarrow{\varphi(V,W)} V$ be a cover of absolutely irreducible, normal, quasi-projective varieties such that W, V, $\varphi(V, W)$ are defined over a perfect field F. All function fields are assumed to be embedded in a fixed algebraically closed field containing F. We retain the notations of the introduction and we assume that $\varphi(V, W)$ is a separable morphism of degree n. Let $\widehat{F(W)}$ be the Galois closure of the field extension $F(W)/F(V)$.

There is a variety over F, $\hat{W}$, such that we have a cover $\hat{W} \to W \to V$ and $F(\hat{W}) = \widehat{F(W)}$ [Mum, pp. 396–397]. Also: $\hat{W}$ is called the *normalization* of W in $\widehat{F(W)}$; $\hat{W}$ is absolutely irreducible if and only if $\hat{F} = F$ where F is the algebraic closure of F in $\widehat{F(W)}$ and, the automorphisms of $\hat{W}$ as a cover of V which are defined over F (denoted $\mathrm{Aut}(\hat{W}/V, F)$) are in one-one correspondence with the elements of $G(\widehat{F(W)}/F(V))$.

Let S_n be the symmetric group on n letters. Our notation throughout this paper is: elements of S_n act on the right of the integers $1, 2, \ldots, n$; elements of $\mathrm{Aut}(W/V, F)$ (for any cover $W \to V$ defined over F) act on the left of points of W; elements of $G(\widehat{F(W)}/F(V))$ act on the right of elements of $\widehat{F(W)}$, and, the identification between the groups $G(\widehat{F(W)}/F(V))$ and $\mathrm{Aut}(\hat{W}/V, F)$ is denoted by $f^{\sigma}(\mathfrak{p}) = f(\sigma^{-1}(\mathfrak{p}))$ for $\mathfrak{p} \in \hat{W}$, $f \in F(\hat{W})$, and $\sigma \in \mathrm{Aut}(\hat{W}/V, F)$.

The group $G(\widehat{F(W)}/F(V))$ has a natural permutation representation: $T(W/V)$: $G(\widehat{F(W)}/F(V)) \to S_n$ (faithful and transitive) given by the action on the right cosets of $G(\widehat{F(W)}/F(W))$. For H, a subgroup of a group H', we let $N_{H'}(H)$ be the normalizer of H in H'.

LEMMA 1.1. *The group $G(\widehat{F(W)}/\hat{F}(V))$ is canonically identified with $G(\bar{F}(W)/\bar{F}(V))$ (the geometric monodromy group of W/V). Also, $G(\hat{F}/F)$ is identified with a subgroup of the quotient $N_{S_n}(G(\widehat{F(W)}/\hat{F}(V)))/G(\widehat{F(W)}/\hat{F}(V))$ where $G(\widehat{F(W)}/\hat{F}(V))$ is identified with its image under $T(W/V)$.*

PROOF. The first part is well known, and the second part follows from the definitions applied to the expression (0.1). □

REMARK 1.1. There can be certain notational problems in identifying $\mathrm{Aut}(\hat{W}/V, F)$ and $G(\widehat{F(W)}/F(V))$, especially when we give these groups the structure of permutations groups. For example, the group of automorphisms of W as a cover of V (defined over F; $\mathrm{Aut}(W/V, F)$) is canonically identified with $\mathrm{Cen}_{S_n}(G(\widehat{F(W)}/F(V)))$ (the centralizer in S_n of the image of $G(\widehat{F(W)}/F(V))$ under $T(W/V)$). However, the group of automorphisms of $F(W)/F(V)$ is canonically identified with the quotient group:

$$N_{G(\widehat{F(W)}/F(V))}\big(G(\widehat{F(W)}/F(W))\big)/G(\widehat{F(W)}/F(W)).$$

Of course, these two groups are isomorphic; the isomorphism is just a simple fact of group theory [Fr, 1, §2]. □

1.A. *Branch cycles.* We assume that K is an arbitrary field of zero characteristic. Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a cover of irreducible nonsingular projective curves defined over $\bar{K}$ (a fixed algebraic closure of K). Let $u(1), \dots, u(r) \in \mathbf{P}^1$ be the places of $\mathbf{P}^1$ ramified in the cover. We let $\zeta_n = e^{2\pi i/n}$ to obtain a compatible system of roots of 1: $(\zeta_{nm})^m = \zeta_n$ for n and $m \geqslant 1$. Refer to the notation in the introduction. We let $e(j)$ be the order of the inertial group of a place of $\bar{K}(Y)$ lying over the place $u(j)$ of $\bar{K}(\mathbf{P}^1) = \bar{K}(x)$. The formal power series field $\bar{K}(((x - u(j))^{1/e(j)}))$ (with $(x - u(j))^{1/e(j)}$ replaced by $(1/x)^{1/e(j)}$ if $u(j) = \infty$) has a canonical automorphism, denoted $\overline{\sigma(j)}$, induced from the substitution

$$(x - u(j))^{1/e(j)} \to \zeta_{e(j)}(x - u(j))^{1/e(j)}.$$

For each j we obtain an embedding (by Puiseux expansions):

$$\widehat{\varphi(j)}: \widehat{\bar{K}(Y)} \to \bar{K}\Big(\big((x - u(j))^{1/e(j)}\big)\Big), \qquad j = 1, \dots, r. \tag{1.1}$$

This embedding is determined up to composition with an automorphism of $\widehat{\bar{K}(Y)}$, and therefore, the restriction of $\sigma(j)$ determines an element $\overline{\sigma(j)}$ of $G(\widehat{\bar{K}(Y)}/\bar{K}(\mathbf{P}^1))$ up to conjugation. *We note that it is possible to determine the conjugacy class of $\sigma(j)$ in a constructive way from knowledge of the polynomials used to define Y and the graph of φ as projective varieties.*

Riemann's existence theorem. *For some choice of the embeddings $\widehat{\varphi(j)}$, $j = 1, \dots, r$, the collection $\sigma(1), \dots, \sigma(r)$ satisfies:*

$$\text{(1.2)}\quad \begin{aligned} &\text{(a)}\ \ \sigma(1), \dots, \sigma(r) \textit{ generate } G\big(\widehat{\bar{K}(Y)}/\bar{K}(\mathbf{P}^1)\big), \textit{ and,} \\ &\text{(b)}\ \ \sigma(1) \cdots \sigma(r) = \mathrm{Id}. \end{aligned}$$

We call such a collection $\sigma(1), \dots, \sigma(r)$ (obtained from embeddings $\widehat{\varphi(j)}$, $j = 1, \dots, r$) satisfying (1.2)(a) *and* (b), *a description of the branch cycles of the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$. The group generated by $\sigma(1), \dots, \sigma(r)$ is called the monodromy group of the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$.*

Conversely, suppose we are given: $\sigma(1), \dots, \sigma(r) \in S_n$ *(the symmetric group on n letters) satisfying* (1.2)(b) *and generating a transitive subgroup of S_n, and, $u(1), \dots, u(r) \in \bar{K}$. Then there exists*

(1.3) $Y\xrightarrow{\varphi}\mathbf{P}^1$, *with* Y *and* φ *defined over* $\bar{K}$, $\deg(\varphi) = n$, *such that* $\sigma(1), \ldots, \sigma(r)$ *are obtained from* (1.3) *as in the process above.*

REMARK 1.2 (RIEMANN-HURWITZ FORMULA). We call the collection $\sigma(1), \ldots, \sigma(r)$ a description of the branch cycles for the cover $Y\xrightarrow{\varphi}\mathbf{P}^1$. If $\deg(\varphi) = n$, we have an embedding $G(\widehat{\bar{K}(Y)}/\bar{K}(x)) \hookrightarrow S_n$. For $\sigma \in S_n$, we can write $\sigma = \beta_1 \cdots \beta_t$ where $\beta_1, \ldots, \beta_t$ are disjoint cycles. If the order of β_i is $s(i)$, we abuse terminology and write $\sigma = (s(1)) \cdots (s(t))$, and $\operatorname{ind}(\sigma) = \Sigma_{i=1}^{t}(s(i) - 1)$. The Riemann-Hurwitz formula says that the genus of the curve Y, $g(Y)$, is determined from the formula [Sp, p. 268]

$$2(n + g(Y) - 1) = \sum_{i=1}^{r} \operatorname{ind}(\sigma(i)). \quad \square \tag{1.4}$$

REMARK 1.3 (ANALYSIS VERSUS ALGEBRA). There are many collections $\sigma(1), \ldots, \sigma(r)$ of elements of $G(\widehat{\bar{K}(Y)}/\bar{K}(x))$ that can arise as a description of the branch cycles for $Y\xrightarrow{\varphi}\mathbf{P}^1$, by varying the choice of the embeddings $\widehat{\varphi(j)}$, $j = 1, \ldots, r$. The fact that at least one collection exists satisfying the conditions (1.2)(a) and (b) is a consequence of the explicit description of the fundamental group of $\mathbf{P}^1 - \{u(1), \ldots, u(r)\}$ using paths (that is, using topology). In fact, the collections $\sigma(1), \ldots, \sigma(r)$ which arise this way (by abuse, an *analytic description of the branch cycles of the cover* $Y\xrightarrow{\varphi}\mathbf{P}^1$; as in [Fr, 1, §3]) may be a proper subset of the collections satisfying (1.2)(a) and (b). This is indeed the case if and only if a certain combinatorial quantity called the *Hurwitz Number* of $\sigma(1), \ldots, \sigma(r)$ is not equal to 1 [Fr, 1, §3].

