ACTA ARITHMETICA
XXV (1974)

Arithmetical properties of function fields (II)
The generalized Schur problem

by

MICHAEL D. FRIED (Stony Brook, N. Y.)

Let K be a field, with K^* a fixed algebraic closure of K. Let $Y \xrightarrow{\varphi} \boldsymbol{P}^1(K^*)$ be a connected finite (branched) covering of algebraic curves where $\boldsymbol{P}^1(K^*)$ denotes projective 1-space over K^*. Suppose that Y and φ are defined over K, and that $K(Y)$ is the field of functions on Y defined over K. Thus, $K(Y) = K(\boldsymbol{P}^1)(y) = K(x, y)$ where $K(\boldsymbol{P}^1) = K(x)$ with x transcendental over K and y is a primitive generator of $K(Y)$ over $K(\boldsymbol{P}^1)$. We denote the conjugates of y over $K(x)$ by $y_1 = y, y_2, \ldots, y_n$. The Galois closure of $K(Y)/K(x)$, denoted $\widehat{K(Y)}$ (or Ω_Y in the text) is $K(x, y_1, \ldots, y_n)$. The *arithmetic monodromy group of* (Y, φ), denoted $\mathrm{Mon}(Y, \varphi, K)$, is the Galois group $G\big(\widehat{K(Y)}/K(\boldsymbol{P}^1)\big)$ equipped with a permutation representation class T obtained by the action of $G\big(\widehat{K(Y)}/K(\boldsymbol{P}^1)\big)$ on the set $\{y_1, \ldots, y_n\}$. The general motivating problem for this paper is:

EXTENSION OF CONSTANTS PROBLEM. *Let $\hat{K}$ denote the algebraic closure of K in $\widehat{K(Y)}$. Describe $\hat{K}$.*

Obviously, as stated, the extension of constants problem is too imprecise to generate a research plan (see, however, Section 5). Therefore we describe an illustrative special case of the general problem.

GENERALIZED SCHUR PROBLEM. *The group $G\big(\widehat{K(Y)}/\hat{K}(\boldsymbol{P}^1)\big)$ is contained in $G\big(\widehat{K(Y)}/K(\boldsymbol{P}^1)\big)$ as a subgroup of index $[\hat{K} : K]$. Assume that:*

(0.1) *$K(x, y_1)$ is a regular extension of $K(x)$ (i.e.*

$$[\hat{K}(x, y_1) : K(x, y_1)] = [\hat{K} : K]);$$

and also that

(0.2) *each orbit of $G\big(\widehat{K(Y)}/K(x, y_1)\big)$ on $y_2, \ldots, y_n$ breaks up into strictly smaller (shorter length) orbits under the action of $G\big(\widehat{K(Y)}/\hat{K}(x, y_1)\big)$.*

We say that (Y, φ) is a *virtually-one-one cover over* K if (0.1) and (0.2) hold. Describe the virtually one-one covers over K.

We mention an arithmetic (and diophantine) application of the notion of virtual-one-one-ness. Suppose that (Y, φ) has an affine model given by the zeros of a polynomial $g(x, y) \in K[x, y]$ (where projection onto the x variable corresponds to the morphism φ). Condition (0.1), in this case, is that $g(x, y)$ is absolutely irreducible over K. Assume also that $K = L$ is a finite field. Then (Proposition 1 of [8]) (Y, φ) is virtually-one-one over L if and only (Y, φ) defines a *one-one map for infinitely many finite field extensions* L' *of* L. That is, there exist infinitely many finite field extensions L' of L such that:

(0.3) for each $x_0 \in L' \dot{\cup} \{\infty\}$, there exists a unique $y_0 \in L' \dot{\cup} \{\infty\}$ such that $g(x_0, y_0) = 0$.

We come closer to the state of the literature with further specialization of the generalized Schur problem to:

GENERALIZED SCHUR PROBLEM FOR RATIONAL FUNCTIONS. *Let* $f \in K(y)$ *be a rational function in one variable. We say that* f *is virtually-one-one* (called *exceptional* in [15]; we find the term virtually-one-one more suggestive) *if*

(0.2a) $\dfrac{f(y)-f(z)}{y-z}$ *has no absolutely irreducible factors over* K (Definition 5). *Classify virtually one-one rational functions.*

In [3] (the paper preceding this one) we considered a general class of problems about value sets of polynomials. In this paper we focus our attention almost entirely (except for Section 4, where we finish some loose ends from [3]) on the generalized Schur problem for rational functions. For the relation between the generalized Schur problem for rational functions and the work of Wells and Lidl, see the introduction of [8]. For previous literature consult the excellent bibliography prepared by Charles Wells (with the aid of W. Nöbauer [15]).

Eventually these problems should be treated as part of a generalized Riemann existence theorem. We are being heuristic here, but roughly: suppose we are given a set of elements $\sigma_1, \ldots, \sigma_r$ in the symmetric group on n letters with $\prod_{i=1}^{r} \sigma_i = \mathrm{Id}$. We might hope to have a combinatorial procedure where we could find out if there exists a field K and a cover $Y \xrightarrow{\varphi} \boldsymbol{P}^1(K^*)$ (as above) with a description of its branch cycles given by $\sigma_1, \ldots, \sigma_r$, such that (Y, φ) is virtually-one-one over K. The important thing is that this desired procedure should involve only finite computations with the elements $\sigma_1, \ldots, \sigma_r$. The problems, theorems, and examples of this paper give empirical data toward a formulation of such a generalized

Riemann existence theorem. In Section 5 we give a formulation (conjectural) of such an existence theorem, and then, assuming its truth, show how the generalized Schur problem would be reduced to group theory (albeit, very hard group theory).

Continuing the results of [4], we show in Theorem 1 that if $f(y)$ is a tame (Definition 4) virtually-one-one polynomial, then f is a composition of cyclic and Chebychev polynomials (expressions (1.16) and (1.17)). Since it is possible to decide which compositions of cyclic and Chebychev polynomials are virtually-one-one over a given finite field, the generalized Schur problem can be considered solved if we restrict ourselves to tame polynomials.

Preceding Proposition 1 is a discussion of a procedure for computing the nature of the ramification over the place $x = \infty$ on the curve $f(y) - x = 0$ for $f \in L[y]$ (f is no longer assumed tame). See [7] and Section VIII of [16]. Suppose $f \in L(y)$ is a virtually-one-one rational function with

$$(0.4) \qquad f = \frac{p(y)}{q(y)} \quad \text{where } p \text{ and } q \text{ are relatively prime polynomials,}$$

and we define $\bar{n}(f) = \deg p - \deg q$. Proposition 1 shows that q has no L-rational zeros and if $(\bar{n}(f), \operatorname{char} L) = 1$ then L can contain no non-trivial $\bar{n}(f)$th roots of 1 (in particular, since $-1 \in L$, $\bar{n}(f)$ must be odd). Also, if f is a virtually-one-one polynomial, we have the following particular consequence of Proposition 1. Suppose that

$$f(y) = y^{p^{v(0)} \cdot d(0)} + y^{d(1)} + \text{lower terms where } \operatorname{char} L = p,$$

and

$$(0.5) \qquad (d(0), p) = (d(1), p) = 1 \quad \text{and} \quad p^{v(0)} \cdot d(0) > d(1).$$

Then,

$$(d(0) - d(1), p^{v(0)} - 1) > 1.$$

In Theorem 2 we consider $f(y) \in L(y)$ (as in (0.4)) such that f is a virtually-one-one, tame function (actually the proof needs only that the curve defined by $f(y) - x = 0$ is tame over $x = \infty$). As a particular consequence (Corollary 1) we obtain: for $1 \leqslant \deg q \leqslant 9$ there exist only finitely many integers $\bar{n}$ (the bound on $\bar{n}$ is independent of L) such that there exists $f \in L(y)$ as above with $\bar{n}(f) = \bar{n}$.

Let L^* be a fixed algebraic closure of L. It is possible that $f(y) \in L(y)$ is indecomposable over L, but decomposable over L^*. Thus, unlike the case where $f(y)$ is a tame polynomial, in general we are not able to reduce to the case where f is virtually-one-one and indecomposable over L^*. In Section 2 we consider this situation under the additional assumption that $f(y)$ is tame. The work of this section is continued in [6] and is mainly

a contribution to the computation of the lattice of fields between $L^*(y)$ and $L^*(f(y))$ in our situation using Riemann surface techniques.

In Section 3 we give a list of tame rational functions (over C) of prime degree (following some computations implicit in [12], we give an unusual characterization of these functions via modular functions) which must contain the tame virtually-one-one rational functions of prime degree. See Section VII of [16] for the conclusion.

Section 4 contains problems and counterexamples related to the "Polynomial conjecture" discussed in [3]. A good portion of the significant work in this paper is contained in the problems and examples placed at the end of each section.

Most of the results presented here were known to the author over four years ago, and this paper is an updated version of a paper written at that time. A word of warning is in order. This is a very down-to-earth paper (say, in relation to [7] or [16]). However, it is not a simple paper, as I have been willing to use difficult combinatorial arguments where general arguments seemed not to work. The idea of the paper is to bridge the present literature with the extension of constants problem by giving some solid results and problems from which research direction might be indicated. The reader, I hope, will come to appreciate the task, and bear with me whatever meager success results.

We thank Don Lewis for suggesting the title *virtually-one-one cover* as in (0.2). Also, Roger Howe gave us the p-group counterexample of Example 9.

1. Generalization of Schur's conjecture. Let L be an arbitrary perfect field, and L^* a fixed algebraic closure of L. Unless otherwise stated, all function field extensions and polynomials will be assumed to be separable. Let $f(y) \in L(y)$ where $f(y) = p(y)/q(y)$ and $p, q \in L[y]$ are relatively prime polynomials.

DEFINITION 1. If $f(y) \in L(y)$ is of form $p(y)/q(y)$ where p, q are relatively prime polynomials, then *degree* f is by definition the maximum of degree p and degree q. This notion of degree is multiplicative with respect to composition of functions.

DEFINITION 2. A rational function $f(y) \in L(y)$ is said to be *decomposable over* L if we can write $f(y) = f_1(f_2(y))$ where f_1 and f_2 are rational functions over L of degree greater than 1. Then f_1 and f_2 are called *composition factors* of f over L.

DEFINITION 3. Let $h(x, y) \in L(x, y)$ (where x and y are algebraically independent indeterminants). Then $\deg_y h$ is by definition the degree of h as an element of $M(y)$ where $M = L(x)$. If the algebraic curve described by setting h equal to zero is irreducible, we say that h is an *irreducible rational function in two variables.*

Let $f(y) \in L(y)$ be of degree n. We denote by $y_1, \ldots, y_n$ the zeros of $f(y)-x$. As in [4] we let $\Omega_{f-x} = L(y_1, \ldots, y_n)$. Then $G\left(\Omega_{f-x}/L(x)\right)$ denotes the Galois group of $\Omega_{f-x}/L(x)$.

DEFINITION 4. We say that a rational function $f(y) \in L(y)$ is *tame over* L if either

(1.1) The characteristic of L is zero,

or

(1.2) The abstract Riemann surface of $f(y)-x$ is tamely ramified over the x-sphere.

Condition (1.1) automatically implies condition (1.2). Let $\bar{n} = \deg p - \deg q = \bar{n}(f)$. For the problems that concern us we may replace f by

$$\frac{af(y)+b}{cf(y)+d} \quad \text{for} \quad a, b, c, d \in L \tag{1.3}$$

such that $ad-bc \neq 0$. By suitable choice of a, b, c, d we may assume that $\bar{n}\left(\frac{af+b}{cf+d}\right) \geqslant 1$.

DEFINITION 5. We say that $f(y) \in L(y)$ is *virtually-one-one* (called *exceptional* in [15]) over L if

$$\frac{f(y)-f(z)}{y-z} = \varphi(y, z) \text{ has no absolutely irreducible factors over } L. \tag{1.4}$$

Let R be either the ring of integers of a number field K or a finite field. We denote by $\mathrm{Res}(R)$ the collection of finite field extensions of residue class fields of R. We say that $f(y) \in K(y)$ (where K is the quotient field of R) is *virtually-one-one over* $\mathrm{Res}(R)$ if (1.4) holds for infinitely many $L \in \mathrm{Res}(R)$. Let $C > 0$ be a constant. We say that $f(y)$ is *virtually-one-one over* $\mathrm{Res}(R, C)$ if f is virtually-one-one for infinitely many $L \in \mathrm{Res}(R)$ with $\mathrm{char}\, L > C$.

LEMMA 1. *Let $h(y, z) \in L(y, z)$ (rational function field in two indeterminates y and z) be irreducible over L. Then $h(y, z)$ is absolutely irreducible over L iff*

$$M \cap L^* = L \tag{1.5}$$

where M is the function field of the curve $h(y, z) = 0$.

