Reprinted from ILLINOIS JOURNAL OF MATHEMATICS
Vol. 17, No. 1, March 1973
Printed in U.S.A.

THE FIELD OF DEFINITION OF FUNCTION FIELDS AND A PROBLEM IN THE REDUCIBILITY OF POLYNOMIALS IN TWO VARIABLES

BY
MICHAEL FRIED

Introduction

Let K be a number field, $\mathcal{O}_K$ the ring of integers of K. Suppose we are given a projective curve Z, and a morphism $\phi : Z \to \mathbf{P}'(\mathbf{C})$ (where $\mathbf{P}'(\mathbf{C})$ is the projective line) such that ϕ and Z are both defined over K. We denote by $K(Z)$ the field of functions of Z defined over K, and from this data we obtain a permutation representation T of the Galois group $G(K(Z)^\wedge/K(\mathbf{P}'(\mathbf{C})))$ (where $K(Z)^\wedge$ is the normal closure of $K(Z)$ over $K(\mathbf{P}'(\mathbf{C}))$).

In Section 1 we investigate (for our needs) the combinatorial and group theoretical aspects of the situation where

(*) G is a group equipped with two (permutation inequivalent) doubly transitive permutation representations $T_1 = T$ and T_2 which are equivalent as group representations.

Such groups arise, for instance, as the group of Projective linear transformations on the points (respectively hyperplanes) of a projective space over a finite field.

Section 3 contains the arithmetic results. Assume (*) holds for

$$G = G(K(Z)^\wedge/K(\mathbf{P}'(\mathbf{C}))),$$

and also assume that

(**) the (ramified) cover $Z \to \mathbf{P}'(\mathbf{C})$ has one totally ramified place.

As a particular case of Theorem 2 we obtain the fact that Z cannot be defined over $\mathbf{Q}$ ($K = \mathbf{Q}$ is impossible). Proposition 8 describes another general situation where $K = \mathbf{Q}$ is impossible.

In Section 2 we develop the theory of the reducibility of polynomials of form $g(y) - h(z)$ for $g(y), h(y) \in K[y]$. This problem was considered by many authors including Cassels [2], Schinzel [17], et al. [4], [5], [6]. The case where g and h are rational functions may be treated in a similar manner, although the theory would not yield such decisive results. In Theorem 1 we assume that g is not the functional composition of non-linear polynomials of lower degree. We exclude the trivial situation (where $h = g(m(y))$ for some polynomial $m(y)$) to obtain: if $g(y) - h(z)$ is reducible, then $g(y) - x = f(x, y)$ (where x is a generator of $K(\mathbf{P}'(\mathbf{C}))$ defines a curve $Z \to \mathbf{P}'(\mathbf{C})$ satisfying (*) and (**), and the Riemann surface for $f(x, y)$ over the x-sphere

Received May 13, 1969; received in revised form March 8, 1972.

has at most three finite branch points. This immediately gives strong conditions on the degree of g, shows that $K = \mathbf{Q}$ is not possible (Theorem 2) and (modulo a well-known conjecture from finite group theory on the situation described by (*)) allows us to write out (explicitly) the complete list of polynomials g of degree 7, 11, 13, 15, 21, 31 (respectively) for which $g(y) - h(z)$ is (non-trivially) reducible, for some polynomial h. For these latter computations see [12].

While our main desire is to put an emphasis on a general situation where our arithmetic setup has application, we wish to point out here that the particular problem considered in Section 2 is a convenient tool for investigation of many problems in number theory, combinatorial theory, and group theory. This problem, for instance, arises whenever we consider an irreducible polynomial $\phi(x, y) \in K[x, y]$ and we investigate the condition that the set

$$R_\phi = \{x_0 \in \mathcal{O}_K \mid \phi(x_0, y) \in K[y] \text{ is reducible as a polynomial in one variable}\}$$

is an infinite set. See [10] and [11] for this and other problems related to Hilbert's irreducibility theorem. Schinzel has treated a different type of reducibility theorem in several papers. See [13] for results that can be obtained from a combination of our techniques. In combinatorial theory, the technique of this paper can be used to show that for any even integer k, there are only finitely many possible Moore graphs of rank k.

The results of this paper were obtained during the academic year 1968–69 while the author was a member of the Institute for Advanced Study. Delay in publication corresponds to delay in publication of the applications (for which we'd like to thank the editors and referees of several journals). Companion to this paper is [12] which considers the problems treated in this paper as a part of the general theory of diophantine equations, and in particular discusses some examples relevant to this paper.