Grothendieck [Gr] has shown that $\sigma(1), \ldots, \sigma(r)$ exist satisfying (1.2)(a) and (b) in the case that K is replaced by any field when $Y\xrightarrow{\varphi}\mathbf{P}^1$ is a *tamely ramified cover. However, as yet, there exists no purely algebraic proof of the existence of* $\sigma(1), \ldots, \sigma(r)$ *satisfying* (1.2)(a) *and* (b), *although this existence may be checked by a purely algebraic computation.*

When K is replaced by a field F of positive characteristic the converse part (condition (1.3)) is false, in general, unless the order of $G(\bar{F}(Y)/\bar{F}(\mathbf{P}^1))$ is relatively prime to the characteristic of F [Gr]. Even in the characteristic zero case *there is no purely algebraic proof of* (1.3). $\square$

1.B. *Rigidifying data.* In this subsection all computations take place over an algebraically closed field $\bar{K}$ of characteristic zero. Let $Y\xrightarrow{\varphi}\mathbf{P}^1$ be a connected cover of $\mathbf{P}^1$ and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ be a collection of distinct points on Y. We say that the points $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ provide *rigidifying data* for the cover $Y\xrightarrow{\varphi}\mathbf{P}^1$ if the identity is the only automorphism α: $Y \to Y$ for which

(1.4) (a) α: $Y \to Y$ is commutative, and

$$\begin{tikzcd} Y \arrow[rr] \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\varphi"] \\ & \mathbf{P}^1 & \end{tikzcd}$$

(1.4) (b) α leaves each of the points $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ fixed.

Let $Y' \xrightarrow{\varphi'} \mathbf{P}^1$ have rigidifying data $\mathfrak{p}'_1, \dots, \mathfrak{p}'_m$. We say that $\{Y, \varphi; \mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ and $\{Y', \varphi'; \mathfrak{p}'_1, \dots, \mathfrak{p}'_m\}$ are isomorphic if there exists an analytic isomorphism β: $Y \to Y'$ such that

(1.5) (a) β:
$$\begin{tikzcd} Y \arrow[rr] \arrow[dr, "\varphi"'] & & Y' \arrow[dl, "\varphi'"] \\ & \mathbf{P}^1 & \end{tikzcd}$$
is commutative, and

(1.5) (b) $\beta(\mathfrak{p}_i) = \mathfrak{p}'_i, \quad i = 1, \dots, m.$

Since $\mathfrak{p}'_1, \dots, \mathfrak{p}'_m$ is rigidifying data for $Y' \xrightarrow{\varphi'} \mathbf{P}^1$, if β *exists, it is unique.*

Let $u(1), \dots, u(r) \in \mathbf{P}^1$ be the branch points of the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ and let $\mathfrak{p}(i,j), j = 1, \dots, n(i)$ be the points of Y lying over $u(i)$. Thus,

$$\sum_{j=1}^{n(i)} e(\mathfrak{p}(i,j)/u(i)) = \deg(\varphi) = n$$

where $e(\mathfrak{p}(i,j)/u(i))$ is the ramification index of the place $\mathfrak{p}(i,j)$ over the place $u(i)$. Since $u(i)$ is a branch point, $e(\mathfrak{p}(i,j)/u(i)) > 1$ for at least one value of j. In the remainder of this subsection we find necessary and sufficient conditions that the collection of points $P(Y, \varphi) = \{\mathfrak{p}(i,j);\, j = 1, \dots, n(i),$ $i = 1, \dots, r\}$ is rigidifying data for the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$.

We return to the notation of §1.A. Let $\widehat{\varphi(j)}$: $\widehat{\bar{K}(Y)} \to \bar{K}(((x - u(j))^{1/e(j)}))$, $j = 1, \dots, r$ be embeddings of $\widehat{\bar{K}(Y)}$ into Laurent series expansions in terms of $(x - u(j))^{1/e(j)}$. We assume that the embeddings are chosen so that the restriction of the substitution automorphism

$$(x - u(j))^{1/e(j)} \to \zeta_{e(j)} \cdot (x - u(j))^{1/e(j)}$$

induces $\sigma(j)$ on the image of $\widehat{\bar{K}(Y)}$ where $\sigma(1), \dots, \sigma(r)$ is a description of the branch cycles of the cover. Each disjoint cycle of $\sigma(i)$ corresponds to one of the places $\mathfrak{p}$ of '$\bar{K}(Y)$ lying over the place $u(i)$ of $\bar{K}(x)$. Let $\beta(\mathfrak{p})$ be the cycle in $\sigma(i)$ corresponding to $\mathfrak{p}$.

Let y be a primitive generator for $\bar{K}(Y)/\bar{K}(x)$, and let $y = y^{(1)}, \dots, y^{(n)}$ be the conjugates of y over $\bar{K}(x)$. Thus each $y^{(j)}$ corresponds to an explicit embedding $\psi(j)$: $\bar{K}(Y) \to \widehat{\bar{K}(Y)}$. The image of $\bar{K}(Y)$ under $\psi(j)$ is $\bar{K}(x, y^{(j)})$, and the action of $\sigma(j)$ on $\widehat{\bar{K}(Y)}$ is given by a permutation $y^{(1)}, \dots, y^{(n)}$. For notational simplicity, suppose that the cycle $\beta(\mathfrak{p})$ is $(1\ 2 \cdots t)$ (i.e. corresponds to the permutation

$$y^{(1)} \to y^{(2)} \to \cdots \to y^{(t)} \to y^{(1)}).$$

As in the discussion preceding Lemma 1.1, an automorphism α of $Y \xrightarrow{\varphi} \mathbf{P}^1$

may be naturally regarded as an element of S_n that centralizes the group generated by $\sigma(1), \ldots, \sigma(r)$. Also, α induces an automorphism α^* of $\bar{K}(Y)/\bar{K}(x)$. Consider $\psi(j)^{-1} \circ \alpha^* \circ \psi(j)$ as acting on (the right of) the image of $\bar{K}(Y)$ under $\psi(j)$. Let j be an integer between 1 and t. *Let α be an automorphism that leaves $\mathfrak{p}$ fixed.* Then

(1.6) $\psi(j)^{-1} \circ \alpha^* \circ \psi(j)$ acting on $\bar{K}(x, y^{(j)})$ is induced by some power of the cycle $\beta(\mathfrak{p})$ (i.e. is given by the substitution in Puiseux expansions).

Let $\bar{\beta}(1), \ldots, \bar{\beta}(s)$ be exactly the disjoint cycles of α which contain at least one of the integers $1, 2, \ldots, t$. Since, from (1.6) each of these is some power of $\beta(\mathfrak{p})$, *only* the integers $1, 2, \ldots, t$ appear in the cycles $\bar{\beta}(1), \ldots, \bar{\beta}(s)$. Since $\alpha^{-1} \cdot \sigma(i) \cdot \alpha = \sigma(i)$, it is easy to deduce that $\bar{\beta}(1) \cdots \bar{\beta}(s)$ is a power of $\beta(\mathfrak{p})$.

Definition 1.1. Given a cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ we denote by $\mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$ the subgroup of $\mathrm{Aut}(Y/\mathbf{P}^1)$ consisting of elements α such that each point of the set $P(Y, \varphi)$ is left fixed by α. We let Y^{Rig} be the nonsingular projective curve that fits in the diagram

(1.7) $Y \xrightarrow{\varphi_1} Y^{\mathrm{Rig}} \xrightarrow{\varphi_2} \mathbf{P}^1$ where φ_1 is a Galois cover of nonsingular curves with Galois group naturally isomorphic to $\mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$.

Proposition. *The group* $\mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$ *is cyclic and consists of the elements α of* $\mathrm{Aut}(Y/\mathbf{P}^1)$ *such that: α commutes with each disjoint cycle of $\sigma(i)$, $i = 1, \ldots, r$, and if α is of order t then t divides the order of each disjoint cycle of $\sigma(i)$, $i = 1, \ldots, r$.*

In addition, $Y \xrightarrow{\varphi_1} Y^{\mathrm{Rig}}$ is a cover with cyclic Galois group such that, if $\deg \varphi_1 > 1$, *every point $\mathfrak{p} \in P(Y, \varphi)$ is totally ramified over $\varphi_1(\mathfrak{p}) \in Y^{\mathrm{Rig}}$.*

Proof. Let $\alpha \in \mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$ and let α^* be the associated automorphism of $\bar{K}(Y)/\bar{K}(x)$. The following facts follow from the discussion above: α, regarded as an element of S_n centralizes every disjoint cycle of $\sigma(i)$, $i = 1, \ldots, r$; if α is of order t, then t divides the order of each disjoint cycle of $\sigma(i)$, $i = 1, \ldots, r$, and; if we denote the fixed field of α^* in $\bar{K}(Y)$ by L^α, then the place of $\bar{K}(Y)$ corresponding to $\mathfrak{p} \in P(Y, \varphi)$ is totally ramified over its restriction to L^α, for each $\mathfrak{p} \in P(Y, \varphi)$.