Also, we obtain equality in the expression

$$G\left(\hat{M}/L(y)\right) \cong G\left(L^* \cdot \hat{M}/L^*(y)\right) \tag{1.6}$$

where $\hat{M}$ is the Galois closure of $M/L(y)$, iff

$$\hat{M} \cap L^* = L. \tag{1.7}$$

Remark 1. Since the elements of Ω_{f-x} are all rational functions in $y_1, \dots, y_n$ with coefficients in L, the absolute constants $\hat{L}$ of Ω_{f-x} lie in any field obtained by adjoining to L the coefficients of Puiseux expansions for $y_1, \dots, y_n$ over any rational tamely ramified place of the x-sphere. If $a \in L \cup \{\infty\}$ corresponds to a place of the x-sphere, call the field just described L_a. In particular, if $a = \infty$ and f is a polynomial tamely ramified over ∞, then $L_\infty = L(\zeta_n)$ where ζ_n is primitive nth root of 1. From Hilbert's irreducibility theorem, in the case where $L = K$ is a number field we have $\bigcap_{a \in K} K_a = \hat{L}$ (see Section VII of [16]).

We introduce some notation to be retained throughout this paper. Let S_n be the symmetric group on n letters. An element $\sigma \in S_n$ can be written as a product of disjoint cycles

$$\sigma = \prod_{i=1}^{r} \gamma_i, \quad \text{where} \quad \text{length of } \gamma_i \text{ is } s(i), i = 1, \dots, r. \tag{1.8}$$

We will sometimes abuse standard notation and write

$$\sigma = \prod_{i=1}^{r} (s(i)) \quad \text{or} \quad (s(1))(s(2)) \dots (s(r)). \tag{1.9}$$

Then we have, order of $\sigma = [s(1), \dots, s(r)]$ (l.c.m. of $s(1), \dots, s(r)$) and

$$\text{ind } \sigma = \sum_{i=1}^{r} (s(i) - 1). \tag{1.10}$$

Lemma 2. *Let $f(y) \in L[y]$ (f is a polynomial), with $(\deg f, \text{char } L) = 1$. Then the lattice of fields between $L(y)$ and $L(f(y))$ is isomorphic (as a lattice) to the lattice of fields between $L^*(y)$ and $L^*(f(y))$* (Lemma 1 of [9]).

Theorem 1. *With the notation of Definition 5, let K be the quotient field of R. Let $L \in \text{Res}(R)$ and $f(y) \in L(y)$. Suppose*

$$f = f_1(f_2(\dots(f_l(y))\dots)) \quad \text{where} \quad f_i \in L(y) \text{ for } i = 1, \dots, l. \tag{1.12}$$

Then there exists an index i such that

$$f_i \text{ is not virtually-one-one over } L, \text{ iff} \tag{1.13}$$

$$f \text{ is not virtually-one-one over } L. \tag{1.14}$$

Also, (1.13) *holds if*

$$f_i \text{ is indecomposable over } L^* \text{ and } G(L^* \cdot \Omega_{f_i - x} / L^*(x)) \text{ is doubly-transitive on } y_1(i), \dots, y_{n(i)}(i) \text{ (the zeros of } f_i - x). \tag{1.15}$$

Suppose $f(y) \in L[y]$ is a tame polynomial over L. Then (1.14) *holds unless f is a composition of polynomials of the following type:*

$$ay^n + b \quad (\text{cyclic polynomials}) \tag{1.16}$$

and

$$T_n(y) = 2^{-n-1}\{(y+(y^2+4)^{1/2})^n + (y-(y^2+4)^{1/2})^n\} \tag{1.17}$$

(*Chebychev polynomials*).

Now assume $f \in K(y)$, *and* (1.12) *and* (1.13) *hold* (*see Problem* 1) *with* L *replaced by* K. *Then there exists a constant* $C > 0$ (*dependent on* f) *such that* f *is not virtually-one-one over* $\mathrm{Res}(R, C)$.

Proof. There are many ways to proceed. We have chosen the most expedient, not the most elementary. From the generalization of MacCluer's theorem (Proposition 1 of [8] or [18]) f describes a one-one map on $L_k \cup \infty \to L_k \cup \infty$ for infinitely many field extensions $L_k \in \mathrm{Res}(L)$ iff f is virtually-one-one. However, f is one-one (and therefore onto, since L is a finite field) on $L_k \cup \infty$ iff f_i is one-one on $L_k \cup \infty$ for $i = 1, \ldots, l$ (as in (1.12)). Thus (1.13) is equivalent to (1.14). Note that (1.15) implies that $\varphi_i(y, z) = \dfrac{f_i(y) - f_i(z)}{y - z}$ is absolutely irreducible, because the zeros of $\varphi_i(y_1(i), z)$ are $z = y_2(i), \ldots, y_{n(i)}(i)$. If $f(y) \in L[y]$ is a tame polynomial then Lemma 2 implies that f can be decomposed (over L) into polynomials which are indecomposable over L^*. Then Lemma 9 of [4] shows that these composition factors of f must be linear changes of polynomials of type (1.16) or (1.17).

If $f \in K(y)$, and (1.12) and (1.13) hold with L replaced by K, then Noether's lemma applies as in Theorem 1 of [4]. ∎

Let L be a finite field; $L\{\{1/x\}\}$ the ring of formal power series in $1/x$ with coefficients in L; $M = L((1/x))$ the quotient field of $L\{\{1/x\}\}$. We have the following exact sequence

$$1 \to G^{\mathrm{geom.}} \to G^{\mathrm{arith.}} \to G(L^*/L) \to 1 \tag{1.18}$$

where $G^{\mathrm{arith.}} = G(M^*/M)$, and $G^{\mathrm{geom.}} = G(M^*/L\ ((1/x)))$. Let $G^{\mathrm{arith.}}_{\mathrm{tame}}$ be the Galois group of the maximal tamely ramified subfield M_T of M^*. Then

$$M_T = \bigcup_{\substack{n \geqslant 1 \\ (n,p)=1}} L^*((1/x)^{1/n}).$$

Let $\sigma(F) \in G(L^*/L)$ be the Frobenius generator $a^q = \sigma(F)(a)$ for $a \in L^*$ (where q is the order of L). We define $\hat{\sigma}(F) \in G^{\mathrm{arith.}}_{\mathrm{tame}}$ to be the element obtained by operating on the coefficients of Puiseux expansions (elements of M_T) by $\sigma(F)$. We fix, once and for all, a *compatible system of primitive roots of* 1; that is, a collection $\{\zeta_n\}_{\substack{n \geqslant 1 \\ (n,p)=1}}$ where

$$\zeta_n \text{ is a primitive } n\text{th root of } 1, \tag{1.19}$$

and

$$(\zeta_{nm})^m = \zeta_n \quad \text{for all } n, m \text{ such that } (n \cdot m, p) = 1. \tag{1.20}$$

We define $\sigma(Br) \in G\big(M_T/L^*\big((1/x)\big)\big)$ by

$$\sigma(Br)(1/x)^{1/n} = (\zeta_n)^{-1}(1/x)^{1/n}. \tag{1.21}$$

Then $\hat{\sigma}(F)$ and $\sigma(Br)$ are topological generators of $G_{\text{tame}}^{\text{arith.}}$ with the single relation

$$\big(\sigma(Br)\big)^q \hat{\sigma}(F) = \hat{\sigma}(F)\sigma(Br). \tag{1.22}$$

Let $f(y) \in L[y]$. We introduce some concepts for the computation of the Galois closure of $L\big((1/x)\big)(y)$ over $L\big((1/x)\big)$ where $f(y) = x$. These computations are carried on extensively in [7], which contains a general treatment of wild ramification. Suppose $\deg f(y) = d = d(0)p^{v(0)}$ where $\big(d(0), p\big) = 1$. Write $\sum_{k=0}^{l} \big(f_k(y)\big)^{p^{v(k)}}$ where

$$\deg f_k = d(k), \quad \big(d(k), p\big) = 1, \tag{1.23}$$

and

(1.24) $p^{v(k)}$ is a strictly decreasing function of k, with $p^{v(l)} = 1$.

Such an expression for f is not unique.

Let $e(0)$ be the ordered two-tuple of integers, $\big(d(0)p^{v(0)}; p^{v(0)}\big)$ and define $e(i)$ inductively by

$$e(i) \overset{\text{def}}{=} \big(d(k_i)p^{v(k_i)}; p^{v(k_i)}\big) \tag{1.25}$$

where k_i is the least integer such that

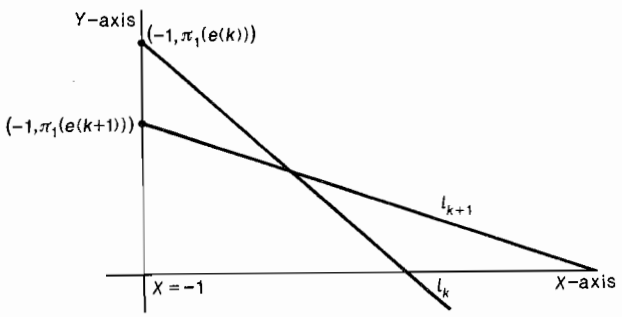
$$k_i > k_{i-1} \quad \text{and} \quad d(k_i)p^{v(k_i)} = \deg\Big(\sum_{k=k_{i-1}+1}^{l} \big(f_k(y)\big)^{p^{v(k)}}\Big).$$

Definition 6. We call the collection $\{e(i)\}_{i=0}^{s}$ (with its ordering by size of coordinates) the *ramification data* (over ∞) for the polynomial $f(y) \in L[y]$. See [7] or [16] for other interpretations of $\{e(i)\}_{i=0}^{s}$ (which in particular show that $\{e(i)\}_{i=0}^{s}$ is an invariant of the valuated fields $L\big((1/x)\big)(y)/L\big((1/x)\big)$. Let $\pi_1\big(e(i)\big)$ (respectively $\pi_2\big(e(i)\big)$) be the first (respectively the second) coordinate of $e(i)$.

Consider the lines

$$l_k : \; Y = \pi_1\big(e(k)\big) - (X+1)p^{v(k)}, \quad k = 0, \ldots, s. \tag{1.26}$$

Denote the



X-coordinate of the intersection of l_i and l_j by $I\big(e(i), e(j)\big)$. Let $E(0) = e(0)$ and define $E(i)$ inductively by

(1.27) $E(i) \stackrel{\text{def}}{=}$ the minimum of $e(k) < E(i-1)$ such that the minimum value of $I\big(E(i-1), e(k)\big)$ is achieved.

Then the ordered two-tuples

$$\Big\{\big(I(E_i, E_{i+1}); \pi_1(E_i) - \big(1 + I(E_i, E_{i+1})\big) \cdot \pi_2\big(E(i)\big)\big)\Big\}_{i=0}^{t-1}$$

are the 'corners' of the outer concave hull of the lines $\{l_k\}_{k=0}^{s}$. The collection $\{E(i)\}_{i=0}^{t}$ generalizes the notion of higher ramification indices. The following computation shows, in particular, that if $L\big((1/x)\big)(y)$ is Galois over $L\big((1/x)\big)$, then the quantities $I(E_i, E_{i+1})$ are higher ramification indices (so in this case, they are integers).

Let $\sigma\colon L^*\big((1/y)\big) \to \bigcup_{\substack{n \geqslant 1 \\ (n,p)=1}} L^*\big((1/y)^{1/n}\big)$ be a field embedding, fixed on $L^*\big((1/x)\big)$ such that for some integer $n \geqslant 1$

$$\sigma(y) = y + \sum_{i=-(n-1)}^{\infty} a_i y^{-i/n}. \tag{1.28}$$

From the equation

$$f\big(\sigma(y)\big) \equiv f(y) \tag{1.29}$$

we inductively solve for the coefficients $\{a_i\}_{i=-(n-1)}^{\infty}$. From (1.26) and (1.27) if

$$I\big(E(m), E(m+1)\big) \leqslant j/n < I\big(E(m+1), E(m+2)\big) \quad \text{for} \quad m \leqslant t-1,$$

then a_j appears in the term where y has coefficient $g(a_j)$ and exponent

$$\pi_1\big(E(m)\big) - \left(\frac{j}{n} + 1\right) \pi_2\big(E(m)\big) \tag{1.30}$$

in the left side of (1.29) (and a_j does not appear in the coefficient of a term of higher degree). In addition

$$g(a_j) = h\big(a_j^{\pi_2(E(m+1))}\big) \tag{1.31}$$

and h is a universal separable polynomial (dependent only on f) with coefficients in $L^*[a_{-(n-1)}, \ldots, a_{j-1}]$. Also h has the property that

$$\deg h = \begin{cases} \dfrac{\pi_2\big(E(m)\big)}{\pi_2\big(E(m+1)\big)} & \text{if} \quad j/n = I\big(E(m), E(m+1)\big), \\ 1, & \text{otherwise.} \end{cases} \tag{1.32}$$

PROPOSITION 1. *Let* $f(y) = \dfrac{p(y)}{q(y)} \in L(y)$ *be virtually-one-one over* L,

where p, q are relatively prime polynomials, and (as in (1.3))

$$\bar{n}(f) = \deg p - \deg q \geqslant 1.$$

Suppose

$$(\bar{n}(f), p) = 1. \tag{1.33}$$

Then

(1.34) *L contains no non-trivial $\bar{n}(f)$-th root of 1, and $q(y)$ has no zeros in L.*

In particular, since $-1 \in L$, $\bar{n}(f)$ is odd.