In addition, we'd like to thank Tom Storer for his contribution to the proof of Lemma 5.

1. Facts on permutation representations

Much of the material of this section is folklore. The pair (G, T) designates a finite group G with a *faithful permutation representation* T. Unless otherwise stated, all permutation representations will also be assumed to be transitive. For $\sigma \in G$, if $T(\sigma) = \prod_{i=1}^{k_\sigma} \beta_i$ is the decomposition of σ into a product of disjoint cycles β_i (of length $s(\sigma, i)$) then we define

$$\text{tr}\,(T(\sigma)) = \{\#\text{ of integers } i \mid s(\sigma, i) = 1\}, \tag{1.1}$$

$$\text{ind}\,(T(\sigma)) = \sum_{i=1}^{k_\sigma} (s(\sigma, i) - 1). \tag{1.2}$$

Sometimes we abuse notation and write $T(\sigma) = (s(\sigma, 1)) \cdots (s(\sigma, k_\sigma))$.

DEFINITION 1. Let (G, T_1) and (G, T_2) be two permutation representa-

tions of G of the same degree, deg T_1 = deg $T_2 = n$ (so $T_1 : G \to S_n$ where S_n is the symmetric group on n letter, for $i = 1, 2$). We say (G, T_1) is permutation equivalent to (G, T_2) if there exists $\sigma \in S_n$ such that

$$\sigma \cdot T_1(\tau) \cdot \sigma^{-1} = T_2(\tau) \quad \text{for each } \tau \in G. \tag{1.3}$$

We say that (G, T_1) is equivalent to (G, T_2) if

$$\text{tr } (T_1(\sigma)) = \text{tr } (T_2(\sigma)) \quad \text{for each } \sigma \in G. \tag{1.4}$$

LEMMA 1. *Let G be a finite group with permutation representation T_1 and T_2, of the same degree such that* (1.4) *holds. Then, if $T_1(\sigma)$ is a product of disjoint cycles of length $s(1), \cdots, s(k)$ then so is $T_2(\sigma)$, for all $\sigma \in G$.*

Proof. We must show that for each integer l, $T_1(\sigma)$ and $T_2(\sigma)$ contain the same number of disjoint cycles of length l. For any positive integer s

$$\text{tr } (T_i(\sigma^s)) = \sum_{d \mid s} n_{d,i}(\sigma) \cdot d, \quad \text{for} \quad i = 1, 2, \tag{1.5}$$

where $n_{d,i}(\sigma)$ = number of disjoint cycles of length d in $T_i(\sigma)$. Assume that l is the smallest integer for which there exists some element $\sigma \in G$ such that $n_{l,1}(\sigma) \neq n_{l,2}(\sigma)$. However, $n_{d,1}(\sigma) = n_{d,2}(\sigma)$ for $d \mid l$ and $d < l$, so this contradicts (1.5) when $l = s$, since

$$\text{tr } T_1(\sigma^l) = \text{tr } T_2(\sigma^l). \tag{1.6}$$

∎

LEMMA 2. *Let (G, T_i), $i = 1, 2$, be two doubly transitive permutation representations of the same degree such that*

$$\text{tr } (T_1(\sigma)) > 0 \text{ iff } \text{tr } (T_2(\sigma)) > 0 \quad \text{for each} \quad \sigma \in G. \tag{1.7}$$

Then (G, T_1) and (G, T_2) are equivalent.

Proof. From [15, Theorem 16.6. 15, p. 284] a doubly transitive permutation representation is the sum of the identity representation and an irreducible representation. Thus

$$\text{tr } (T_i(\sigma)) = 1 + \theta_i(\sigma) \quad \text{for} \quad i = 1, 2 \tag{1.8}$$

where θ_i is the character of an irreducible representation. The representations T_1 and T_2 are equivalent if and only if $\theta_1(\sigma) = \theta_2(\sigma)$ for all $\sigma \in G$. But $\theta_1 \not\equiv \theta_2$ if and only if

$$0 = (\theta_1, \theta_2) = \sum_{\sigma \in G} \theta_1(\sigma)\theta_2(\sigma^{-1}) \tag{1.9}$$

(see [15, Theorem 16.6.5, p. 279]). Since θ_1 and θ_2 take on integral values ≥ -1, and $\theta_1(\sigma) = -1$ if and only if $\theta_2(\sigma) = -1$, we must have $(\theta_1, \theta_2) > 0$. Thus T_1 is equivalent to T_2. ∎

LEMMA 3. *Let G be a finite group with permutation representations T_1 (on the letters $x(1), \cdots, x(n)$) and T_2 (on the letters $z(1), \cdots, z(m)$). Assume*

that expression (1.7) *holds for* $T = T_1$, *and* T_2. *Then*

(1.10) $G_{x(1)}$ (*stabilizer of* $x(1)$ *in* G) *is not transitive on* $z(1), \cdots, z(m)$ *and* $G_{z(1)}$ *is not transitive on* $x(1), \cdots, x(n)$.