Let $\mathfrak{p} \in P(Y, \varphi)$ and let L be a field between $\bar{K}(Y)$ and $\bar{K}(x)$ such that

(1.8) the place corresponding to $\mathfrak{p}$ is totally ramified over its restriction to L.

Then L, with property (1.8) is determined by the integer $[\bar{K}(Y): L]$, by use of Puiseux expansions. For α and $\beta \in \mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$ we deduce that $[\bar{K}(Y):$

$L^\alpha \cap L^\beta$] is the least common multiple of the orders of α and β, and $\bar{K}(Y)/L^\alpha \cap L^\beta$ is a cyclic extension. From this we easily deduce that $\mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$ is a cyclic group.

The only assertion that remains unproved is that if $\alpha \in \mathrm{Aut}(Y/\mathbf{P}^1)$, the order of α divides the order of each disjoint cycle of $\sigma(i)$ and α commutes with each disjoint cycle of $\sigma(i)$ for $i = 1, \ldots, r$, then $\alpha \in \mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}}$. That is, we must show that α fixes the points in $P(Y, \varphi)$. However, this is immediate from (1.6) since this is equivalent to the statement that $\psi(j)^{-1} \circ \alpha^* \circ \psi(j)$ maps $y^{(j)}$ to a Puiseux expansion having the same center (i.e. leading value at $x = u(j)$) as does $y^{(j)}$. □

DEFINITION 1.2. Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a cover of nonsingular curves for which $\mathrm{Aut}(Y/\mathbf{P}^1)^{\mathrm{Rig}} = \{\mathrm{Id}\}$. We say that *ramification provides rigidifying data for* $Y/\mathbf{P}^1$.

If we are given a description of the branch cycles for $Y/\mathbf{P}^1$, then the proposition above gives a necessary and sufficient (and computable) condition that ramification provides rigidifying data for $Y/\mathbf{P}^1$.

In §3 we explain the more general context to which the specific problems of §2 belong. For covers $Y \xrightarrow{\varphi} \mathbf{P}^1$ for which ramification provides rigidifying data we may form Hurwitz type families of covers of $\mathbf{P}^1$ having a given description of their branch cycles. For covers $Y \xrightarrow{\varphi} \mathbf{P}^1$ for which ramification does not provide rigidifying data, "Kummer Theory" is an especially appropriate and explicit tool for extending these families. Indeed, a very special case of Kummer Theory allows explicit presentation of the totally ramified cyclic cover $Y \xrightarrow{\varphi_1} Y^{\mathrm{Rig}}$ (as in the statement of the proposition). However, we have yet to carry out these considerations in detail. These comments are included here, since they *may* be the sort of thing that Herbrand had in mind in his sketchy letter [He] to E. Noether.

2. The Schur problem: Elliptic curves and complex multiplication.

Let K be a number field, and let $\mathcal{O}_K$ be the ring of integers of K. Let $f(y) \in \mathcal{O}_K[y]$ be a polynomial having the property that:

(2.1) $f(y)$ gives a one-one map on the cosets $\mathcal{O}_K/\mathfrak{q}$ for infinitely many prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$.

The original Schur Problem (conjecture; [Sc]) was to show that a polynomial satisfying (2.1) is a composition of polynomials of two types:

(2.2)(a) $ay^n + b$ (nth degree *cyclic polynomial*), or;

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

There are, of course, two aspects to this problem. The first, that the conjecture is true, is proven in [Fr, 4]. The second, *finding the polynomials that are compositions of the polynomials of type* (2.2) *that do indeed satisfy condition* (2.1), *is a very special case of the arithmetic considerations of this paper.*

In §2.A we state the general Schur problem which specializes to the problem above. The genus zero case (corresponding to the analogue of (2.1), where $f(y) \in K(y)$ is a rational function instead of a polynomial) is treated in great detail by listing the possible descriptions of the *branch cycles* for the corresponding curves as cover of $\mathbf{P}^1$. The most difficult part of this problem is to show that there is at least one cover of $\mathbf{P}^1$ corresponding to each branch cycle type in this list, which yields a *rational* function $f(y)$ satisfying condition (2.1). This is accomplished in §2.B through the use of division points on elliptic curves and the theory of complex multiplication. We hasten to add that an elementary argument suffices to show that for $K = \mathbf{Q}$, condition (2.1) is satisfied for compositions of *polynomials* of type (2.2) whose degrees are relatively prime to 6 [Fr, 4, Lemma 13].

For the reader's convenience we add a comment on the use of Hilbert's Irreducibility Theorem in §2.B. Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a cover of nonsingular projective curves such that Y and φ are defined over the number field K. For $\mathfrak{p}$, a point of $Y \otimes \bar{K}$, where $\bar{K}$ is the algebraic closure of K, we let $K(\mathfrak{p})$ denote the field generated by inhomogeneous coordinates for $\mathfrak{p}$ over K. Then Hilbert's theorem says there exist infinitely many K-rational points $\mathfrak{q} \in \mathbf{P}^1$ such that $\mathfrak{p} \in Y \otimes \bar{K}$ lying over $\mathfrak{q}$, $[K(\mathfrak{p}): K] = n = \deg(\varphi)$. In fact, we may even take $\mathfrak{q}$ to be $\mathbf{Q}$-rational.

2.A. *The general Schur problem.* Let F be a perfect field. We retain previous notation. Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a cover defined over F, etc. Let $\hat{F} = \hat{F}(Y, \varphi)$ be the algebraic closure of F in $F(Y)$ (as in the introduction). For $\tau \in G(\hat{F}/F)$ we let $\hat{F}^{(\tau)}$ be the fixed field of τ in $\hat{F}$. We consider two groups: $G(1) = G(\widehat{F(Y)}/\hat{F}(Y))$, and; $\hat{G}(1, \tau) = G(\widehat{F(Y)}/\hat{F}^{(\tau)}(Y))$. In the natural embedding of $G(\widehat{F(Y)}/F(\mathbf{P}^1))$ in S_n (discussion before Lemma 1.1) both $G(1)$ and $\hat{G}(1, \tau)$ act as permutations on the set $Z = \{2, 3, \ldots, n\}$. Let $Z_1, \ldots, Z_t$ be the orbits of $\hat{G}(1, \tau)$ on $\{2, 3, \ldots, n\}$.

Definition 2.1. We say that a cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ satisfies the *Schur condition* (over F) if there exists $\tau \in G(\hat{F}/F)$ such that for each orbit Z_i, Z_i breaks up into *strictly smaller* orbits under the action of $G(1)$.

This complicated, but entirely Galois theoretic definition is equivalent (surprisingly!) to a far more pleasant diophantine condition.

Definition 2.2. We say that the triple (Y, φ, F) has the *diophantine covering property* if: for each F-rational place $\mathfrak{q}$ of $\mathbf{P}^1$ there is one and only one F-rational place $\mathfrak{p}$ of Y lying over $\mathfrak{q}$ (in the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$). In the case that $F = \mathcal{O}_K/\mathfrak{q}$ and Y is a projective model of the affine curve $f(y) - x = 0$

where $f(y) \in F[y]$, we have condition (2.1).

PROPOSITION 2.1. *Suppose that the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ satisfies the Schur condition (over F). We consider two cases.*

If F is a finite field then:

(2.3) *(Y, φ, F') has the diophantine covering property for all extensions F' of F such that $[F' \colon F]$ is relatively prime to $[\hat{F} \colon F]$.*

If $F = K$ is a number field we denote by $(Y_\mathfrak{q}, \varphi_\mathfrak{q}, \mathcal{O}_K/\mathfrak{q})$ the reduction of the triple (Y, φ, K) modulo a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$. Then:

(2.4) *$(Y_\mathfrak{q}, \varphi_\mathfrak{q}, \mathcal{O}_K/\mathfrak{q})$ has the diophantine covering property for infinitely many prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$.*

Conversely, if either (2.3) *or* (2.4) *hold, then $Y \xrightarrow{\varphi} \mathbf{P}^1$ satisfies the Schur condition (over F).*

PROOF. Proposition 1 of [Fr, 5] shows that if F is a finite field and (Y, φ, F) satisfies the Schur condition (in the special cases considered in [Fr, 5] this property is referred to as: (Y, φ, F) is a *virtually one-one cover*) then (Y, φ, F) has the diophantine covering property. If F is a finite field we immediately deduce (2.3) since (Y, φ, F') also satisfies the Schur condition if $[F' \colon F]$ is relatively prime to $[\hat{F} \colon F]$.

Now assume that $F = K$ is a number field, and that $\tau \in G(\hat{F}/F)$ is the element for which Definition 2.1 holds. From the Čebotarev density theorem there exist infinitely many primes $\mathfrak{q}$ of $\mathcal{O}_K$ such that τ is the Frobenius element for a prime of $\hat{F}$ lying above $\mathfrak{q}$. Applying Noether's Lemma (as in [Fr, 3, §2]) we deduce that for all but a finite number of the primes $\mathfrak{q}$ for which τ is the Frobenius element for $\mathfrak{q}$ we have:

(2.5)
(a) $G\big(\widehat{(\mathcal{O}_K/\mathfrak{q})(Y_\mathfrak{q})}/\,(\mathcal{O}_K/\mathfrak{q})(P^1_\mathfrak{q})\big)$ is isomorphic to $G\big(\widehat{K(Y)}/\hat{K}^{(\tau)}(\mathbf{P}^1)\big)$, and;
(b) $G\big(\widehat{(\mathcal{O}_K/\mathfrak{q})(Y_\mathfrak{q})}/\,\widehat{(\mathcal{O}_K/\mathfrak{q})}(P^1_\mathfrak{q})\big)$ is isomorphic to $G\big(\widehat{K(Y)}/\hat{K}(\mathbf{P}^1)\big)$.