Assume now that $f(y) \in L[y]$ is virtually-one-one. Then (in the notation above)

(1.35) *the g.c.d. of $\pi_1(E(t-1)) - \pi_1(E(t))$ and $\pi_2(E(t-1)) - 1$ (where $\pi_2(E(t)) = 1$) is greater than 1.*

In particular, let $f(y) = y^{p^{v(0)} \cdot d(0)} + by^{d(1)} + $ lower terms, where $(d(0), p) = (d(1), p) = 1$, $b \neq 0$, and $v(0) \neq 0$.

Then, if f is virtually-one-one over L,

$$(d(0) - d(1), p^{v(0)} - 1) > 1. \tag{1.36}$$

Proof. From MacCluer's theorem (Theorem 1 of [8]) if $f(y)$ is virtually-one-one, then there is at most one L-rational place of $L(y)$ over the place $x = \infty$ (where $f(y) = x$). Since $\bar{n}(f) \geqslant 1$, $y = \infty$ is one such L-rational place. If $q(y)$ has a zero in L, then we would obtain an L-rational place by setting y equal to this zero. Thus, $q(y)$ has no zero in L.

Again, since $y = \infty$ in an L-rational place, one of the Puiseux expansions y_1, for $f(y) = x$ about this place, is an element of $L\left((1/ax)^{1/\bar{n}(f)}\right)$ for some $a \in L$. If L contains a non-trivial $\bar{n}(f)$th root of 1, then some conjugate of y_1 (say y_2) over $L((1/x))$ is also in $L\left((1/ax)^{1/\bar{n}(f)}\right)$. From Lemma 1, f virtually-one-one implies that

$$L(y_1, y_2) \cap L^* \neq L. \tag{1.37}$$

But this contradicts the fact that

$$L\left((1/ax)^{1/\bar{n}(f)}\right) \cap L^* = L.$$

Thus we have demostrated (1.34).

Now suppose that $f(y)$ is a virtually-one-one polynomial. We use the notation preceding Proposition 1. In (1.28), let $a_i = 0$ for $i < \omega \overset{\text{def}}{=} I(E(t-1), E(t))$. We set $\pi_u(E(t-1)) - \pi_u(E(t)) = r_u$ for $u = 1, 2$. We have $I(E(t-1), E(t)) = \dfrac{r_1}{r_2} - 1$. From the procedure described in expressions (1.28) through (1.32), there are $\pi_2(E(t-1))$ distinct solutions for a_ω, and inductively we solve uniquely for a_i for $i > \omega$. If $(r_1, r_2) = 1$, then some non-zero solution for a_ω corresponds to an element $y_2 \neq y_1$

where

$$y_2 \in L\left(\left((1/ay)^{1/r_2}\right)\right) \quad \text{for some constant } a \in L. \tag{1.38}$$

From Lemma 1, f virtually-one-one implies that

$$L(y_1, y_2) \cap L^* \neq L. \tag{1.39}$$

But this contradicts the fact that

$$L(y_1, y_2) \cap L^* \subseteq L\left(\left((1/ay)^{1/r_2}\right)\right) \cap L^* = L. \tag{1.40}$$

Thus we have demonstrated that (1.35) holds. ■

LEMMA 3. *Let $r > 1$ be any fixed integer. Then there exist only finitely many (dependent on r) integers n such that: n = degree f for some rational function $f \in L(y)$; and* $\deg q = r$ *where* $f = \dfrac{p(y)}{q(y)}$; *and* $\dfrac{f(y)-f(z)}{y-z}$ *has an irreducible factor of degree* 1 *or* 2.

Proof. Suppose $f(y) = f_1(f_2(y))$. The quantity $\overline{n}(f)$ is the ramification index of the place $y = \infty$ (of the function field $L^*(y)$) over the place $x = \infty$ (where $f(y) = x$). By linear fractional change of $z = f_2(y)$, we can guarantee that the place $y = \infty$ lies over the place $z = \infty$ in the function field $L^*(f_2(y))$. From the multiplicative properties of ramification indices, we obtain $\overline{n}(f_1)\cdot\overline{n}(f_2) = \overline{n}(f)$. Since $n - \overline{n}(f) = n_1 \cdot n_2 - -\overline{n}(f_1)\cdot\overline{n}(f_2) = r$, both n_1 and n_2 must be bounded. Thus, we may restrict our attention to indecomposable rational functions $f(y)$.

The case where $\dfrac{f(y)-f(z)}{y-z}$ has an irreducible factor of degree 1 is easily disposed of by noting that $f(y)$ must be linearly related to a cyclic polynomial. Now suppose $\dfrac{f(y)-f(z)}{y-z}$ has an irreducible factor of degree 2 (in both variables from the symmetry in y and z), say $\varphi_1(y, z)$. Let $f(y_1) = x$ and $\varphi_1(y_1, z_1) = 0$. Then the function field $L^*(y_1, z_1)$ is of genus zero. Thus there exists $t \in L^*(y_1, z_1)$ such that $L^*(t) = L^*(y_1, z_1)$. From $[L^*(t) : L^*(y_1)] = 2$ and $[L^*(t) : L^*(z_1)] = 2$, there exist automorphisms σ, τ of $L^*(t)$ such that the fixed field of σ is $L^*(y_1)$ and the fixed field of τ is $L^*(z_1)$. From Luroth's theorem composition factors of $f(y)$ correspond to the subfields of $L^*(y_1)$ containing $L^*(x)$. Thus, if $L^*(y_1) \cap L^*(z_1) \neq L^*(x)$, then f would be decomposable, contrary to assumption. Thus, we have shown that the fixed field in $L^*(t)$ of the group generated by σ and τ is $L^*(x)$. So $L^*(t)$ is the Galois closure of $L^*(y_1)/L^*(x)$. However, this implies that $G(\Omega_{f-x}/L^*(x))$ is a finite group of linear fractional transformations. From the characterization of such groups (see [2], Theorem 3, p. 133), excluding the case where f is a cyclic or Chebychev polynomial, there are only finitely many such groups. ■

THEOREM 2. *Let L be a finite field. Assume that $f(y) \in L(y)$ and that $f(y) = \dfrac{p(y)}{q(y)}$ with $(p, q) = 1$ is tame* (Definition 4). *In addition, assume that f is virtually-one-one over L. Then*

$$(1.41) \qquad \big(|L|-1, \overline{n}(f)\big) = 1, \quad \text{and} \quad q(y) \text{ has no zeros in } L.$$

Let $\sigma_\infty = (\overline{n})\big(s(2)\big) \dots \big(s(r)\big)$ be the branch cycle over ∞ for the curve $f(y) - x = 0$ over the x-sphere. Then either

$$(1.42) \qquad \overline{n}(f) < \deg q,$$

or

$$(1.43) \qquad \big(\overline{n}(f), s(i)\big) > 1 \quad \text{for} \quad i = 2, \dots, r.$$

COROLLARY 1. *With the same assumptions as Theorem 2, for*

$$(1.44) \qquad 1 \leqslant \text{degree } q \leqslant 9$$

there exist only finitely many values (independent of $|L|$) of $\overline{n}$ such that there exists $f \in L(y)$ satisfying the above conditions with $\overline{n}(f) = \overline{n}$.

Proof. We have $\big(|L|-1, \overline{n}(f)\big) = 1$ if and only if L contains no $\overline{n}(f)$th roots of 1 (other than 1). Thus (1.41) follows from Proposition 1. Now suppose neither (1.42) nor (1.43) holds. The numbers $s(2), \dots, s(r)$ are the multiplicities of the zeros of $q(y)$. Then there exists i (say $i = 2$) such that $(\sigma_\infty)^{s(2)}$ is fixed on one of the zeros of $f(y) - x$, and has a cycle of order $\overline{n}$ on $\overline{n}$ of the zeros of $f(y) - x$. Thus, one of the absolutely irreducible factors of $\varphi(y, z)$ (expression (1.41)) has degree at least $\overline{n}$. However, since f is virtually-one-one, there are at least two absolutely irreducible factors of $\varphi(y, z)$ of degree at least $\overline{n}$. By assumption $\overline{n}(f) \geqslant \deg q$ so $2\overline{n}(f) \geqslant \deg f$. However, $\deg_z\big(\varphi(y, z)\big) = \deg f - 1$ which contradicts our deduction that $\deg_z\big(\varphi(y, z)\big) \geqslant 2\overline{n}(f)$.

Now we prove the corollary. We exclude the finite number of values of $\overline{n}$ such that $\overline{n} \leqslant q$. We know from Proposition 1 that $\overline{n}(f)$ can never be even. Since we assume that

$$(1.45) \qquad \overline{n}(f) \geqslant \deg q,$$

then (1.43) holds. Also, since $q(y)$ can have no zeros over L, for each value of $2 \leqslant i \leqslant r$

$$(1.46) \qquad \text{there must exist } j \neq i \text{ such that } s(i) = s(j).$$

By simple combinatorics we can inspect the possible values of $s(2), \dots, s(r)$ for degree $q = 1, 2, 3, 4, 5, 7, 8$ to see that there do not exist corresponding rational functions f. Also, if

$$(1.47) \qquad \deg q = 6, \text{ then } s(2) = s(3) = 3,$$

and if

$$(1.48) \qquad \deg q = 9, \text{ then } s(2) = s(3) = s(4) = 3.$$

From Lemma 3 we see that there are only finitely many rational functions with $\deg q$ prescribed, such that $\varphi(y, z)$ has a factor of degree 1 or 2; and, in fact, these are easily delineated. The case (1.47) and (1.48) are similar, so we assume (1.48) holds. Then $\overline{n} = 3 \cdot k$ for some integer k. The permutation $(\sigma_\infty)^3$ has transitivity classes of length

$$k, k, k \underbrace{1, 1, \ldots, 1}_{9 \text{ times}} \tag{1.49}$$

on the zeros of $f(y) - x$. Let y_1 be a zero of $f(y) - x$. Then these 12 transitivity classes are subsets of the transitivity classes of $G\left(\Omega_{f-x}/L^*(y_1)\right)$ on the zeros of $f(y) - x$. Again we use that $\varphi(y, z)$ has at least two absolutely irreducible factors of degree t, if it has one of degree t (and $t \geqslant 3$).

Thus, for k large, we know that there are no transitivity classes of length 2 among $y_2, \ldots, y_n$ under the action of $G\left(\Omega_{f-x}/L^*(y_1)\right)$, and there must be as least two classes of a given length, if there is one class of that length. From this information we combinatorially see that the only possibility is that $G\left(\Omega_{f-x}/L^*(y_1)\right)$ has transitivity classes of length $k, k, k, 4, 4$ on $y_2, \ldots, y_n$. Let $y_1, \ldots, y_{\overline{n}}$ be zeros of $f(y) - x$ whose Puiseux expansions about the place $x = \infty$ start with $x^{1/\overline{n}}$. One of these (say y_1) is actually a Laurent series in $x^{-1/\overline{n}}$ with coefficients in L (versus in L^*). Then, as in (1.18) through (1.22), the action of the Frobenius symbol $\hat{\sigma}(F)$ is obtained by operating on the coefficients of the Puiseux expansions, and $\hat{\sigma}(F)$ represents an element of $G\left(\Omega_{f-x}/L(y_1)\right)$. If $k > 4$, $\hat{\sigma}(F)$ is transitive on the three transitivity classes of length k; transitive on the two transitivity classes of length 4; and maps the collection $y_2, \ldots, y_{\overline{n}}$ into itself. Suppose one of the transitivity classes of length k (under the action of $G\left(\Omega_{f-x}/L^*(y_1)\right)$) contains $k - t$ members of the set $\{y_2, \ldots, y_{\overline{n}}\}$. Then so does each of the other transitivity classes of length k. Also, each of the transitivity classes of length 4 contains $3t/2$ members of the set $\{y_2, \ldots, y_{\overline{n}}\}$. Thus t is even, and $t = 0$ or 2. However, among the remaining nine zeros of $f(y) - x$, an odd number must appear among the three transitivity classes of length k. This is a contradiction to t even; and finishes the case $\deg q = 9$. ■

EXAMPLE 1. In Section VIII of [16] we describe all virtually-one-one prime degree polynomials over L. For now, we give one example where f is not a composition of cyclic and Chebychev polynomials, but is virtually-one-one over L. Take $L = \boldsymbol{Z}/(5)$. Then L does not contain $\sqrt{2}$. Let $f(y) = y^5 - y^3 + 2y^2 + y$. We obtain

$$\varphi(y, z) = \left((y-z)^2 + \sqrt{2}(y+z) + \frac{1-\sqrt{2}}{2}\right)\left((y-z)^2 - \sqrt{2}(y+z) + \frac{1+\sqrt{2}}{2}\right).$$

In the next set of problems K denotes an algebraic number field.