Conversely, if T_1 *and* T_2 *are doubly transitive representations and* (1.10) *holds, then*

(1.11) (G, T_1) *and* (G, T_2) *are equivalent representations.*

Also, if we assume only that $\deg T_1 = \deg T_2 = p$ *for some prime* p, *then* (1.10) *holds.*

Proof. Condition (1.7) implies that

$$G_{x(1)} \subset \bigcup_{i=1}^{m} G_{z(i)} . \tag{1.12}$$

Thus, if $G_{x(1)}$ is transitive on $z(1), \cdots, z(m)$, then the conjugates of the subgroup $G_{x(1)} \cap G_{z(1)}$ (denoted H) of $G_{x(1)}$, make up all of $G_{x(1)}$. That is $\bigcup_{\sigma \in G_{x(1)}} \sigma H \sigma^{-1} = G_{x(1)}$. However, as is well known, the conjugates of a proper subgroup of a group cannot cover the whole group. Thus (1.10) must hold.

Now, suppose (G, T_1) and (G, T_2) are doubly transitive representations and (1.10) holds. It is known (see [1, p. 163, exercise 14]) that a doubly transitive group G (with representation T_2) does not contain an intransitive subgroup (say $G_{x(1)}$) of index ($(G : G_{x(1)}) = n$) less than its degree ($\deg T_2 = m$). Thus, $n \geq m$, similarly, $m \geq n$, or $\deg T_1 = \deg T_2$. Consider the vector space over $\mathbf{C}$ generated by $\{X_i\}_{i=1}^{n}$. The representation T_1 is obtained by

$$\sigma \to A_1(\sigma) \tag{1.13}$$

where

$$A_1(\sigma)(X_i) = X_j \quad \text{if} \quad T_1(\sigma)(x(i)) = x(j).$$

Let $G_{z(1)}$ be transitive on $x(1), x(\alpha(2)), \cdots, x(\alpha(k))$. Then

$$Z_1 = X_1 + X_{\alpha(2)} + \cdots + X_{\alpha(k)}$$

has n conjugates (under the action of G) and we denote these by $\{Z_i\}_{i=1}^{n}$. It is easy to see that the representation T_2 is obtained from the $\{Z_i\}_{i=1}^{n}$. Thus, T_1 and T_2 are equivalent representations, since they are obtained from each other by a change of basis of a representation module for G.

Now assume only that degree T_1 = degree $T_2 = p$ for some prime p. Then $| G_{x(1)} |$ is not divisible by p, so $G_{x(1)}$ cannot be transitive on $z(1), \cdots, z(p)$. This concludes the proof of the lemma. ∎

Definition 2. Let F be a finite ring. A set of distinct elements $D = \{d_1, \cdots, d_k\}$ form a *difference set* of multiplicity r if the differences $\{d_i - d_j \text{ for } i \neq j\}$ run over all values of $F - \{0\}$ exactly r times. If $| F | = n$ we say we have an $\{n, k, r\}$ design. Our notation differs slightly from standard

notation. If F is the integers $\mathbf{Z}$ modulo n (or $\mathbf{Z}/(n)$), then D is said to be a cyclic difference set. In the latter case, an element $\alpha \in \mathbf{Z}/(n)$ is said to be a *multiplier* of the difference set D if

$$\{\alpha d_1, \cdots, \alpha d_k\} = \{d_1 + t, \cdots, d_k + t\} = D + t$$

for some integer t. The sets $D, D + 1, \cdots, D + (n - 1)$ are the *blocks* of the design.

From Lemma 4 we see that difference sets are relevant to our special assumptions. According to T. Storer the fact that -1 is not a multiplier is an old chestnut in the theory of difference sets. He has provided us with a simple proof of this fact, upon which we base the proof of Lemma 5.