Therefore $(Y_\mathfrak{q}, \varphi_\mathfrak{q}, \mathcal{O}_K/\mathfrak{q})$ satisfies the Schur condition. We again apply Proposition 1 of [Fr, 5] to see that $(Y_\mathfrak{q}, \varphi_\mathfrak{q}, \mathcal{O}_K/\mathfrak{q})$ has the diophantine covering property.

Now assume that either (2.3) or (2.4) hold. In either case this implies that there exists a finite field F' of arbitrarily large cardinality and a triple (Y, φ, F') with $\deg(\varphi) = n$ such that (Y, φ, F') satisfies the diophantine covering property. We may (in order to establish the converse) assume that (Y, φ, F') does *not* satisfy the Schur condition.

Let $Y_1 \xrightarrow{\varphi_1} \mathbf{P}^1$ and $Y_2 \xrightarrow{\varphi_2} \mathbf{P}^1$ be two copies of the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$. The F'-irreducible components of $Y_{1\times_{\mathbf{P}^1}} Y_2$ (fiber product) are in one-one correspondence with the orbits $\{1\}, Z_1, \ldots, Z_l$ of $G(\widehat{F'(Y)}/F'(Y))$ acting on the integers $1, 2, \ldots, n$. Of course the integer 1 is itself an orbit of length 1. The absolutely irreducible components of $Y_{1\times_{\mathbf{P}^1}} Y_2$ are in one-one correspondence with those orbits X among $\{1\}, Z_1, \ldots, Z_l$ such that

(2.6) $\widehat{G\big(F'(Y)}/\hat{F}'(Y)\big)$ acts transitively on the elements of X.

We define: $Y_{1\times_{\mathbf{P}^1}} Y_2 \xrightarrow{\mathrm{pr}_1} Y_1$ and $Y_{1\times_{\mathbf{P}^1}} Y_2 \xrightarrow{\mathrm{pr}_2} Y_2$. The irreducible components of $Y_{1\times_{\mathbf{P}^1}} Y_2$ give (nontrivial) correspondences between Y and itself. The identity correspondence is represented by the orbit $\{1\}$. Since (Y, φ, F') does not satisfy the Schur condition, there exists an orbit X ($\neq \{1\}$) satisfying (2.6).

Let $\mathcal{C}(X) \subset Y_{1\times_{\mathbf{P}^1}} Y_2$ be the absolutely irreducible curve corresponding to X. Since $\mathcal{C}(X)$ is not the identity correspondence the intersection of $\mathcal{C}(X)$ and the identity correspondence has support whose degree (as a point set) can be bounded as a function of n.

Let $\mathfrak{p} \in \mathcal{C}(X)$ be an F'-rational place such that

(2.7) $\mathfrak{p}$ is *not* on the identity correspondence.

From the Riemann hypothesis for curves over finite fields there are $|F'| + O(|F'|^{1/2})$ F'-rational places $\mathfrak{p}$ satisfying (2.7) where: $O(|F'|^{1/2})$ is bounded in absolute value by $C \cdot |F'|^{1/2}$ for some constant C which can be given explicitly as a function of n. Thus, for $|F'|$ large there is at least one such F'-rational place $\mathfrak{p}$ satisfying (2.7). In addition: $\varphi_1(\mathrm{pr}_1(\mathfrak{p})) = \varphi_2(\mathrm{pr}_2(\mathfrak{p}))$ (equal to an F'-rational place $\mathfrak{q}$ on $\mathbf{P}^1$), and, if we identify Y_1 and Y_2 with Y, from (2.7), $\mathrm{pr}_1(\mathfrak{p}) \neq \mathrm{pr}_2(\mathfrak{p})$.

Therefore Y has two F'-rational places lying above the same F'-rational place on $\mathbf{P}^1$. This contradicts our assumption that (Y, φ, F') has the diophantine covering property, and we conclude the proof of the converse. □

Let $(\mathbf{Z}/(n))^*$ denote the invertible integers modulo n. For A a subgroup of $(\mathbf{Z}/(n))^*$ let

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

be a group of 2 × 2 matrices (under multiplication). The standard representation of this group on the integers modulo n is designated by $T(A, n)$. We identify A with the subgroup of $G(A, n)$ given by $\{(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}) | a \in A\}$.

THEOREM 2.1. *Let (Y, φ, F) be a triple satisfying the Schur condition where*:

(2.8) *the degree of* φ *is a prime* p $(p = n)$. *Then*:

(2.9) (a) $G(\widehat{F(Y)}/F(\mathbf{P}^1)) = G(A(\varphi), p)$, *and*;

(b) $G(\widehat{F(Y)}/\hat{F}(\mathbf{P}^1)) = G(\widehat{A(\varphi)}, p)$, *where* $\widehat{A(\varphi)} \subsetneq A(\varphi)$ *are subgroups of* $(\mathbf{Z}/(p))^*$.

Assume that the characteristic of F *is zero (or just that* $Y \xrightarrow{\varphi} \mathbf{P}^1$ *is a tamely ramified cover). If, in addition, we assume that* Y *is of genus zero, then a description of the branch cycles for* (Y, φ) (§1.A) *is given by*:

(2.10)

(a) $r = 4, \sigma(i) = \begin{pmatrix} -1 & b(i) \\ 0 & 1 \end{pmatrix}, i = 1, \ldots, 4$, *or*;

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

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

(d) $r = 3$, $a(1)$ *is of order* 2, $a(2)$ *and* $a(3)$ *are of order* 4, *or*;

(e) $Y \xrightarrow{\varphi} \mathbf{P}^1$ *has a totally ramified place (and therefore comes from a polynomial* $f(y)$ *satisfying* (2.1) *where* $f(y)$ *is of form* (2.2)(a) *or* (b)).

Outline of Proof. For details see the proof of Lemma 5 of [Fr, 5].

Since (Y, φ, F) satisfies the Schur condition, the group $G(\widehat{F(Y)}/\hat{F}(\mathbf{P}^1))$ (equipped with its natural embedding in S_p) is not a doubly transitive group. By a theorem of Burnside [Bu] this implies that (2.9)(b) holds. Since $G(\widehat{F(Y)}/\hat{F}(\mathbf{P}^1))$ is a normal subgroup of $G(\widehat{F(Y)}/F(\mathbf{P}^1))$ we deduce (2.9)(a). Also, $F \neq \hat{F}$ implies that $\widehat{A(\varphi)} \subsetneq A(\varphi)$.

When Y is of genus zero the Riemann-Hurwitz formula (1.4) implies that

$$2(p-1) = \sum_{i=1}^{r} \operatorname{ind}(\sigma(i)). \tag{2.11}$$

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 $[(p-1)/e(i)](e(i)-1)$. Therefore, if $\sigma(i)$ is not of order p for $i = 1, \ldots, r$, (2.11) becomes $2 = \Sigma_{i=1}^{r}(e(i)-1)/e(i)$.

Combinatorics show that the possible values of $e(1), \ldots, e(r)$ are given by (2.10)(a) through (e). □

Statement of the general Schur problem. In a search for covers $Y \xrightarrow{\varphi} \mathbf{P}^1$

having the diophantine covering property we come upon the Schur condition (Proposition 2.1). Putting aside the geometric and arithmetic aspects of the problem, our search is for transitive subgroups G of S_n having certain properties. These properties are:

(a) G must be a normal subgroup of some group $\hat{G} \subset S_n$ where,

(b) $\hat{G}/G$ is a cyclic group, and, if $G(1)$ (resp. $\widehat{G(1)}$) is

(2.12) the stabilizer of 1 in G (resp. $\hat{G}$) and $\mathbf{Z}_1, \ldots, \mathbf{Z}_l$ are the orbits of $\widehat{G(1)}$ on the integers $2, \ldots, n$, then for each i

(c) $\mathbf{Z}_i$ breaks up into *strictly smaller* orbits under the action of $G(1)$, $i = 1, \ldots, l$.

Suppose that G and $\hat{G}$ are given satisfying the conditions (2.12)(a), (b), and (c). Assume also that we are given $\sigma(1), \ldots, \sigma(r) \in S_n$ such that

(2.13) (a) $\sigma(1), \ldots, \sigma(r)$ generate $G(\sigma) = G$, and;
(b) $\sigma(1) \cdots \sigma(r) = \mathrm{Id}$.

DEFINITION 2.3. We say that a triple (Y, φ, F) is a *solution of the Schur problem* corresponding to the data $\mathfrak{D} = \{\sigma(1), \ldots, \sigma(r); \hat{G}\}$ if:

(a) The cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ is defined over the field F,

(2.14) (b) $\sigma(1), \ldots, \sigma(r)$ is a description of the branch cycles of the cover (Y, φ), and,

(c) $\hat{G} = G(\widehat{F(Y)}/F(\mathbf{P}^1))$.