PROBLEM 1. From Theorem 1, if $f(y) \in K[y]$ is virtually-one-one over $\mathrm{Res}(\mathcal{O}_K, C)$ for all $C > 0$ (where $\mathcal{O}_K$ is the ring of integers of K), then f is a composition of polynomials of type (1.16) and (1.17). Does the same conclusion follow if $f(y) \in K[y]$ is virtually-one-one over K?

PROBLEM 2. Let $r \geqslant 1$ be any integer. Can Theorem 2 be strengthened to: there exist only finitely many integers $\bar{n}$ (dependent on r) such that there exist tame rational virtually-one-one functions $f(y) = \dfrac{p(y)}{q(y)} \in L(y)$ with $\deg q = r$, $\bar{n} = \bar{n}(f)$. The reader will note that the combinatorial arguments used in the proof of Theorem 2 are applicable to the case $\deg q \geqslant 10$. But they do not suffice to demonstrate Theorem 2. The case $\deg q = 10$ itself is tractable by making some arithmetic observations. However, we have not yet found the proper abstract setup (for general function fields) whereby these computations become a simple special case.

2. Decomposability of rational functions. In this section we consider rational functions $f(y) \in L(y)$ where

(2.1) f is indecomposable over L, but f is decomposable over L^*.

For most of this section L could be any perfect field. From Lemma 2, either

(2.2) f is not a polynomial,

or

(2.3) $(\mathrm{Char}\, L, \deg f) \neq 1$.

For a general function field $K(Y)/K(x)$ (as in the introduction), the condition of indecomposability corresponds to the condition that $G(\widehat{K(Y)/K(x)})$ is a primitive permutation group when represented on the letters $y_1, \ldots, y_n$ (Lemma 2 of [4]).

The general treatment of condition (2.1) is difficult, and is a source of arithmetic problems (versus purely group theoretic or Riemann surface type problems). We shall in order: normalize the problem, indicate important special cases and related problems, and then give some results related to some of the special cases. The purely combinatorial aspects of these problems are left here and taken up again in [6].

Suppose $f = f_1(f_2) \in L(y)$ where $f_1, f_2 \in L^*(y)$. By replacing f by a linear fractional transformation of f we may assume that $\bar{n}(f) > 0$. Similarly, there is a linear fractional transformation $u(f_2)$ (of f_2) such that $\bar{n}(u(f_2)) > 0$. So, by replacing f_2 by $u(f_2)$ and f_1 by $f_1(u^{-1}(y))$ we may assume

(2.4) $\bar{n}(f_1) > 0, \quad \bar{n}(f_2) > 0$.

For questions about value sets of rational functions these are assumptions we may make with no loss.

The proof of Lemma 2 shows that if $f(y) \in L[y]$ and $(\deg f, \text{char } L) = 1$, then

(2.5) there exist $a, b \in L^*$ such that $af_2(y) + b \in L[y]$.

DEFINITION 7. We say that $f \in L(y)$ is *decomposably stable* if there is a one-one correspondence between the lattice of fields between $L(x)$ and $L(f(x))$ and those between $L^*(x)$ and $L^*(f(x))$.

Our next examples are not decomposably stable, but they do not satisfy (2.1).

EXAMPLE 2. In this example $f(y) = y(y^{p+1}-1)^{p-1} \in L[y]$ where $L = \mathbf{Z}/(p)$ (p a rational prime). Then $f(y) = f_1(f_2(y))$ with $f_1(y) = y - y^2 + \ldots + y^p$, $f_2(y) = y + y^2 + \ldots + y^p$. But, for a any $(p+1)$th root of 1, we also have $f(y) = \frac{1}{a}(f(ay))$. Thus, $f = g_1(g_2(y))$ where $g_1 = \frac{1}{a} f_1(y)$, and $g_2(y) = f_2(ay)$.

EXAMPLE 3. Here L is any field not containing a primitive 3rd root of 1, which we call a. Let

$$f_1 = \frac{1}{a}\left(\frac{y^2-4}{y-1}\right), \qquad f_2 = \frac{a^2y^2+2}{ay+1}$$

so

$$f_1(f_2) = f(y) = y\left(\frac{y^3-8}{y^3+1}\right).$$

As in Example 2 we also have

$$f(y) = g_1(g_2(y)) \quad \text{where} \quad g_1 = \frac{y^2-4}{y-1},\ g_2 = \frac{y^2+2}{y+1} \in L(y).$$

We now consider

(2.6) *Classes of Pairs of Rational Functions*

f, g such that: $f, g \in L^*(y)$, $f(y_1) = x$, $g(z_1) = x$ and $L^*(y_1, z_1)$ is of genus zero; and either

a) $f(y) - g(z)$ is irreducible as a rational function in y and z (so the genus of $L^*(y_1, z_1)$ does not depend on the choice of z_1);

b) Given a choice of y_1 the genus of $L^*(y_1, z_1)$ may depend on the choice of the zero z_1 of $g(z) = x$; or

c) f, g rational functions such that there exists $\sigma \in G(L^*/L)$ with $f^\sigma(y) = g(y)$.

Remark 2. Certain sub-classes of the problem (2.6) b) have been treated in the literature ([12], for example). However, the very proliferation of examples seems to demand a method of keeping track, of the information obtained by computation, which does not exist. Assumption (2.6) a) is more tractable, especially if f and g are polynomials (see [6] and also Example 5)). Let $f_1, f_2 \in L^*(y)$ satisfy $f_1(f_2) = f(y) \in L(y)$, where

f is indecomposable over L. Then there exists $\sigma \in G(L^*/L)$ such that $f_1^\sigma(f_2^\sigma(y)) = f(y)$ and $f_2^\sigma \neq f_2$. Let $x = f(y_1)$, so that we have $L^*(y_1) \supset L^*(f_2^\sigma(y_1), f_2(y_1)) \supset L^*(x)$. By Luroth's theorem $L^*(f_2^\sigma(y_1), f_2(y_1))$ is of genus zero. Since $f_2^\sigma(y_1)$ is a zero of $f_1^\sigma(y) - x$, and $f_2(y_1)$ is a zero of $f_1(y) - x$, we have the situation of (2.6) c).

Let $f, g \in L(y)$ with $f(y_1) = x$ and $g(z_1) = x$. Let $\lambda_1, \ldots, \lambda_r, \lambda_\infty$ be the branch points of $L^*(y_1, z_1)$ over $L^*(x)$. Assume that f, g are tame, as in Definition 4. We denote by $\sigma_1, \ldots, \sigma_r, \sigma_\infty$ the corresponding branch cycles viewed as elements of $G(\Omega_{f-x} \cdot \Omega_{g-x}/L^*(x))$. It is desirable to view the action of the branch cycles on Ω_{f-x} and Ω_{g-x} separately. We let $\sigma_i(y)$ (respectively $\sigma_i(z)$) denote the restriction of σ_i to Ω_{f-x} (respectively Ω_{g-x}) and by abuse of notation we let

$$\sigma_j(y) = (s(j,1)) \ldots (s(j,k_j)), \qquad \sigma_j(z) = (t(j,1)) \ldots (t(j,l_j)), \qquad j = 1, \ldots, r, \infty. \tag{2.7}$$

DEFINITION 8. We say f, g have the *same branching* if $\sigma_j(y)$ is similar to $\sigma_j(z)$ for $j = 1, \ldots, r, \infty$.

PROPOSITION 2. *Let $f, g \in L(y)$ and assume that*

$$f(y) - g(z) \text{ is absolutely irreducible.} \tag{2.8}$$

Then (in the above notation), the genus of $L(y_1, z_1)$ is given by p where

$$2(\deg f + p - 1) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \operatorname{ind}(\sigma_i^{t(i,j)}(y)) + \sum_{j=1}^{l_\infty} \operatorname{ind}(\sigma_\infty^{t(\infty,j)}(y)). \tag{2.9}$$

In particular, if $f, g \in L[y]$, then

$$2(\deg f + p - 1) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \operatorname{ind}(\sigma_i^{t(i,j)}(y)) + n - (n, m) \tag{2.10}$$

where $m = \deg g$.

Suppose f satisfies

$$\frac{f(y) - f(z)}{y - z} \text{ is absolutely irreducible.} \tag{2.11}$$

Then, if y_1, y_2 are zeros of $f(y) - x$, the genus of $L(y_1, y_2)$ is given by p where

$$2(\deg f + p - 2) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \operatorname{ind}(\sigma^{s(i,j)}(y)) + \sum_{j=1}^{l_\infty} \operatorname{ind}(\sigma_\infty^{s(\infty,j)}(y)). \tag{2.12}$$

Proof. From (2.8), $[L(y_1, z_1) : L(z_1)] = \deg f$. The Riemann–Hurwitz formula gives the genus of $L(y_1, z_1)$ as p where

$$2(\deg f + p - 1) = \sum (e(\mathfrak{p}) - 1) \tag{2.13}$$

where the summation is over places of $L^*(y_1, z_1)$ and $e(\mathfrak{p})$ is the ramification index of such a place over $L(z_1)$. Let $\mathfrak{p}$ be a place of $L^*(y_1, z_1)$. If $\mathfrak{p}$ is ramified over $L^*(x)$, then $\mathfrak{p}$ lies above one of the branch points (say λ_1) of $L(y_1, z_1)$ over $L(x)$. Let $\bar{\mathfrak{p}}$ (respectively $\bar{\bar{\mathfrak{p}}}$) be the restriction of $\mathfrak{p}$ to $L(y_1)$ (respectively $L(z_1)$). Then $\bar{\mathfrak{p}}$ (respectively $\bar{\bar{\mathfrak{p}}}$) has ramification index $s(1, u)$ for some $1 \leqslant u \leqslant k_1$ (respectively $t(1, v)$ for some $1 \leqslant v \leqslant l_1$). We compute

$$e(\mathfrak{p}) - 1 = \frac{[s(1, u), t(1, v)]}{t(1, v)} - 1. \tag{2.14}$$

The sum over places lying over λ_1 is easily seen to be $\sum_{j=1}^{l_1} \operatorname{ind} \sigma^{i(1,j)}(y)$. Formula (2.9) is obtained by summing over all places $L^*(x)$ and substituting in (2.13).

If $f, g \in L[y]$, then $\sigma_\infty(y) = n$-cycle, and $\sigma_\infty(z) = m$-cycle. Thus,

$$\sum_{j=1}^{l_\infty} \operatorname{ind}\left(\sigma_\infty^{i(\infty,j)}(y)\right) = \left(\frac{n}{(n, m)} - 1\right)(n, m). \tag{2.15}$$

This proves (2.10).

Suppose f satisfies (2.11). Then $[L(y_1, y_2) : L(y_1)]$ is $n-1$. The argument above applies almost without change to $L(y_1, y_2)$ to give (2.12). ■

The following corollary (expression (2.27)) shows that under the conditions of problem (2.6) a) there is a great deal of ramification over just one place on the x-sphere for the covers given by $f(y) - x$ and $g(z) - x$.

COROLLARY 2. *Let $f, g \in L(y)$ satisfy* (2.8). *Suppose also that*:

(2.16) *neither f nor g are cyclic or Chebychev polynomials, nor is f or g a polynomial of degree n where $n \leqslant 8$ (see Example* 4),

and

(2.17) $L^*(y_1, z_1)$ *is of genus zero.*

For $r \in \mathbf{Z}$ let

$$\tilde{r} = \begin{cases} r & \text{if } r > 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then, there exists a finite index i and a finite index j (possibly $i = j$) such that:

$$n - \sum_{u=1}^{k_i} \tilde{s}(i, u) = 0 \text{ or } 1, \quad \text{and} \quad m - \sum_{v=1}^{l_j} \tilde{t}(j, v) = 0 \text{ or } 1. \tag{2.18}$$

Suppose f satisfies (2.11), *and*

(2.19) $L^*(y_1, y_2)$ *is of genus zero.*

Then, for any $g \in L^*(y)$ *with the same branching as* f *(see Definition* 8*) we must have*

(2.20) $f(y)-g(z)$ *is reducible as a rational function in two variables.*

Suppose f *satisfies* (2.11), *and*

(2.21) $L^*(y_1, y_2)$ *is of genus* 1.

Then, for any $g \in L^*(y)$ *with the same branching as* f, *either* (2.20) *holds, or*

(2.22) $L^*(y_1, z_1)$ *is of genus zero where* $g(z_1) = x$.

Proof. Suppose $m - \sum_{u=1}^{l_j} \tilde{t}(j, u) \geqslant 2$ for all j. Since $p = 0$ is the genus of $L^*(y_1, z_1)$, we have $2(\deg f - 1) \geqslant \sum_{i=1}^{r} 2 \operatorname{ind}(\sigma_i(y))$ with equality iff

(2.23) $$m - \sum_{u=1}^{l_j} \tilde{t}(j, u) = 2 \quad \text{for all } j \text{ such that } \sigma_j(y) \neq 1;$$

(2.24) a) $\operatorname{ind}(\sigma_\infty(y)) = \deg f - 1$

(from $2(\deg f - 1) = \sum_{i=1}^{r} \operatorname{ind} \sigma_i(y) + \operatorname{ind} \sigma_\infty(y)$), and

b) $\sigma_j^{\tilde{t}(j,u)}(y) = 1$ for $u = 1, \ldots, l_j$ and all j such that $\sigma_j(y) \neq 1$ (this includes $j = \infty$, where we may replace $\tilde{t}(j, u)$ by $t(j, u)$ in this expression).