The *general Schur problem* for a given set of data $\mathfrak{D} = \{\sigma(1), \ldots, \sigma(r); \hat{G}\}$ is to decide whether or not there is a triple (Y, φ, F) that is a solution of the Schur problem corresponding to $\mathfrak{D}$. Of course, we would hope to be able to answer this question in an arithmetic-geometric fashion that would reflect on the true diophantine nature of this problem. That is, the solutions should correspond to points on some algebraic variety.

In §2.B we solve the general Schur problem (affirmatively) in the special case that $Y \xrightarrow{\varphi} \mathbf{P}^1$ must be a *genus zero cover* of $\mathbf{P}^1$ *of prime degree p* (i.e. $\deg(\varphi) = p$). The condition on the branch cycles $\sigma(1), \ldots, \sigma(r) \in S_p$ is

$$2(p-1) = \sum_{i=1}^{r} \mathrm{ind}(\sigma(i)). \tag{2.15}$$

From Theorem 2.1 this is equivalent to solving the Schur problem (affirmatively) in the case that the data $\mathfrak{D}$ is given by $\{\sigma(1), \ldots, \sigma(r); \hat{G}\}$ where $\sigma(1), \ldots, \sigma(r)$ are elements of S_p that appear in the list (2.10)(a)–(e), and $\hat{G}$ is any one of the subgroups $G(\widehat{A(\varphi)}, p)$ containing $G(A(\varphi), p)$ (as in (2.9)(b)).

REMARK 2.1 (FURTHER PROBLEMS). From the properties that must be satisfied by the groups G and $\hat{G}$ (conditions (2.12)(a), (b), and (c)) we know in particular that G is *not* a *doubly transitive group*. In the case that n is a prime p, Burnside's Theorem (as in Theorem 2.1) describes the possible groups G and $\hat{G}$ quite explicitly. For general n, it is of particular interest to consider the case that G is a *primitive* (not doubly transitive) *subgroup of* S_n. At the end of §2.B we suggest further such groups that may arise in geometric situations and thereby be amenable to the same type of methods that are used in §2.B. However, even for these groups there are further conditions (besides those listed in expression (2.12)) that must be satisfied. These conditions are a consequence of arithmetic results and are listed in [Fr, 1, §2] under the title of *Limitation conditions*. These are relevant to the general consideration of the *extension of constants problems* (§0).

We might add that the generalization of the results of §2.B to the case when $n = p$ but (2.15) does *not* hold would seem to be quite significant.

2.B. *Elliptic curves and complex multiplication*. In this subsection F is a subfield of $\mathbf{C}$. Let E, E' denote elliptic curves (over $\mathbf{C}$). That is: E (resp. E') is a projective algebraic curve of genus 1 having distinguished point $\mathfrak{p}_0$ (resp. $\mathfrak{p}_0'$) which acts as the origin for the natural addition structure on E (resp. E'). We say that E is defined over F if the projective structures on E and point $\mathfrak{p}_0$ are defined over F. The algebraic addition law is then automatically defined over F. We denote the elliptic curve (determined up to isomorphism over $\mathbf{C}$) with 4 (resp. 6) automorphisms by E_α (resp. E_β). Let $\theta(E)$ be a nontrivial subgroup of the automorphisms (fixing $\mathfrak{p}_0$) of E. We may regard E as a complex torus $\mathbf{C}/(2\omega_1, 2\omega_2)$ where $(2\omega_1, 2\omega_2)$ denotes the $\mathbf{Z}$ lattice of $\mathbf{C}$ generated by $2\omega_1$ and $2\omega_2$. For E different from E_α or E_β, $\theta(E)$ is induced by multiplication by -1 on $\mathbf{C}$.

Let p be an odd prime. We consider 4-tuples $(E, E'; \Phi, F)$ where $E \xrightarrow{\Phi} E'$ is a degree p morphism of elliptic curves with E, E', and Φ defined over F. Thus, $E' = E/G^{(0)}$ where $G^{(0)}$ is a subgroup of E generated by some p-division point $\mathfrak{p}$ on E. Also, $G^{(0)}$ as a set is defined over F. We assume also that the elements of $\theta(E)$ are defined over F and that $G^{(0)}$ (as a set) is $\theta(E)$ invariant. The curve $E/\theta(E)$ (quotient of E by the group $\theta(E)$) is a projective genus zero curve (Kummer variety of dimension 1). From the 4-tuple (E, E', Φ, F) we obtain a commutative diagram

(2.16)
$$\begin{tikzcd}
E \arrow[r, "\Phi"] \arrow[d, "\mathrm{pr}(E)"'] & E' \arrow[d, "\mathrm{pr}(E')"] \\
E/\theta(E) \arrow[r, "\bar{\varphi}"] & E'/\theta(E')
\end{tikzcd}$$

of projective curves and morphisms, where Φ, $\bar{\varphi}$, $\mathrm{pr}(E)$, $\mathrm{pr}(E')$, $E/\theta(E)$, and $E'/\theta(E')$ are all defined over F.

LEMMA 2.1. *For suitable choices of E and $\theta(E)$, each of the covers $Y \xrightarrow{\varphi} \mathbf{P}^1$ having a description of its branch cycles given by* (2.10)(a), (b), (c), *or* (d) *is isomorphic to the cover $E/\theta(E) \xrightarrow{\bar{\varphi}} E'/\theta(E')$ (a cover of genus zero curves).*

PROOF. We interpret the conclusion to mean: there is an isomorphism ψ': $E'/\theta(E') \to \mathbf{P}^1$; an isomorphism ψ: $E/\theta(E) \to Y$, and; a commutative diagram

$$\begin{tikzcd}
E/\theta(E) \arrow[r, "\bar{\varphi}"] \arrow[d, "\psi"'] & E'/\theta(E') \arrow[d, "\psi'"] \\
Y \arrow[r, "\varphi"] & \mathbf{P}^1
\end{tikzcd}$$

First we describe the branch cycles that occur in the cover given by the lower line of the diagram (2.16). There are 4 cases:

(a) $\theta(E)$ is generated by multiplication by -1;

(b) $E' \simeq E \simeq E_\beta$ and $\theta(E) = \theta(E')$ is generated by multiplication by ρ, a cube root of 1;

(2.17) (c) $E' \simeq E \simeq E_\beta$ and $\theta(E) = \theta(E')$ is generated by multiplication by $-\rho$, and;

(d) $E' \simeq E \simeq E_\alpha$ and $\theta(E) = \theta(E')$ is generated by multiplication by $i = \sqrt{-1}$.

A point $\mathfrak{p}'$ of E' projects to a branch point of $E/\theta(E) \to E'/\theta(E')$ if and only if two or more points $\mathfrak{p}_1, \dots, \mathfrak{p}_p$ of E above $\mathfrak{p}'$ are equivalent under the action of $\theta(E)$. This implies that $\mathfrak{p}'$ is a fixed point of $\theta(E')$. In case (2.17)(a) the group $\theta(E')$ has 4 fixed points, the division points on E' of order 2. Above each such division point $\mathfrak{p}'$ is one of the division points (say $\mathfrak{p}_1$) of E of order 2. The remaining points $\mathfrak{p}_1, \dots, \mathfrak{p}_p$ are permuted in pairs by $\theta(E)$. Thus, in the case (2.17)(a) the branch cycles for the cover $E/\theta(E) \xrightarrow{\bar{\varphi}} E'/\theta(E')$ are of form

(2.18) $\sigma(j) = (2)(2)\dots(2)$ $(p-1)/2$ times, $j = 1, 2, 3, 4$.

We denote by $\wp(z; \omega_1, \omega_2)$ the Weierstrass $\wp$-function of a complex variable z (where $E \simeq \mathbf{C}/(2\omega_1, 2\omega_2)$, as above). The field of functions on $E/\theta(E)$ over $\mathbf{C}$ (resp. $E'/\theta(E')$ over $\mathbf{C}$) is given by $\mathbf{C}(\wp(z; \omega_1, \omega_2))$ (resp. $\mathbf{C}(\wp(z; \omega_1', \omega_2'))$). We recall the addition formula for $\wp(z; \omega_1, \omega_2) = \wp(z)$:

$$(2.19) \qquad \wp(u + v) = -\wp(u) - \wp(v) + \frac{1}{4}\left\{\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right\}^2$$

where u and v are independent complex variables and $\wp'(z;\ \omega_1, \omega_2) = d/dz(\wp(z;\ \omega_1, \omega_2))$ [Hi, p. 136].

Let the p-division point $\mathfrak{p}$ on E generating $G^{(0)}$ (where $E' \simeq E/G^{(0)}$) be represented by the complex number $z_0 \in \mathbf{C}$. Then the conjugates of $\wp(z;\ \omega_1, \omega_2)$ over $\mathbf{C}(\wp(z;\ \omega_1', \omega_2'))$ are given by

$$(2.20) \qquad \wp(z + j \cdot z_0;\ \omega_1, \omega_2), \qquad j = 0, 1, \ldots, p-1.$$

From (2.19) we easily deduce that the Galois closure of the field extension $\mathbf{C}(\wp(z;\ \omega_1, \omega_2))/\mathbf{C}(\wp(z;\ \omega_1', \omega_2'))$ is the field

$$\mathbf{C}(\wp(z;\ \omega_1, \omega_2), \wp'(z;\ \omega_1, \omega_2), \wp(z;\ \omega_1', \omega_2')) = M.$$

Clearly the group $G(M/\mathbf{C}(\wp(z;\ \omega_1', \omega_2')))$ is isomorphic to the group $G(A, p)$ (see discussion before Theorem 2.1) where A is generated by $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$. In fact, the substitutions $z \to -z$ and $z \to z + z_0$ in the functions generating M induce generators of $G(M/\mathbf{C}(\wp(z;\ \omega_1', \omega_2')))$ corresponding (resp.) to $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ in $G(A, p)$. Thus, to show that the branch cycles of (2.10)(a) come from covers as in (2.17)(a) we have only to count the number of inequivalent types of branch cycles in (2.17)(a), and then show that each of these arise from (2.18).