However, we must have equality in the above because

$$\sum_{i=1}^{r} \operatorname{ind}(\sigma_i(y)) \geqslant (\deg f - 1)$$

with equality if and only if $\operatorname{ind}(\sigma_\infty(y)) = \deg f - 1$ (or, equivalently, f is a polynomial).

For any j such that $\sigma_j(y) \neq 1$, we easily compute from (2.23) that

(2.25) $$\operatorname{ind}(\sigma_j(z)) \geqslant \frac{m-2}{2}.$$

We will now show that f has at most 2 finite branch points, and that $s(i, u) = 1$ or 2 for all i and u unless f or g yield one of the cases of Example 4. From Lemma 9 of [4], excluding this latter possiblity, f is a cyclic or Chebychev polynomial (this includes the case when f is a polynomial with two finite branch points whose corresponding cycles are of type $(1)(1)(2) \ldots (2)$ and $(2)(2) \ldots (2)$). This will conclude the demonstration of (2.18).

With the roles of f and g switched in the above discussion, we obtain

$$2(\deg g-1) \geqslant \sum_j \Big(n - \sum_{u=1}^{k_j} \tilde{s}(j,u)\Big)\big(\mathrm{ind}(\sigma_j(z))\big) + \mathrm{ind}(\sigma_\infty^n(z)). \tag{2.26}$$

From (2.25) we see that

$$\sum_{j=1}^{r}{}'' \Big(n - \sum_{u=1}^{k_j} \tilde{s}(j,u)\Big) \leqslant 4\left(\frac{m-1}{m-2}\right) \tag{2.27}$$

where $\sum_{j=1}^{r}{}''$ indicates that the sum is over all j such that $\sigma_j(y) \neq \mathrm{Id}$.

Let $\mathrm{tr}\ \sigma_i(y)$ be the number of fixed points of σ_i acting on $y_1, \ldots, y_n$. Then $\big(n - \sum_{u=1}^{k_j} \tilde{s}(j,u)\big) = \mathrm{tr}\ \sigma_j(y)$. From (2.27) we have

$$\sum_{j=1}^{r} \mathrm{tr}(\sigma_j(y)) \leqslant 4\left(\frac{m-1}{m-2}\right). \tag{2.28}$$

From (2.16) we may exclude m with $m \leqslant 6$ to obtain

$$\sum_{j=1}^{r} \mathrm{tr}(\sigma_j(y)) \leqslant 4. \tag{2.29}$$

Also, by the Riemann–Hurwitz formula applied to $L(y_1)/L(x)$ we obtain

$$\sum_{i=1}^{r}\sum_{u=1}^{k_i} \big(s(i,u)-1\big) + n - 1 = 2(n-1). \tag{2.30}$$

In particular,

$$\sum_i \frac{n - \mathrm{tr}(\sigma_i(y))}{2} \leqslant n-1$$

with equality iff $r = 2$ and $\sigma_i(y)$ is of order 2 for $i = 1, 2$. This latter is the Chebychev polynomial case (excluded by (2.16)). In either case we easily deduce $r = 2$. Assume $\mathrm{tr}(\sigma_1(y)) \leqslant \mathrm{tr}(\sigma_2(y))$ (with no loss). We have 3 cases:

a) $\mathrm{tr}(\sigma_1(y)) = 0$, $\mathrm{tr}(\sigma_2(y)) \leqslant 4$;
b) $\mathrm{tr}(\sigma_1(y)) = 1$, $\mathrm{tr}(\sigma_2(y)) \leqslant 3$; and
c) $\mathrm{tr}(\sigma_1(y)) = 2$, $\mathrm{tr}(\sigma_2(y)) = 2$.

In all cases, if two of the values $s(i,u)$ are different from 1 or 2, these values must be 3. However, if just one value is distinct from 1 or 2, this value must be 4. All cases are much the same (but time consuming). We illustrate one case, leaving the remainder to the reader.

Assume, for example, case b) where $\sigma_1(y)$ is of order 2 and

$\sigma_2(y) = (3)(3)(2)\dots(2)(1)(1)(1)$. Then, with the roles of g and f switched in (2.10) we obtain:

$$2(n-1) = \sum_{i=1}^{2}\sum_{j=1}^{l_i} \operatorname{ind}\left(\sigma_i^{t(i,j)}(y)\right) + n - (n, m). \tag{2.31}$$

But

$$\operatorname{ind}\,\sigma_1^{t(1,j)}(y) = \begin{cases} \dfrac{n-1}{2} & \text{if} \quad t(1,j) \text{ is odd,} \\ 0 & \text{if} \quad t(1,j) \text{ is even} \end{cases}$$

and

$$\operatorname{ind}\,\sigma_2^{t(2,j)}(y) = \begin{cases} 4 & \text{if} \quad t(2,j) \text{ is divisible by 2, but not 3,} \\ \dfrac{n-9}{2} & \text{if} \quad t(2,j) \text{ is divisible by 3, but not 2,} \\ \dfrac{n-1}{2} & \text{if} \quad \left(t(2,j), 6\right) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

This shows that $\operatorname{tr}\left(\sigma_1(z)\right) + \operatorname{tr}\left(\sigma_2(z)\right) \leqslant 4$ and $(n, m) = n$. Now g is a cyclic or Chebychev polynomial if $\operatorname{tr}\left(\sigma_1(z)\right) + \operatorname{tr}\left(\sigma_2(z)\right) \leqslant 2$. Thus, from previous computations, g has the same branch cycles as does f. For $n = m > 8$ we compute that the right side of (2.31) is greater than the left.

Assume $f \in L^*(y)$ satisfies (2.11) and (2.19) and suppose there exists g with the same branching as f such that $f(y) - g(z)$ is irreducible. An interpretation of the fact that f and g have the same branching is given by $t(i, u) = s(i, u)$ for all i and u. The right sides of (2.9) and (2.12) are the same. The p in the left side of (2.9) (resp. (2.12)) is the genus of $L^*(y_1, z_1)$ (resp. $L^*(y_1, y_2)$). However, since $p = 0$ in (2.12), we deduce that $L^*(y_1, z_1)$ has genus -1. This contradiction shows that $f(y) - g(z)$ is reducible. The remainder of the Corollary follows from an analogous argument. ■

We now give some examples to illustrate the non-triviality of classifying rational functions satisfying (2.6).

PROPOSITION 3. *Let $f, g \in L^*[y]$ be tame polynomials. Suppose*

(2.30) *$f(y) - g(z)$ is reducible as a polynomial in two variables,*

and

(2.31) *f is indecomposable over L^*.*

Suppose there does not exist $h(y) \in L^*[y]$ *with* $\deg h > 1$ *such that* $g(y) \equiv g_1(h(y))$ *and* $f(y) - g_1(z)$ *is reducible. Then:*

(2.32) g *is indecomposable and* $\Omega_{f-x} = \Omega_{g-x}$,

(2.33) g *and* f *have the same branching, and either* $f(ay+b) = g(y)$ *for the same* $a, b \in L^*$

or,

(2.34) $f(y) - g(z)$ *has exactly two irreducible factors of degree* s *and* $n-s$ *where* $n-1 \mid s(s-1)$.

Since these two factors have distinct degrees (*because* $n-1 \nmid \frac{n}{2}\left(\frac{n}{2}-1\right)$) *if* $f, g \in L[y]$ *as above, then the irreducible factors of* $f(y) - g(z)$ *are absolutely irreducible over* L (Theorem 1 of [5]).

EXAMPLE 4. We give two examples of polynomial pairs f, g that satisfy (2.6) a). These examples are part of the excluded situation of (2.16) in Corollary 2.

I) Let the Riemann surface for $f(y) - x$ have branch cycles

(2.35) $\sigma_1(y) = (y_1 y_2 y_4 y_6)$ (over $x = \lambda_1$), $\sigma_2(y) = (y_3 y_4)(y_5 y_6)$ (over $x = \lambda_2$),

and let the Riemann surface for $g(z) - x$ have branch cycles

(2.36) $\sigma_1(z) = (z_1 z_3 z_4 z_6)$ (over $x = \lambda_1$), $\sigma_2(z) = (z_2 z_3)(z_5 z_6)$ (over $x = \lambda_2$).

If $f(y)$ of degree 6 were decomposable, then Lemma 2 of [4] implies that either $\{y_1 y_4\}$, $\{y_2 y_5\}$, $\{y_3 y_6\}$ or $\{y_1 y_3 y_5\}$, $\{y_2 y_4 y_6\}$ would be sets of imprimitivity for σ_1 and σ_2. We are using the fact that $\sigma_1(y) \cdot \sigma_2(y) = (y_1 \dots y_6)$ and similarly $\sigma_1(z) \cdot \sigma_2(z) = (z_1 \dots z_6)$. However, $\sigma_2(y)$ fixes y_1 and moves y_3 to y_4, so neither system yields sets of imprimitivity. Thus, we may apply Proposition 3 to deduce from (2.30) that $f(y) - g(z)$ is irreducible. A simple computation using (2.9) shows that the genus of $C(y_1, z_1)$ is zero.

II) Here we have $\deg f = \deg g = 8$. Let the Riemann surface for $f(y) - x$ have branch cycles

(2.37) $\sigma_1(y) = (y_1 y_2 y_8)(y_3 y_5 y_7)$ (over $x = \lambda_1$) and
$\sigma_2(y) = (y_3 y_8)(y_4 y_5)(y_6 y_7)$ (over $x = \lambda_2$).

Let the Riemann surface for $g(z) - x$ have branch cycles

(2.38) $\sigma_1(z) = (z_1 z_3 z_8)(z_4 z_5 z_7)$ (over $x = \lambda_1$) and
$\sigma_2(z) = (z_2 z_3)(z_4 z_8)(z_6 z_7)$ (over $x = \lambda_2$).

We leave to the reader the proof of the fact that f is indecomposable. Proposition 3 ((2.30)) then implies that $f(y)-g(z)$ is irreducible, since $7 \mid s(s-1)$ implies that $s = 7$ or $s = 1$. Again (2.9) may be used to show that $\boldsymbol{C}(y_1, z_1)$ is of genus zero.

EXAMPLE 5. We now give an example of polynomials $f, g \in \boldsymbol{C}[y]$ such that $\deg f = \deg g = 7$ and $f(y)-g(z)$ is reducible where $\boldsymbol{C}(y_1, z_1)$ is of genus zero for some z_1 such that $g(z_1) = x$. We highlight certain relevant points here. The production of polynomial pairs f, g such that $f(y)-g(z)$ is reducible is not in general an easy task. However, if $f(y)-x$ has branch cycles of the form

$$\sigma_1(y) = (2)(2), \quad \sigma_2(y) = (3)(3) \tag{2.39}$$

then f is not a cyclic or Chebychev polynomial and $\dfrac{f(y)-f(z)}{y-z}$ is absolutely irreducible (Lemma 9 of [4]). From (2.11) the field $\boldsymbol{C}(y_1, y_2)$ is of genus zero. By Corollary 2 (expression (2.20)) if f and g have the same branching, then $f(y)-g(z)$ is reducible. It is not difficult to find two (inequivalent) polynomials f and g with branching of form (2.39). From Proposition 3, if $f(y)-g(z)$ is reducible where $\deg f = \deg g = 7$, then $\Omega_{f-x} = \Omega_{g-x}$. Therefore, the branch cycles for the Riemann surface of $f(y)-x$ can also be represented on $z_1, \ldots, z_7$ (where z_i is given by the set $\{y_i, y_{i+1}, y_{i+3}\}$, $i = 1, \ldots, 7$).