Consider the cycles of (2.10)(a). Since $\sigma(1) \cdot \sigma(2) \cdot \sigma(3) \cdot \sigma(4) = \mathrm{Id}$, we have $b(1) - b(2) + b(3) - b(4) = 0$. By conjugating each of $\sigma(1), \ldots, \sigma(4)$ by $\left(\begin{smallmatrix}1 & -b(1)/2\\ 0 & 1\end{smallmatrix}\right)$ (thereby giving an equivalent description of the branch cycles) we may assume that $b(1) = 0$. By conjugating each of the cycles by $\left(\begin{smallmatrix}a & 0\\ 0 & 1\end{smallmatrix}\right)$ we may assume that $b(2) = 0$ or 1, and in the former case $b(3) = 1$. Note that $b(2) = b(3) = b(4) = 0$ is not allowed as the group generated by $\sigma(1)$, $\sigma(2)$, $\sigma(3)$, and $\sigma(4)$ is not transitive in this case. Therefore we conclude case (2.10)(a) if we show that there are $p + 1$ distinct covers $E/\theta(E) \xrightarrow{\bar{\varphi}} E'/\theta(E')$ with E' fixed, $\deg(\bar{\varphi}) = p$.

For given $E \xrightarrow{\Phi} E'$ we have the dual isogeny $E' \xrightarrow{\hat{\Phi}} E$ (also of degree p). There are $p + 1$ such distinct morphisms $\hat{\Phi}$ (with E' fixed) corresponding to the $p + 1$ distinct subgroups of order p of the p-division points on E'. By dualizing back to $E \xrightarrow{\Phi} E'$ it is easy to show (or use the modular scheme argument of Lemma 2.1) that these give the $p + 1$ desired covers ramified over the image of the fixed points of $\theta(E')$ in $E'/\theta(E')$.

Now we must show that the cases (2.10)(b), (c), and (d) correspond, respectively to (2.17)(b), (c), and (d). Since the three cases are very similar we consider only (2.17)(d) except to say that: in case (2.17)(b), $E_\beta/\theta(E_\beta)$ is uniformized by $\wp'(z;\ \omega, e^{2\pi i/3}\omega)$; in case (2.17)(c), $E_\beta/\theta(E_\beta)$ is uniformized by $\wp^3(z;\ \omega, e^{2\pi i/3}\omega)$, and; in case (2.17)(d), $E_\alpha/\theta(E_\alpha)$ is uniformized by $\wp^2(z;\ \omega, i\omega)$.

When $\omega_1 = 1/2$, $\omega_2 = i/2$, multiplication by i fixes the cosets of 0 and $(1 + i)/2$ and, permutes the cosets of $1/2$ and $i/2$ in $\mathbf{C}/(2\omega_1, 2\omega_2)$. Thus, if

$E_\alpha \xrightarrow{\Phi} E_\alpha$ is a degree p morphism, the branch points of the induced morphism $E_\alpha/\theta(E_\alpha) \xrightarrow{\bar{\varphi}} E_\alpha/\theta(E_\alpha)$ are the 3 points representing the images of 0 and $(1+i)/2$ and the point which is the image of both $1/2$ and $i/2$. Using arguments very similar to the above (case (2.17)(a)), we find: the group of the Galois closure of the function field extension given by $\bar{\varphi}$ is isomorphic to a group $G(A,p)$ where A is the cyclic subgroup of order 4 of $(\mathbf{Z}/(p))^*$. We easily conclude that the branch cycles for the cover given by $\bar{\varphi}$ are as in (2.10)(d).

Let $\bar{\alpha} \in \mathbf{Z}/(p)$ such that $\bar{\alpha}^2 + 1 \equiv 0$ modulo (p). Such an $\bar{\alpha}$ exists since $p \equiv 1$ modulo (4). On the other hand, we have need to make a distinction between $\bar{\alpha}$ and the complex number i. The p-division points on E_α are a group H isomorphic to $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$. With this isomorphism the action of i (as an element of $\theta(E_\alpha)$ restricted to H) is given by: $(a, b) \to (-b, a)$ for $(a, b) \in H$. In order to create a diagram such as (2.16) in the situation of (2.17)(d) we need only find a subgroup $G^{(0)}$ of H of order p such that $G^{(0)}$ is invariant under the action of $\theta(E)$. Each such distinct subgroup gives a distinct cover of $\mathbf{P}^1$ with branching of type (2.10)(d). We obtain two such distinct subgroups by considering: $G_1^{(0)}$, the group generated by $(1, \bar{\alpha}) \in H$, and; $G_2^{(0)}$, the group generated by $(\bar{\alpha}, 1) \in H$. From these we obtain: two covers $Y_1 \to \mathbf{P}^1$ and $Y_2 \to \mathbf{P}^1$, each with 3 branch points (which we may select to be any three places on $\mathbf{P}^1$) and each with a description of the branch cycles of type (2.10)(d). We will conclude the lemma if we show that there are only two nonequivalent descriptions of branch cycles satisfying (2.10)(d). When this is done, we conclude that the covers $Y_1 \to \mathbf{P}^1$ and $Y_2 \to \mathbf{P}^1$ give all the covers of $\mathbf{P}^1$ with branch cycles as in (2.10)(d).

The branch cycles $\sigma(1), \sigma(2), \sigma(3)$ of (2.10)(d) are $\sigma(1) = \left(\begin{smallmatrix} -1 & b(1) \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma(2) = \left(\begin{smallmatrix} \pm\bar{\alpha} & b(2) \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma(3) = \left(\begin{smallmatrix} \pm\bar{\alpha} & b(3) \\ 0 & 1 \end{smallmatrix}\right)$ where $\bar{\alpha}^2 + 1 \equiv 0$ modulo (p). By conjugating by an element of $G((\mathbf{Z}/(p))^*, p)$ we may assume that $b(1) = 0$ and $b(2) = 1$ (as we did in the case (2.17)(a)). Using the condition that $\sigma(1)\cdot\sigma(2)\cdot\sigma(3) = \mathrm{Id}$ we have only the two possibilities: $\sigma(2) = \left(\begin{smallmatrix} \bar{\alpha} & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma(3) = \left(\begin{smallmatrix} \bar{\alpha} & \bar{\alpha} \\ 0 & 1 \end{smallmatrix}\right)$, or; $\sigma(2) = \left(\begin{smallmatrix} -\bar{\alpha} & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma(3) = \left(\begin{smallmatrix} -\bar{\alpha} & -\bar{\alpha} \\ 0 & 1 \end{smallmatrix}\right)$. □

Consider the Galois group of the Galois closure of the function field extension $\mathbf{C}(E/\theta(E))/\mathbf{C}(E'/\theta(E'))$ (as in (2.16) and (2.17)(a)) where $\theta(E) = \theta(E') = \{\pm \mathrm{Id}\}$. We have already noted in the proof of Lemma 2.1 that this group is isomorphic to $G(A,p)$ where A is generated by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Lemma 2.2 shows that there exists $(E, E'; \Phi, F)$ as in (2.17)(a) so that:

$$(2.21) \qquad G\left(\widehat{F(E/\theta(E))}/F(E'/\theta(E'))\right) \simeq G\left((\mathbf{Z}/(p))^*, p\right).$$

LEMMA 2.2. *There exists a 4-tuple* $(E, E'; \Phi, F)$ *as in* (2.17)(a) *with*: $E' = E/G^{(0)}$ *where* $G^{(0)}$ *is generated by a p-division point* $\mathfrak{p} \in E$, *and*; $[F(\mathfrak{p}) : F] = (p-1)/2$ *where* $F(\mathfrak{p})$ *is the field obtained by adjoining inhomogeneous* *coordinates of* $\mathfrak{p}$ *to* F. *In particular, from the addition formula of* (2.19) *we find that* $\hat{F}$ (*the Galois closure* F *in* $F(\widehat{E/\theta(E)})$) *is* $F(\mathfrak{p})$ *and* (2.21) *holds.*

PROOF. From [0, p. 108] we have a modular interpretation of the isomorphism classes of pairs $(E, \mathfrak{p})$ where E is an elliptic curve and $\mathfrak{p}$ is a p-division point on E. Such pairs are, in fact, in one-one correspondence with the points of the Poincaré upper half plane $\mathcal{H}$, modulo the action of the group

$$\Gamma_1(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})/(\pm \mathrm{Id}) | a \equiv d \equiv 1 \bmod(p), \right. \tag{2.22}$$
$$\left. \text{and } c \equiv 0 \bmod(p) \right\}.$$

The space $\mathcal{H}/\Gamma_1(p)$ can be compactified. The resulting object has the structure of a projective curve defined over $\mathbf{Q}$, which we denote by $X_1(p)$. Let $X_0(p)$ be the modular curve of level p. Then, there are canonical covering morphisms $X_1(p) \xrightarrow{\psi} X_0(p) \xrightarrow{\gamma} \mathbf{P}^1$ (defined over some finite extension F' of $\mathbf{Q}$) such that: $\deg \psi = (p-1)/2$; ψ maps a pair $(E, \mathfrak{p})$ to the pair $(E, G^{(0)})$ where $G^{(0)}$ is the group generated by $\mathfrak{p}$, and, γ maps $(E, G^{(0)})$ to the point of $\mathcal{H}/SL(2, \mathbf{Z})$ corresponding to the isomorphism class of the elliptic curve E.