Consider the case:

$$\begin{aligned} \sigma_1 &= (y_1y_3)(y_4y_5) = (z_1z_2)(z_3z_5), \\ \sigma_2 &= (y_2y_3)(y_4y_7) = (z_1z_7)(z_3z_6), \\ \sigma_3 &= (y_1y_4)(y_6y_7) = (z_3z_7)(z_4z_5). \end{aligned} \tag{2.40}$$

The group generated by $\sigma_1, \sigma_2, \sigma_3$ has two permutation representations. We construct (by Riemann's existence theorem) a polynomial f of degree 7 having $\sigma_1(y), \sigma_2(y), \sigma_3(y)$ as finite branch cycles. The stabilizer of z_1 in $G\left(\Omega_{f-x}/\boldsymbol{C}(x)\right)$ has as its fixed field the field $\boldsymbol{C}(z_1)$ where z_1 is a zero of $g(z)-x$. Here g is the polynomial with the same finite branch points as f, and $g(z)-x$ has branch cycles $\sigma_1(z), \sigma_2(z), \sigma_3(z)$. Since the group $G\left(\Omega_{f-x}/\boldsymbol{C}(y_1)\right)$ is of order relatively prime to 7, it is intransitive on $z_1, \ldots, z_7$. Thus $f(y)-g(z)$ is reducible. However, neither of the curves defined by the irreducible factors of $f(y)-g(z)$ is of genus zero. We must "coalesce" the branch points to obtain such examples. Denoting the branch points in order by $\lambda_1, \lambda_2, \lambda_3$ we obtain two distinct examples by first coalescing λ_1 and λ_2, then by coalescing λ_2 and λ_3. These are:

$$\begin{aligned} \sigma_1 &= (y_1y_2y_3)(y_4y_5y_7) = (z_1z_2z_7)(z_3z_5z_6), \\ \sigma_2 &= (y_1y_4)(y_6y_7) = (z_3z_7)(z_4z_5), \end{aligned} \tag{2.41}$$

and

$$\sigma_1 = (y_1y_3)(y_4y_5) = (z_1z_2)(z_3z_5),$$
$$\sigma_2 = (y_1y_4y_6y_7)(y_2y_3) = (z_1z_3z_6z_7)(z_4z_5). \tag{2.42}$$

In all these examples,

$$G\big(\Omega_{f-x}/\boldsymbol{C}(z_1)\big) \text{ is transitive on the set } \{y_1, y_2, y_4\}.$$

The genus of $\boldsymbol{C}(z_1, y_1)$ is easily computed. It is found to be $p = 1$ in case (2.41) and $p = 0$ in case (2.42). From Riemann's existence theorem there exist polynomials $h(y)$ of degree 7 such that the Riemann surface for $h(y)-x$ has branching of form

$$\sigma_1 = (2)(2), \quad \sigma_2 = (4)(2), \quad \text{(distinct from (2.42))}. \tag{2.43}$$

However, in this case, for $l(y) \in \boldsymbol{C}[y]$ such that $\deg l = \deg h$ and

$$h(y)-l(z) \text{ is reducible}, \tag{2.44}$$

then $l(ay+b) = h(y)$ for some $a, b \in \boldsymbol{C}$.

For example, we can take $h(y)$ to be the polynomial such that the Riemann surface for $h(y)-x$ (over $\boldsymbol{C}(x)$) has branch cycles

$$\sigma_1 = (y_4y_7)(y_6y_5), \quad \sigma_2 = (y_1y_2y_3y_4)(y_5y_7) \tag{2.45}$$

where $y_1, \ldots, y_7$ are zeros of $h(y)-x$. If $h(y)-l(z)$ were reducible, then Proposition 3 implies that $\Omega_{l-x} = \Omega_{h-x}$ and $G\big(\Omega_{l-x}/\boldsymbol{C}(z_1)\big)$ is intransitive on $y_1, \ldots, y_7$. This is easily seen to be false. The genus of $\boldsymbol{C}(y_1, z_1)$ is 0 by formula (2.10) if $l(y)$ has the same branching as $h(y)$.

Remark 3. The examples above do not exhaust the list of relevant examples to problems (2.6) (see [6]). However, as far as the generalized Schur conjecture is concerned, we should make a few more comments.

Example 6. Case (2.42) does yield polynomial pairs f, g such that $f^\sigma = g$ for some $\sigma \in G(\boldsymbol{Q}^*/\boldsymbol{Q})$ and $M = \boldsymbol{Q}^*(y_1, z_1)$ is of genus zero (see [5], Theorems 1 and 2). Thus we have examples of (2.6) c). However, it can be shown that in this case we cannot find a field $M' \supset \boldsymbol{Q}(x)$ such that M' is defined over the fixed field of σ and $\boldsymbol{Q}^* \cdot M' = M$. Such a field M' would have to exist for these examples to yield rational functions which are indecomposable over the fixed field of σ, but decomposable over $\boldsymbol{Q}^*$. We do not know that Example 4 does yield the situation of (2.6) c).

3. Rational functions of prime degree. In this section we use a trick involving the Weierstrass $\wp$-function (first employed by Ritt in [12]) to help us delineate the rational functions $f(y) \in \boldsymbol{C}(y)$ such that

$$\deg f = p \quad \text{for some prime } p, \tag{3.1}$$

and

$$G\big(\Omega_{f-x}/\boldsymbol{C}(x)\big) \text{ is not doubly transitive on } \{y_i\}_1^p, \text{ the zeros of } f(y) = x. \tag{3.2}$$

From Theorem 1, all tame virtually-one-one rational functions of prime degree must be among these.

Lemma 4 is due to Burnside [1] and Lemma 5 is similar to Lemma 9 of [4].

LEMMA 4. *If G is a group of prime degree p and G is not doubly transitive, then G (as a permutation group) is a subgroup of the group of linear transformations of the integers modulo p. In particular $|G| \mid p(p-1)$.*

LEMMA 5. *Let $f(y) \in \boldsymbol{C}(y)$ be such that* (3.1) *and* (3.2) *hold. Let $\sigma_1, \ldots, \sigma_r$ denote the branch cycles for the Riemann surface of $f(y)-x$ over the x-sphere. For this lemma we do not differentiate between the finite and infinite branch points. Thus $\prod_{i=1}^{r} \sigma_i = 1$. Let a_i be the order of σ_i for $i = 1, \ldots, r$. Then, one of the following must occur. In some order:*

(3.3) $r = 4$ *and* $a_1 = a_2 = a_3 = a_4 = 2$

or

(3.4) $r = 3$ *and* a) $a_1 = a_2 = a_3 = 3$, *or* b) $a_1 = 2$, $a_2 = 3$, $a_3 = 6$, *or* c) $a_1 = 2$, $a_2 = 4$, $a_3 = 4$, *or* d) $a_1 = 2$, $a_2 = 2$, $a_3 = p$

or

(3.5) $r = 2$ *and* $a_1 = p$, $a_2 = p$.

Proof. By Lemma 4, (3.2) implies that $G = G\left(\Omega_{f-x}/\boldsymbol{C}(x)\right)$ is a subgroup of the group of linear transformations of the integers modulo p. From properties of this latter group we deduce that for each $i = 1, \ldots, r$, either

(3.6) $a_i = p$,

or

(3.7) σ_i fixes one letter and is a product of disjoint cycles of length a_i where $a_i \mid p-1$.

If (3.6) occurs for any integer i, then λ_i (the branch point corresponding to σ_i) is a totally ramified place of the Riemann surface of $f(y)-x$, and by a linear fractional change of the variable x we may assume $\lambda_i = \infty$. Thus f may be assumed, in this case, to be a polynomial of degree p. This is treated in Lemma 9 of [4]. So we may assume that (3.6) does not hold. Then from (3.7) the Riemann–Hurwitz formula gives

$$\sum_{i=1}^{r} \operatorname{ind} \sigma_i = \sum_{i=1}^{r} \left(\frac{p-1}{a_i}\right)(a_i - 1) = 2(p-1), \tag{3.8}$$

or

$$\sum_{i=1}^{r} \frac{(a_i - 1)}{a_i} = 2. \tag{3.9}$$

Easily we deduce that $3 \leqslant r \leqslant 4$ with $r = 4$ if and only if $a_1 = a_2 = a_3 = a_4 = 2$. As for the case $r = 3$, for each i, $a_i \leqslant 6$. This leaves only finitely many cases to check, and the valid cases are exactly those described in the Lemma. ■

In Theorem 3 we exclude the case where f is a polynomial since that case is handled in [4]. We denote by $\wp(z; \omega_1, \omega_3)$ the Weierstrass $\wp$-function of a complex variable z of periods $2\omega_1, 2\omega_3$. The basic properties of $\wp$ (and its derivative with respect to z, $\wp'$) can be found in any complex variables text.

THEOREM 3. *Suppose $f(y) \in \boldsymbol{C}(y)$ satisfies* (3.1) *and* (3.2) *and that f is not a polynomial. Then there exist linear functions of y (say $\lambda(y)$, $\bar{\lambda}(y)$) such that with $\bar{\lambda}^{-1}\big(f(\lambda(y))\big)$ replacing f (we say that f is normalized) f is the solution of a certain type of functional equation. Let $\omega_1, \omega_3 \in \boldsymbol{C}$ and denote by $L(2\omega_1; 2\omega_3)$ the $\boldsymbol{Z}$-lattice generated by $2\omega_1$ and $2\omega_3$. Lemma 5 implies that f corresponds to one of the cases:*

(3.10) ((3.3)) *there exist constants $\omega_1, \omega_3, \omega_1', \omega_3'$ such that $\wp(z; \omega_1, \omega_3) = f\big(\wp(z; \omega_1', \omega_3')\big)$ where $\{2\omega_1', 2\omega_3'\} \in L(2\omega_1; 2\omega_3)$;*

(3.11) ((3.4) a)) *there exist constants ω_1, ω_3, a, b such that $\wp'(az+b) = f\big(\wp'(z)\big)$ where $\omega_3 = e^{\pi i/3}\omega_1$, and $\{2a\omega_1, 2a\omega_3, (1-e^{2\pi i/3})b\} \in L(2\omega_1; 2\omega_3)$;*

(3.12) ((3.4) b)) *there exist constants ω_1, ω_3, a, b such that $\wp^3(az+b) = f\big(\wp^3(z)\big)$ where $\omega_3 = e^{\pi i/3}\omega_1$, and $\{2a\omega_1, 2a\omega_3, b(1-e^{\pi i/3})\} \in L(2\omega_1; 2\omega_3)$;*

and

(3.13) ((3.4) c)) *there exist constants ω_1, ω_3, a, b such that $\wp^2(az+b) = f\big(\wp^2(z)\big)$ where $\omega_3 = i\omega_1$ and $\{2a\omega_1, 2a\omega_3, b(1-i)\} \in L(2\omega_1; 2\omega_3)$.*

Conversely, if constants ω_1, ω_3, a, b exist satisfying one of the conditions (3.11) *through* (3.13), *then there exists a rational function $f(y) \in \boldsymbol{C}(y)$ such that the Riemann surface for $f(y) - x$ over the x-sphere has branch cycles as described in Lemma 5.*

Proof. We do these cases in order. First we look at the situation of (3.3). Let $\lambda_1, \ldots, \lambda_4$ be the branch points of the Riemann surface of $f(y) - x$. Let $\lambda(y)$ be a linear fractional transformation such that

$$\lambda^{-1}(\lambda_1) = \infty, \quad \lambda^{-1}(\lambda_2) + \lambda^{-1}(\lambda_3) + \lambda^{-1}(\lambda_4) = 0. \tag{3.14}$$

Let $\lambda^{-1}(\lambda_i) = e_{i-1}$ for $i = 2, 3, 4$. Normalize f using λ (as in the statement of the Theorem) to obtain a new function with corresponding branch points e_1, e_2, e_3, ∞. Construct the elliptic function $\wp(z)$ such that $\wp(\omega_i) = e_i$, $i = 1, 2, 3$. Set $f(y) = \wp(z)$, and expand y in Puiseux expansions about all points in the finite portion of the z-sphere. In fact $\wp(z) - e_i$ has one zero of multiplicity 2 for $i = 1, 2, 3$ (also, ∞ is assumed with multiplicity 2). Thus, the condition (3.3) implies that the zeros $y_1, \ldots, y_p$ of $f(y) - \wp(z)$ are power series in $(z - \omega_i)$ (rather than in $(z - \omega_i)^{1/2}$). We easily see that $y_1, \ldots, y_p$ are meromorphic functions periodic on some lattice, generated by $2\omega_1', 2\omega_3'$ of index p in $L(2\omega_1; 2\omega_3)$. By linear change of $y_1(z)$ (see Section VII of [16]) we may assume

(3.15) $\beta(z) = \wp^{-1}(y_1(z))$ is locally single-valued

Then

(3.16) $$f(\wp(\beta(z))) = \wp(z).$$

So $\wp(\beta(z))$ is algebraically related to $\wp(z)$, and therefore $\wp(\beta(z))$ is elliptic. By differentiating (3.16) we obtain

(3.17) $$\wp'(z) = f'(\wp(\beta(z)))(\wp'(\beta(z)))\beta'(z).$$

Since $\wp'(\beta(z))$ is algebraically related to $\wp(\beta(z))$, $\wp'(\beta(z))$ is an elliptic function. Thus $\beta'(z)$ is an elliptic function. However, from (3.16) we are able to deduce that $\beta(z)$ is entire. In fact, if z_0 were a pole of $\beta(z)$, then z_0 would be an essential singularity of $f(\wp(\beta(z)))$, and therefore z_0 would be an essential singularity of $\wp(z)$. But the only essential singularity of $\wp(z)$ is at ∞. Thus, $\beta'(z)$ is an entire elliptic function. Thus $\beta'(z)$ is constant, or $\beta(z)$ is linear. (Added in proof. We check that

(3.18) $$\beta(z) = \pm z + z_0,$$

where z_0 represents a p-division point of the lattice $L(2\omega_1; 2\omega_3)$. The reader will find details in [16], Section VII, where f is described as the map from $\boldsymbol{P}^1$ to $\boldsymbol{P}^1$ induced from

(3.19) $$\boldsymbol{C}/L(2\omega_1'; 2\omega_3') \xrightarrow{\varphi} \boldsymbol{C}/L(2\omega_1; 2\omega_3).$$

Here φ is the canonical map.)