From Hilbert's irreducibility theorem (see discussion prior to §2.A) there exists a $\mathbf{Q}$-valued point $\mathfrak{q}$ of $\mathbf{P}^1$ such that there is a place $\mathfrak{p}'$ of $X_1(p)$ of degree equal to $\deg(\gamma \circ \psi)$ over $F'(\mathfrak{q})$. Suppose $\mathfrak{p}'$ corresponds to $(E, \mathfrak{p})$ and $\mathfrak{p}''$ (the place of $X_0(p)$ below $\mathfrak{p}'$) corresponds to $(E, G^{(0)})$. Let $F = F'(\mathfrak{p}'')$. Then E and $E/G^{(0)}$ are defined over F, and the conclusion of the lemma follows. □

Let $\sigma(1), \ldots, \sigma(r) \in G(\hat{A}, p)$ be a description of the branch cycles of a genus zero cover of $\mathbf{P}^1$ of prime degree p where $\hat{A}$ is a subgroup of $(\mathbf{Z}/(p))^*$. Let A be a subgroup of $(\mathbf{Z}/(p))^*$ containing $\hat{A}$.

THEOREM 2.2. *For the data* $\mathcal{D} = \{\sigma(1), \ldots, \sigma(r): G(A, p)\}$ (*as in Definition* 2.3) *there exists a solution to the general Schur problem corresponding to the data* $\mathcal{D}$.

PROOF. From Lemma 2.1 we have only to show that for each of the members of the list (2.17)(a), (b), (c), (d), one of the covers $E/\theta(E) \xrightarrow{\bar{\varphi}} E'/\theta(E')$ of the collection satisfies condition (2.21) for some field F. Then, if $\hat{F}$ is the algebraic closure of F in $F(\widehat{E/\theta(E)})$ (the Galois closure of $F(E/\theta(E))/F(E'/\theta(E'))$), we have $G(\hat{F}/F)$ is isomorphic to the quotient of $(\mathbf{Z}/(p))^*$ by $\hat{A}$. Let F' be the fixed field of A in $\hat{F}$. Then, if we extend F to F', we conclude that $(E/\theta(E), \bar{\varphi}, F')$ is a solution of the Schur problem for the data $\mathcal{D}$.

We use the notation of Lemma 2.2. Our task is to show that the coordinates of a p-division point generating $G^{(0)}$ generates an extension of F of degree

$(p-1)/2$. For the case (2.17)(a) it follows from Lemma 2.2 that $(E/\theta(E), \bar{\varphi}, F)$ can be chosen so that this is so. For the other cases this follows from the theory of complex multiplication [Sh & T, p. 135] or [Sw-D]. In fact, in cases (2.17)(b) and (c) we take $F = \mathbf{Q}(\sqrt{-3})$, and in case (2.17)(d) we take $F = \mathbf{Q}(i)$. Our result here is essentially equivalent to that part of the theory of complex multiplication which describes the abelian extensions of the fields $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(i)$. □

REMARK 2.2. Let M be a finite quotient of the additive group $\mathbf{Z} \oplus \mathbf{Z}$. Let A be a subgroup of $\mathrm{Aut}(M)$. Consider the semidirect product $G(A, M) = A \times_* M$ where multiplication of (a_1, m_1) and (a_2, m_2) is given by:

$$(a_1, m_1) * (a_2, m_2) = (a_1 \cdot a_2, (m_1)a_2 + m_2).$$

Note that A is naturally embedded in $G(A, M)$. We use a right action as being more natural than the historical left action. Note that A is naturally embedded in $G(A, M)$ by $a \in A \to (a, \mathrm{Id}) \in G(A, M)$.

The group $G(A, M)$ has a transitive permutation representation $T(A, M)$ on the elements of M given by: (a, m) sends $m' \in M$ to $(m')a + m$. This representation is *primitive* precisely when there does *not* exist a group H with $A \subsetneq H \subsetneq G(A, M)$. If the representation is imprimitive, any such H is a semidirect product of A and a subgroup M' of M which is invariant under the action of A.

This can be generalized still further to consider groups M which are finite quotients of $\mathbf{Z}^n$ for some integer n. All of these groups are especially interesting in relation to the general Schur problem and the extension of constants problem as they correspond to analogues of the theory of complex multiplication involving abelian varieties of dimension greater than 1. □

3. **Determination of arithmetic monodromy from branch cycles.** This section consists of a conjecture and a discussion of the compatibility of the results of §2 with this conjecture. We return to the notations of §1.B, except that initially our discussion is over the field $\mathbf{C}$.

Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a connected cover of nonsingular projective curves and let $\sigma(1), \ldots, \sigma(r) \in S_n$ ($n = \deg(\varphi)$) be a description of the branch cycles of this cover (§1.A). Assume also that *ramification provides rigidifying data* (§1.B) for the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$. From the proposition of §1.B this condition may be checked combinatorially from the data given by $\sigma(1), \ldots, \sigma(r)$. Therefore, if $Y' \xrightarrow{\varphi'} \mathbf{P}^1$ is any other cover having $\sigma(1), \ldots, \sigma(r)$ as a description of its branch cycles, then

(3.1) *ramification provides rigidifying data* for $Y' \xrightarrow{\varphi'} \mathbf{P}^1$.

Let $\mathcal{P}(\sigma(1), \ldots, \sigma(r)) = \mathcal{P}(\sigma)$ be the collection of equivalence classes of pairs consisting of: an isomorphism class of covers $Y' \xrightarrow{\varphi'} \mathbf{P}^1$ having a description of its branch cycles given by $\sigma(1), \ldots, \sigma(r)$, and, an ordering $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_m$ of the collection of points of Y' lying over the branch points of φ'. We say two pairs are equivalent under the conditions given by expression (1.5). The construction of [Fr, 1, §4] shows that $\mathcal{P}(\sigma)$ has the structure of a complex manifold.

For the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$ let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be a fixed ordering of the points of Y lying over the branch points of φ.

DEFINITION 3.1. The *Ramification Parameter Space* $\mathcal{P}^{\mathrm{Ram}} = \mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ is the (unique) connected component of $\mathcal{P}(\sigma)$ containing the pair$\{Y \xrightarrow{\varphi} \mathbf{P}^1;\ \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. There is a natural map from $\mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ to the *Hurwitz Parameter Space* $\mathcal{P}(Y, \varphi)$ given by projection of the pairs $\{Y' \xrightarrow{\varphi'} \mathbf{P}^1;\ \mathfrak{p}'_1, \ldots, \mathfrak{p}'_m\}$ onto the first coordinate (i.e., $Y' \xrightarrow{\varphi'} \mathbf{P}^1$). We denote this canonical map by $\psi(Y, \varphi)$: $\mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) \to \mathcal{P}(Y, \varphi)$.

In addition, the technique of [Fr, 1, §4] shows that there is a complex manifold $\mathcal{T}^{\mathrm{Ram}}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ and a canonical diagram

$$(3.2)\qquad \begin{tikzcd} \mathcal{T}^{\mathrm{Ram}}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) \arrow[r, "\Phi^{\mathrm{Ram}}"] & \mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) \times \mathbf{P}^1 \arrow[r, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) \\ & & \mathbf{P}^1 \end{tikzcd}$$

such that

(3.3)
(a) for $\mathfrak{p} \in \mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ the fiber $\mathcal{T}^{\mathrm{Ram}}_{\mathfrak{p}}$ of $\mathrm{pr}_1 \circ \Phi^{\mathrm{Ram}}$, is presented as a cover of $\mathbf{P}^1$ by restriction of $\mathrm{pr}_2 \circ \Phi^{\mathrm{Ram}}$, and,
(b) the cover $\mathcal{T}^{\mathrm{Ram}}_{\mathfrak{p}} \to \mathbf{P}^1$ represents the isomorphism class of $\psi(Y, \varphi)(\mathfrak{p}) \in \mathcal{P}(Y, \varphi)$.

In [Fr, 2] the following topics are considered:

(i) the minimal field of definition of the diagram of (3.2) and related diagrams (generalizing the results of [Fr, 1, §5]);

(ii) finding *explicit* embeddings of the diagram (3.2) into projective spaces, and,

(iii) computing explicitly the degree of the étale morphism $\psi(Y, \varphi)$.