The remaining cases may be attacked by reasoning similar to the above. Therefore we indicate only the particular difficulties of the case. For (3.11) we seek a meromorphic function $h(z)$ such that:

(3.20) there exist exactly 3 complex numbers (say δ_1, δ_2, ∞) assumed by h with multiplicity 3 at a point,

and

(3.21) all other values of h are assumed at three distinct points.

Let $\omega_3 = e^{\pi i/3}\omega_1$, and consider $\wp(z; \omega_1, \omega_3)$. Since $\wp(z; \omega, e^{\pi i/3}\omega) = \wp(z; e^{2\pi i/3}\omega, -\omega)$ we have

$$\wp(e^{2\pi i/3}z) = e^{2\pi i/3}\wp(z). \tag{3.22}$$

Consider z_1, z_2 the two non-zero solutions of

$$e^{2\pi i/3}z \equiv z \bmod L(2\omega_1; 2\omega_3). \tag{3.23}$$

By differentiating (3.22) twice we see that $\wp''(z_i) = \wp'''(z_i) = 0$ for $i = 1, 2$. Thus $\wp'(z_i)$ is assumed with multiplicity 3 by $\wp'(z)$ at z_i for $i = 1, 2$. Also, ∞ is assumed by $\wp'(z)$ at $z = 0$. Since $\wp'(z)$ is a function on a curve of genus 1, the divisor of $\wp''(z)$ has degree $0 = 2(1)-2$. However, $\wp''(z)$ has only one pole for a coset representative of $C/L(2\omega_1; 2\omega_3)$ and that is at $z = 0$. Thus, the divisor of $\wp''(z)$ is $-4\mathfrak{p}_0+2\mathfrak{p}_1+2\mathfrak{p}_2+r$ where $\mathfrak{p}_0$ is the place corresponding to 0, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the places corresponding (respectively) to z_1 and z_2, and r is positive. Thus, r is the zero divisor. So $\wp'(z)$ has no other multiple values, and $h(z) = \wp'(z)$ is the meromorphic function we desired. The rest of (3.11) is handled in the same manner as we treated (3.10).

Cases (3.12) and (3.13) can be handled by use of the functions indicated. For details see [16], Section VII.

Assume, conversely, that there exist constants ω_1, ω_3, a, b satisfying one of (3.11) through (3.13). We show there exists a rational function $f(y)$ such that $f(\wp(z)) = \wp(az+b)$. Let $\mathfrak{p}$ be a place of $C(\wp(z))$ (the rational field generated by $\wp(z)$ over C). Except for finitely many places $\mathfrak{p}$, $\mathfrak{p}$ determines exactly two values of z (say z_1, z_2) modulo $L(2\omega_1; 2\omega_3)$ such that the value of $\wp(z)$ at $\mathfrak{p}$ is $\wp(z_1) = \wp(z_2)$. The conditions on a and b imply that $\wp(az_1+b) = \wp(az_2+b)$, so the place $\mathfrak{p}$ is uniquely extended to $\wp(az+b)$. By the fundamental theorem of Galois theory this implies $\wp(az+b) \in C(\wp(z))$ or $f(\wp(z)) = \wp(az+b)$ for some rational function $f(y)$. ■

PROBLEM 3. Let $f(y) \in K(y)$ be one of the rational functions described in Theorem 3. Does f define a one-one mapping modulo $\mathfrak{p}$ for infinitely many primes $\mathfrak{p}$ of K? (Added in proof. Solved: Section VII of [16].)

PROBLEM 4. For every integer n we can define analogues of degree n of the rational functions described in Theorem 3. However, the rational functions so constructed corresponding to composite integers n are actually compositions of rational functions of prime degree. Let $f(y) \in K(y)$ where K is a number field, and suppose that f is an *indecomposable* rational function. If f is also one-one modulo $\mathfrak{p}$ for infinitely many primes $\mathfrak{p}$, must f be one of the rational functions described in Theorem 3?

4. Other problems in the arithmetic of value sets of rational functions. For this section only, we have a slight addition to our notation. Let r be a positive integer and suppose $g_r(z) \in L(z)$. Then we denote the zeros of

$g_r(z)-x$ by $z_1(r), \ldots, z_{m(r)}(r)$ where $m(r)$ is the degree of g_r. When K is a number field, $f \epsilon K(y)$ and $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ (ring of integers of K) for which we may reduce f modulo $\mathfrak{p}$, we denote by $V_{\mathfrak{p}}(f)$ the values assumed by f modulo $\mathfrak{p}$.

In [3] the author devoted his attention to:

THE POLYNOMIAL CONJECTURE. *Let* $f, g_1, \ldots, g_l \epsilon K[y]$, *and assume*

$$V_{\mathfrak{p}}(f) \subset \bigcup_{i=1}^{l} V_{\mathfrak{p}}(g_i) \tag{4.1}$$

for all but a finite number of primes $\mathfrak{p}$ (*abbreviated* a.a. $\mathfrak{p}$.).

Then there exists an index i, *and a polynomial* $r(y) \epsilon K^*[y]$, *such that* $f(y) = g_i(r(y))$.

In some sense it was an outrageous conjecture. However, it did turn out to be true in several interesting cases. We list three of these:

(4.2) f is linear, and therefore $\bigcup_{1}^{l} V_{\mathfrak{p}}(g_i)$ = all cosets modulo $\mathfrak{p}$ for a.a. $\mathfrak{p}$.;

(4.3) $g_1, \ldots, g_l$ are cyclic polynomials;

(4.4) $l = 1$, $K = \boldsymbol{Q}$ and the hypotheses are strengthened to read $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for a.a. $\mathfrak{p}$.; if f indecomposable.

It is easy to form a generalization of the polynomial conjecture to:

(4.5) *The rational-function conjecture,*

which we won't bother to state, except to say that the word polynomial should be replaced by rational function. The next theorem is a slight generalization of Theorem 2 of [3]. Let $\Omega_x = \Omega_{g_1-x} \ldots \Omega_{g_l-x} \cdot \Omega_{f-x}$.

THEOREM 4. *Let* $f, g_1, \ldots, g_l \epsilon K(y)$ *and assume* (4.1) *holds. Then*

$$\bigcup_{i=1}^{n} G\big(\Omega_x/K(y_i)\big) \subset \bigcup_{i=1}^{l} \bigcup_{j=1}^{m(i)} G\Big(\Omega_x/K\big(z_j(i)\big)\Big) \tag{4.6}$$

where $\{y_i\}_1^n$ *are the zeros of* $f(y)-x$. *In fact,* (4.6) *and* (4.1) *are "essentially" equivalent* (p. 97 of [3]).

It turns out that the rational-function conjecture is not even true in the case analogous to (4.2). That is, there do exist rational functions $g_1, \ldots, g_l$ such that

$$\bigcup_{i=1}^{l} V_{\mathfrak{p}}(g_i) = \text{all cosets modulo } \mathfrak{p} \text{ for a.a. } \mathfrak{p}., \tag{4.7}$$

but

(4.8) $g_i(y)$ is not a linear fractional transformation for any $i = 1, \ldots, l$.

EXAMPLE 7. Let $h(y) \in \boldsymbol{Q}^*(y)$ be any rational function such that Ω_{h-x} is of *genus zero*. If $\Omega_{h-x} = \boldsymbol{Q}^*(t)$, all automorphisms of $\boldsymbol{Q}^*(t)$ are given by linear fractional transformations of T. Thus, the Galois group of $\Omega_{h-x}/\boldsymbol{Q}^*(x)$ can be identified with a finite group of linear fractional transformations. As a particular case, for cyclic and Chebychev polynomials Ω_{h-x} is of genus zero. For a list of possible groups we refer the reader to p. 133, [2]. Suppose in addition that

(4.9) $$G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right) \text{ is not a cyclic group.}$$

For each $\sigma \in G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ with $\sigma \neq 1$, let M_σ be the fixed field of σ in Ω_{h-x}. By Luroth's theorem $M_\sigma = \boldsymbol{Q}^*(t_\sigma)$ for some element t_σ of M_σ. There exists a rational function $g_\sigma \in \boldsymbol{Q}^*(y)$ such that $g_\sigma(t_\sigma) = x$. Relabel the g_σ's to be $g_1, \ldots, g_l$. Our construction assures that

(4.10) $$G\left(\Omega_x/\boldsymbol{Q}^*(x)\right) \subset \bigcup_{i=1}^{l} \bigcup_{j=1}^{m(i)} G\left(\Omega_x/\boldsymbol{Q}^*\left(z_j(i)\right)\right),$$

where $\Omega_x = \Omega_{h-x}$ in this case.

Now apply Theorem 4 to see that (4.7) holds.

Actually, the polynomial conjecture is false, even in the case where $g_1, \ldots, g_l$ are compositions of cyclic polynomials. Using a method like that of Example 7, the polynomial of (4.12) can be used to give a counterexample even when $g_1, \ldots, g_l$ are compositions of cyclic polynomials.

LEMMA 6 (p. 27 of [13]). *A primitive solvable permutation group is of degree p^m with p prime and $m \geqslant 1$. Also, a primitive solvable group cannot contain a cycle of length equal to its degree unless $m = 1$ or $p = 2$, $m = 2$.*

THEOREM 5. *Let $g_1, \ldots, g_l \in K[y]$ be compositions of cyclic and Chebychev polynomials. Suppose $f \in K[y]$ and $V_{\mathfrak{p}}(f) \subset \bigcup_{i=1}^{l} V_{\mathfrak{p}}(g_i)$ holds for a.a.p. (condition (4.1)). Then, f is a composition $f_1(f_2)$ of polynomials f_1 and f_2 where f_2 is an arbitrary polynomial in $K[y]$ and $\Omega_{f_1-x} \subset \Omega_{g_1-x} \ldots \Omega_{g_l-x}$, and $V_{\mathfrak{p}}(f_1) \subset \bigcup_{i=1}^{l} V_{\mathfrak{p}}(g_i)$ for a.a.p. In addition, f_1 is a composite of*

(4.11) *cyclic and Chebychev polynomials,*

or

(4.12) *polynomials h of degree 4 such that $G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ is the symmetric group on 4 letters.*

Proof. Theorem 4 implies that (4.6) holds. From expression (12) of [3], we know that (4.6) implies that we may replace f by a composition factor f_1 (over K) so that we may assume

(4.13) $$\Omega_{f-x} \subset \Omega_{g,x} = \Omega_{g_1-x} \ldots \Omega_{g_l-x}.$$

By extending scalars to $\boldsymbol{Q}^*$, we obtain

$$\bigcup_{i=1}^{n} G\left(\Omega_{g,x}/\boldsymbol{Q}^*(y_i)\right) \subset \bigcup_{i=1}^{l}\bigcup_{j=1}^{m(i)} G\left(\Omega_{g,x}/\boldsymbol{Q}^*(z_j(i))\right). \tag{4.14}$$

From Lemma 6 a primitive solvable group must be of prime-power degree. Let $h(y)\epsilon\boldsymbol{Q}^*[y]$ be an indecomposable polynomial. If h is a cyclic or Chebychev polynomial, explicit computation shows that $G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ is a solvable group. Also, all groups of degree 4 are solvable groups. Conversely, suppose $G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ is a solvable group. If $\deg h$ is prime, we may apply the argument of Lemma 9 of [4] to the normal subgroup of $G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ of prime order to deduce that h is type (4.11). Since h is indecomposable, $G\left(\Omega_{h-x}/\boldsymbol{Q}^*(x)\right)$ is primitive on the zeros of $h(y)-x$ (Lemma 2 of [4]), so by the argument above h is of prime-power degree. However, Lemma 6 implies that if h is not of prime degree, then degree $h = 4$.

Thus, the hypotheses of our theorem imply that $G\left(\Omega_{g_i-x}/\boldsymbol{Q}^*(x)\right)$ is a solvable group. From (4.14) $G\left(\Omega_{f-x}/\boldsymbol{Q}^*(x)\right)$ is a quotient of the group $G\left(\Omega_{g,x}/\boldsymbol{Q}^*(x)\right)$, which in turn is a subgroup of $G\left(\Omega_{g_1-x}/\boldsymbol{Q}^*(x)\right)\times\ldots\times$ $\times G\left(\Omega_{g_l-x}/\boldsymbol{Q}^*(x)\right)$. Therefore, since products, subgroups and quotient groups of solvable groups are solvable groups, we have ascertained that $G\left(\Omega_{f-x}/\boldsymbol{Q}^*(x)\right)$ is solvable. If $f(y) = f_1\left(f_2\left(\ldots\left(f_r(y)\ldots\right)\right)\right)$ where f_i is an indecomposable polynomial, then

$$G(\Omega_{s_i-x}/\Omega_{s_{i-1}-x}) \text{ is solvable,} \quad \text{where} \quad s_i(y) = f_1\left(f_2\left(\ldots\left(f_i(y)\ldots\right)\right)\right). \tag{4.15}$$

Let θ_{i-1} be a zero of $s_{i-1}(y)-x$. Then the zeros of $f_i(y)-\theta_{i-1}$ generate a subfield of Ω_{s_i-x} that is Galois over $\Omega_{s_{i-1}-x}$. In a natural way the group of this field (which must be a solvable group) is isomorphic to $G\left(\Omega_{f_i-x}/\boldsymbol{Q}^*(x)\right)$ (use the change of variable $\theta_{i-1}\to x$). Thus, f_i is a polynomial of type (4.11) or (4.12). This concludes the proof of the Theorem. ■

Example 8. One other case where the polynomial conjecture is now known to be wrong is the case of (4.4) ($V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for a.a.p) for some number fields $K \neq \boldsymbol{Q}$. This is discussed in great detail in Section 2 of [17]. A reduction technique used there shows that we may assume

$$\Omega_{f-x} = \Omega_{g-y}, \tag{4.16}$$

and

$$f \text{ and } g \text{ are indecomposable.} \tag{4.17}$$

With these assumptions, it turns out that $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for a.a.p. if and only if

4.18) $f(y)-g(z)$ is reducible as a polynomial in two variables.

Non-trivial examples of this phenomenon are now known to occur in degrees 7, 11, 13, 15, 21 and 31, and as explained in [5], these are believed to be the only possible degrees with f indecomposable. The example of degree 7 is described in Example 5 of this paper.

PROBLEM 5. Is the polynomial conjecture true for *any polynomial* f, other than f linear? That is, suppose $f \in K[y]$ is a *given* non-linear polynomial. Do there exist $g_1, \ldots, g_l$ such that $V_{\mathfrak{p}}(f) \subset \bigcup_{i=1}^{l} V_{\mathfrak{p}}(g_i)$ for a.a.p. but there exists no polynomial $h(y)$ and no index i such that $g_i(h(y)) = f(y)$?

5. Generalized Riemann existence theorem, and discussion of problems. We return to the notation of our introduction. Given $Y \xrightarrow{\varphi} \boldsymbol{P}^1(K^*)$, with (Y, φ) defined over K (via an embedding of Y in some projective space), we obtain an exact sequence:

$$(5.1) \qquad \{1\} \to G\left(\widehat{K(Y)}/\hat{K}(\boldsymbol{P}^1)\right) \to G\left(\widehat{K(Y)}/K(\boldsymbol{P}^1)\right) \xrightarrow{\pi} G(\hat{K}/K) \to \{1\},$$

where π is the map obtained by restriction of elements of $G\left(\widehat{K(Y)}/K(\boldsymbol{P}^1)\right)$ to $\hat{K}$. This leads to the following conjecture:

CONJECTURAL FORM OF RIEMANN'S EXISTENCE THEOREM. *Let* G_1 *and* G *be two transitive subgroups of* S_n (*the symmetric group on* n *letters*) *such that*

$$(5.2) \qquad G_1 \Delta G \quad (G_1 \text{ is normal in } G).$$

Then there exists a triple (Y, φ, K) *such that* $[K : \boldsymbol{Q}] < \infty$, *and*

$$(5.3) \qquad G\left(\widehat{K(Y)}/K(\boldsymbol{P}^1)\right) = G \quad \text{and} \quad G\left(\widehat{K(Y)}/\hat{K}(\boldsymbol{P}^1)\right) = G_1.$$

In order to strengthen the conjecture, we might use the concept of Hurwitz schemes as in [16], Section V. Let $\{\sigma_i\}_1^r \in G_1$ be generators of G_1 such that

$$(5.4) \qquad \prod_{i=1}^{r} \sigma_i = \mathrm{Id}.$$

Then, we may construct (over $\boldsymbol{C}$), a Riemann surface $\tilde{Y}$ covering $\boldsymbol{P}^1(\boldsymbol{C})$, having branch points $u_1^{(0)}, \ldots, u_r^{(0)} \in \boldsymbol{C}$, and having a description of its branch cycles given by $\{\sigma_i\}_1^r$. As in [16], Section V, under general conditions there exists a (possibly non-unique) symmetrized Hurwitz scheme parametrizing a natural family of Riemann surfaces covering $\boldsymbol{P}^1$, of which $\tilde{Y} \to \boldsymbol{P}^1$ is one member of the family. If $\mathrm{Aut}(\tilde{Y}, \varphi, \boldsymbol{C})$ consists of Id, then the Hurwitz scheme is unique, and (by a Galois descent argument) the field of definition $K(\mathscr{T})$ of the Hurwitz scheme is the *smallest possible* field

of definition for any cover $Y \xrightarrow{\varphi} \boldsymbol{P}^1$ having a description of its branch cycles given by $\{\sigma_i\}_1^r$. Although it is possible that no member of the family of the Hurwitz scheme $\mathscr{T}$ will actually be defined over $K(\mathscr{T})$, nevertheless the intersection of the fields of definition of members of the family will be $K(\mathscr{T})$. As Theorem 1 and Corollaries 1 and 2 of [16] show, there are many examples where $K(\mathscr{T}) \neq \boldsymbol{Q}$.

Our next example shows that, even if the conjectured form of Riemann's existence theorem were true, the field $\hat{K}$, that results from a triple (Y, φ, K), has a very strong dependency on the branch cycles $\{\sigma_i\}_1^r$ of the cover $Y \xrightarrow{\varphi} \boldsymbol{P}^1$.

EXAMPLE 9. Suppose that $G_1 \Delta G \subseteq S_n$ (as in the notation above), where G_1 contains the n-cycle $(1\,2 \ldots n)$. Let $\{\sigma_i\}_1^r$ be generators of G_1 satisfying (5.4) and the additional condition that:

$$\sigma_r = (1\,2 \ldots n). \tag{5.5}$$

If $Y \xrightarrow{\varphi} \boldsymbol{P}^1$ has a description of its branch cycles given by $\{\sigma_i\}_1^r$; (Y, φ) is defined over K; and $u_r^{(0)}$ (the branch point corresponding to σ_r) is contained in K; then:

$$\hat{K} \subseteq K(\zeta_n), \quad \text{where} \quad \zeta_n \text{ is a primitive } n\text{th root of } 1. \tag{5.6}$$

This follows from Remark 1 (Section 1). In fact, if we denote the group generated by σ_r by $\langle \sigma_r \rangle$, and the normalizer (in G) of $\langle \sigma_r \rangle$ by $N(\langle \sigma_r \rangle)$, we immediately obtain (from Galois theory):

$$N(\langle \sigma_r \rangle)/\langle \sigma_r \rangle \xrightarrow{\psi} G/G_1 \text{ is } \textit{onto}, \tag{5.7}$$

where ψ is given by the natural inclusion of $N(\langle \sigma_r \rangle)$ in G.

On the other hand: if the conjectured form of Riemann's existence theorem were true, and if G and G_1 were such that (5.7) was not satisfied; then there would exist covers of $\boldsymbol{P}^1$ such that the field K would not satisfy

$$G(\hat{K}/K) \text{ is a quotient of } N\big(\langle (1\,2 \ldots n) \rangle\big)/\langle (1\,2 \ldots n) \rangle. \tag{5.8}$$

We show how to obtain pairs G and G_1 that do not satisfy (5.7). Let $X^{(1)} = \langle (1\,2 \ldots n) \rangle$, and let $X^{(\alpha)}$, $\alpha = 1, \ldots, k$, denote the *distinct* subgroups of G which are conjugate to $X^{(1)}$. Let G_1 be the subgroup of G (normal in G) generated by $\{X^{(\alpha)}\}_{\alpha=1}^k$. Then, we obtain an action of G on $\{X^{(\alpha)}\}_{\alpha=1}^k$ by conjugation, and the stabilizer of $X^{(1)}$, denoted $G(X^{(1)})$, is $N\big(\langle (1\,2 \ldots n) \rangle\big)$. The map

$$G(X^{(1)})/G_1(X^{(1)}) \xrightarrow{\psi} G/G_1 \tag{5.9}$$

is *onto*, iff the orders of the left and right side of (5.9) are the same. In turn, these orders are the same iff G_1 is transitive by conjugation of $\{X^{(\alpha)}\}_{\alpha=1}^k$.

Roger Howe gave the following example where ψ is not onto. Let $n = p^a$ where p is any prime. Let G be the p-sylow of S_{p^a} containing $(1\,2\,\ldots\,p^a)$. It is part of the general p-group theory (see [1]) that if $H_1 \subsetneq H$ are p-groups, then there exists $\tilde{H}$ with $H_1 \subseteq \tilde{H} \underset{\neq}{\triangle} H$. In particular, if we let G_1 be the smallest normal subgroup of G containing $(1\,2\,\ldots\,p^a)$, then for $a \geqslant 2$ (so that G does not consist entirely of $\langle(1\,2\,\ldots\,p^a)\rangle$) $G_1 \underset{\neq}{\triangle} G$. If $a \geqslant 3$ (so that G_1 does not consist entirely of $\langle(1\,2\,\ldots\,p^a)\rangle$), then the smallest normal subgroup of G_1 containing $\langle(1\,2\,\ldots\,p^a)\rangle$ is properly contained in G_1. In particular, G_1 is not transitive on $\{X^{(a)}\}_{a=1}^{k}$. This concludes our example. ■

In spite of Example 9, we feel that the *Hurwitz scheme approach* will provide a very reasonable, precise conjectural form of the Riemann existence theorem. This is taken up in [16], Section VII. For now, we assume that such an existence theorem exists, and show how it relates to the *generalized Schur conjecture.*

DEFINITION 8. Let H be a transitive subgroup of S_n, where we denote the stabilizer of i by $H(i)$, $i = 1, \ldots, n$. Let $1 \leqslant s_1 < s_2 < \ldots < s_u$ be integers. If $H(1)$ has l_i orbits of length s_i, $i = 1, \ldots, u$ on the set $\{2, \ldots, n\}$, we say that H is of *stabilizer type* $\{(s_1; l_1); (s_2; l_2); \ldots; (s_u; l_u)\}$.

If the triple (Y, φ, K) is a solution to the generalized Schur problem, then

$$G_1 = G\big(\widehat{K(Y)}/\hat{K}(\boldsymbol{P}^1)\big) \tag{5.10}$$

is of stabilizer type, as above, with $l_i \geqslant 2$ for $i = 1, \ldots, u$, and

$$G_1 \triangle G\big(\widehat{K(Y)}/K(\boldsymbol{P}^1)\big) = G \tag{5.11}$$

where $G(1)$ leaves fixed *no* orbit of $G_1(1)$ on $\{2, \ldots, n\}$.

If, in addition, we are looking to solve the Schur problem for rational functions, then (by the Riemann–Hurwitz formula) we consider the case there exist generators $\{\sigma_i\}_1^r \in G_1$, of G_1 such that

$$\prod_{i=1}^{r} \sigma_i = \mathrm{Id}, \tag{5.12}$$

and

$$\sum_{i=1}^{r} \mathrm{ind}(\sigma_i) = 2(n-1). \tag{5.13}$$

Section 2 of this paper, [6] and Corollary 4 of [16] are contributions to the computations needed to find generators satisfying (5.12) and (5.13).

We feel that Problems 1 and 3, and problems related to the concept of decomposably stable (Definition 7) are best attacked by the Hurwitz scheme approach; and whatever the outcome, they should provide interesting data toward the more complete formulation of the *generalized Riemann existence theorem.*

References

[1] W. Burnside, *On simply transitive groups of prime degree*, Quart. J. Math 37 (1906), pp. 215–221.
[2] L. R. Ford, *Automorphic Functions*, New York 1951.
[3] M. Fried, *Arithmetical properties of value sets of polynomials (I)*, Acta Arith. 15 (1969), pp. 91–125.
[4] — *On a conjecture of Schur*, Mich. Math. J. 17 (1970), pp. 41–55.
[5] — *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. 17 (1973), pp. 128–146.
[6] — *On a theorem of Ritt*, to appear in Crelle's J., June 1974.
[7] — *Naive class field theory for local function fields over finite fields*, in preparation.
[8] — *On a theorem of MacCluer*, Acta Arith. 25 (1974), pp. 121–125.
[9] — (with R. E. MacRae), *On the invariance of chains of fields*, Illinois J. Math. 13 (1969), pp. 165–171.
[10] R. Lidl and C. Wells, *Chebychev polynomials in several variables*, Crelle 1972.
[11] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), pp. 51–66.
[12] — *Permutable rational functions*, Trans. Amer. Math. Soc. 25 (1923), pp. 399–448.
[13] — *On algebraic functions which can be expressed in terms of radicals*, Trans. Amer. Math. Soc. 24 (1922).
[14] G. Springer, *Introduction to Riemann Surfaces*, Reading, Mass., 1957.
[15] C. Wells (with the aid of W. Nöbauer), *Bibliography of Literature on Representable Mappings of an Algebraic Structure Into Itself*, Dept. of Math, Case Western Reserve University.

Added in References

[16] M. Fried and D. J. Lewis, *Solution spaces to diophantine problems*, Bull. Amer. Math. Soc., to appear.
[17] M. Fried, *On Hilbert's Irreducibility Theorem*, Journal of Number Theory, to appear June 1973.
[18] S. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), pp. 259–273.

Received on 12. 6. 1970 (312)