For $\mathfrak{p} \in \mathcal{P}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) = \mathcal{P}$ let $B_{\mathfrak{p}}$ be the subset of points $\bar{\mathfrak{p}} \in \mathcal{T}^{\mathrm{Ram}}_{\mathfrak{p}}$ such that $\bar{\mathfrak{p}}$ lies over a branch point of the cover of (3.3)(b). For example, if $\mathfrak{p}$ corresponds to $\{Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ then $B_{\mathfrak{p}}$ consists of the points $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. It is easy to establish that $\bigcup_{\mathfrak{p} \in \mathcal{P}^{\mathrm{Ram}}} B_{\mathfrak{p}} = \mathcal{B}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ has a natural structure of a complex manifold and there is a natural étale morphism

$$(3.4)\qquad \mathcal{B}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m) \xrightarrow{\Delta_{\mathrm{Ram}}} \mathcal{P}(Y, \varphi).$$

For each integer i, $i = 1, \ldots, m$ let $\mathcal{B}_i$ be the connected component of

$\mathfrak{B}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ *containing* $\mathfrak{p}_i$ in the fiber over the point corresponding to (Y, φ) in $\mathfrak{P}(Y, \varphi)$.

For the rest of the discussion we renumber $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ to be compatible with the numbering in §1.B. That is, we list these points as $\mathfrak{p}(i, j)$, $j = 1, \ldots, n(i)$ and $i = 1, \ldots, r$ where $\mathfrak{p}(i, j)$ lies over the branch point $u(i)$ of the cover $Y \xrightarrow{\varphi} \mathbf{P}^1$. With this renumbering we label $\mathfrak{B}_i$ by $\mathfrak{B}_{\mathfrak{p}(l,k)}$ where $\mathfrak{p}(l, k) = \mathfrak{p}_i$.

The Hurwitz Parameter Space has a natural morphism to an open subset of $\mathbf{P}^r$

$$\begin{aligned} \mathfrak{P}(Y, \varphi) \xrightarrow{\alpha} \mathbf{P}^r \quad & \text{where } \alpha\colon \left\{ Y' \xrightarrow{\varphi'} \mathbf{P}^1 \right\} \\ & \to \{\text{the unordered collection of branch points of } \varphi'\}. \end{aligned} \tag{3.5}$$

Thus we have a map

$$\mathfrak{B}_{\mathfrak{p}(l,k)} \xrightarrow{\alpha \circ \Delta_{\mathrm{Ram}}} \mathbf{P}^r \quad \text{for all } \mathfrak{p}(l, k). \tag{3.6}$$

From the methods of [Fr, 1, §5] it is easy to show that the pair $(\mathfrak{B}_{\mathfrak{p}(l,k)}, \alpha \circ \Delta_{\mathrm{Ram}})$ is defined over some finite extension of $\mathbf{Q}$.

Definition 3.2. The *field of moduli* of $(\mathfrak{B}_{\mathfrak{p}(l,k)}, \alpha \circ \Delta_{\mathrm{Ram}})$ is the fixed field in $\overline{\mathbf{Q}}$ of the subgroup H of $G(\overline{\mathbf{Q}}/\mathbf{Q})$ consisting of $\sigma \in G(\overline{\mathbf{Q}}/\mathbf{Q})$ such that: the conjugate $(\mathfrak{B}^{\sigma}_{\mathfrak{p}(l,k)}, (\alpha \circ \Delta_{\mathrm{Ram}})^{\sigma})$ of $(\mathfrak{B}_{\mathfrak{p}(l,k)}, \alpha \circ \Delta_{\mathrm{Ram}})$ under σ is isomorphic to $(\mathfrak{B}_{\mathfrak{p}(l,k)}, \alpha \circ \Delta_{\mathrm{Ram}})$. That is, there exists γ_σ, an analytic isomorphism, fitting in a commutative diagram:

$$\begin{tikzcd} \gamma_\sigma\colon \mathfrak{B}^{\sigma}_{\mathfrak{p}(l,k)} \arrow[rr] \arrow[dr, "(\alpha \circ \Delta_{\mathrm{Ram}})^{\sigma}"'] & & \mathfrak{B}_{\mathfrak{p}(l,k)} \arrow[dl, "(\alpha \circ \Delta_{\mathrm{Ram}})"] \\ & \mathbf{P}^1 & \end{tikzcd} \tag{3.7}$$

Let $K_{\mathfrak{p}(l,k)}$ be the *field of moduli* of $(\mathfrak{B}_{\mathfrak{p}(l,k)}, \alpha \circ \Delta_{\mathrm{Ram}})$.

Let $\mathfrak{p}' \in \mathfrak{P}(Y, \varphi)$ correspond to a cover $Y' \xrightarrow{\varphi'} \mathbf{P}^1$ where this cover is defined over a field K'. Let $P(l, k)_1, \ldots, P(l, k)_t \in \mathfrak{B}_{\mathfrak{p}(l,k)}$ be the points of $\mathfrak{B}_{\mathfrak{p}(l,k)}$ lying over $\mathfrak{p}'$, and let $K_{\mathfrak{p}(l,k)}(P(l, k))$ be the field generated over $K' \cdot K_{\mathfrak{p}(l,k)}$ by the inhomogeneous coordinates of the points $P(l, k)_1, \ldots, P(l, k)_t$.

Arithmetic form of Riemann's existence theorem (Conjectural). *Consider the field extension of K' given by*:

$$\bigcap_{i=1}^{r} \big(K_{\mathfrak{p}(i,1)}(P(i, 1)) \cdot K_{\mathfrak{p}(i,2)}(P(i, 2)) \cdots K_{\mathfrak{p}(i,n(i))}(P(i, n(i)))\big) = M_{\mathfrak{p}'}.$$

Then, if $\hat{K}'$ is the algebraic closure of K' in $\widehat{K'(Y')}$ (the Galois closure of $K'(Y)/K'(\mathbf{P}^1)$), the field $\hat{K}'$ is contained in a cyclotomic extension of $M_{\mathfrak{p}'}$.

In fact, the methods used in the branch cycle argument in [Fr, 1, §5, proof of Theorem 5.1] give a reasonable prediction for a cyclotomic field L such that $L \cdot M_{p'} = \hat{K}'$.

We comment quickly on the case given by $(\sigma(1), \sigma(2), \sigma(3), \sigma(4)) = \boldsymbol{\sigma}$ as in (2.10)(a). In this case the proof of Lemma 2.2 is equivalent to the statement that $\mathfrak{B}(Y, \varphi; \mathfrak{p}_1, \ldots, \mathfrak{p}_m)$ has one connected component which we denote by $\mathfrak{B}$. In addition the morphism $\mathfrak{B} \xrightarrow{\Delta_{\mathrm{Ram}}} \mathcal{P}(Y, \varphi)$ is of degree $(p-1)/2$. Lemma 2.1 amounts, in this case, to the proof that the conjectured form of Riemann's existence theorem holds (although there are some substantial details to check to make this precise) in the strong form that $\hat{K}' = M_{\mathfrak{p}'}$.

In [Fr, 1, §6] there is an example to show that the field of moduli of a cover is not necessarily a field of definition of the cover (although it is contained in every field of definition of the cover).

Bibliography

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

[Cl] A. Clebsch, *Zür Theorie der Riemannshen Fläche*, Math. Ann. **6** (1872), 216–230.

[Fr, 1] M. Fried, *Field of definition of function fields, and Hurwitz families*; and *Groups as Galois groups over* Q(x), Comm. Algebra **5** (1977), 17–82.

[Fr, 2] ______, *General moduli problems with application to the stable existence of Hurwitz families* (preprint).

[Fr, 3] ______, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231. MR **50** #2117.

[Fr, 4] ______, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55. MR **41** #1688.

[Fr, 5] ______, *Arithmetical properties of function fields*. II, Acta Arith. **25** (1974), 225–258.

[Fu] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. of Math. (2) **90** (1969), 542–575. MR **41** #5375.

[Gr] A. Grothendieck, *Géométrie formelle et géométrie algébrique*, Séminaire Bourbaki, 11 ième annee: 1958/59, Fasc. 3, Exposé 182, Secrétariat Mathématique, Paris, 1959. MR **28** #1091.

[He] J. Herbrand, *Zur theorie der algebraischen Functionen* (*Aus Briefen an E. Noether*), Math. Ann. **106** (1932), 502.

[Hi] E. Hille, *Analytic function theory*, Vol. II, Ginn, Boston, 1962, pp. 136–141. MR **34** #1490.

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

[L] S. Lang, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962. MR **26** #119.

[Mum] D. Mumford, *Introduction to algebraic geometry*, Harvard Univ. Notes, 1966.

[O] A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111. MR **45** #178.

[Ri] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.

[Sc] I. Schur, *Über den Zusammenhang Zwischen einem Problem der Zahlentheorie and einem Satz über algebraische Functionen*, S. B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1923), 123–134.

[Sh & T] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan 6, Math. Soc. Japan, Tokyo, 1961. MR **23** #A2419.

[Sp] G. Springer, *Introduction to Riemann surfaces*, Addison-Wesley, Reading, Mass., 1957. MR **19**, 1169.

[Sw-D] H. P. F. Swinnerton-Dyer, *Applications of algebraic geometry to number theory*, 1969 Number Theory Institute (Stony Brook, 1969), Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc. Providence, R.I., 1971, pp. 1–52. MR **49** #2720.

Department of Mathematics, University of California, Irvine, California 92717