LEMMA 4. *Let* (G, T_i), $i = 1, 2$, *be doubly transitive permutation representations such that*

(1.14) *condition* (1.7) *holds, and*

(1.15) *there exists* $\sigma \in G$ *such that* $T_1(\sigma)$ *is an* n*-cycle.*

In the notation of Lemma 3, *assume we have labeled*

$$\{x(1), \cdots, x(n)\}, \quad \{z(1), \cdots, z(n)\}$$

so that $T_1(\sigma)(x(i)) = x(i + 1)$, $i = 1, \cdots, n$ *and* $T_2(\sigma)(z(i)) = z(i + 1)$, $i = 1, \cdots, n$. *Then,*

(1.16) if $G_{x(1)}$ *acts on* $z(1), z(\alpha(2)), \cdots, z(\alpha(k))$ *transitively, the integers* $\{1, \alpha(2), \cdots, \alpha(k)\}$ *form a difference set modulo* n.

Proof. From Lemma 3 our hypotheses imply that there exists a set

$$\{z(1), z(\alpha(2)), \cdots, z(\alpha(k))\}$$

with $k < n$ as in (1.16). The argument of Lemma 3 shows that the n sets

$$\begin{aligned} R_1 &= \{(z(1), z(\alpha(2)), \cdots, z(\alpha(k))\}, \\ R_2 &= \{z(2), z(\alpha(2) + 1), \cdots, z(\alpha(k) + 1)\}, \\ &\vdots \\ R_n &= \{z(n), z(\alpha(2) + n - 1), \cdots, z(\alpha(k) + n - 1)\} \end{aligned}$$

(these sets are conjugate by the n cycle σ) provide a representation of G that is the same as T_1. The number of times an integer u modulo n appears as a difference from the set $\{1, \alpha(2), \cdots, \alpha(k))\}$ is the same as the number of times the pair $\{z(1), z(u + 1)\}$ appears in the sets $R_1, \cdots, R_n$. But since T_2 is a doubly transitive representation of G, the number of times the pair $\{z(1), z(u + 1)\}$ appears in the sets $R_1, \cdots, R_n$ is independent of u for $u = 1, \cdots, n - 1$. Thus, every non-zero integer modulo n occurs as a difference from the set $\{1, \alpha(2), \cdots, \alpha(k)\}$ the same number of times, and this set is a difference set. ∎

LEMMA 5. *Let $D = \{d_1, \cdots, d_k\}$ be a difference set modulo n. Let $\mathfrak{M}$ be the group of multipliers of D. Then -1 and $-1 + n/2$ (if n is even) are not multipliers if $k \neq 0, 1, n-1, n$ (the trivial cases).*

Proof. Given an element $m \in \mathfrak{M}$, some block of the difference set is fixed by m (see [16, Theorem 11.5.3]). Thus we assume in each case that

$$D = \{d_1, \cdots, d_k\}$$

is fixed by m. We consider $m = -1$ and $m = -1 + n/2$ separately. First, let $m = -1$.

Suppose a is an integer such that $a \neq 2d_i$ for $i = 1, \cdots, k$. Since -1 is a multiplier the representations for a as differences come in distinct pairs;

$$a = d_\alpha - d_\beta \quad \text{and} \quad a = -d_\beta - (-d_\alpha). \tag{1.17}$$

Thus, r (the multiplicity of the difference set) must be even. Now suppose $a = 2d_i$ for some $i = 1, \cdots, k$. In order for a to be represented as differences an even number of times there must exist $j \neq i$ such that $a = 2d_j = d_j - (-d_j)$. But this implies that $2(d_i - d_j) = 0$ modulo n or $d_j = d_i + n/2$. Thus, for each i, $d_i + n/2 \in D$, $i = 1, \cdots, k$. This implies that $n/2$ can be represented as a difference in at least $k - 1$ ways. However, one of the simple combinatorial formulas relates r, k, n by $r(n-1) = k(k-1)$. Therefore we see that $r \geq k - 1$ is impossible except in the cases $k = 0, 1, n - 1, n$.

Now we consider the case $m = -1 + n/2$. Let a be an integer such that

$$a \text{ is even, but } a \neq -2d_i + (n/2)d_i \text{ for } i = 1, \cdots, k. \tag{1.18}$$

A simple argument shows that a exists. In this case the representations of a as differences occur in distinct pairs.

$$a = d_\alpha - d_\beta = (-1 + n/2)d_\beta - (-1 + n/2)d_\alpha. \tag{1.19}$$

Note that a even is important. Thus r is even. Now assume

$$a = -2d_i + (n/2)d_i \quad \text{for some} \quad i = 1, \cdots, k.$$

Then since r is even, the number of representations of a in this form must be even. So there exists $j \neq i$ such that

$$-2d_i + (n/2)d_i = (-1 + n/2)d_i - d_i = (-1 + n/2)d_j - d_j. \tag{1.20}$$

Equivalently $(-2 + (n/2))(d_i - d_j) = 0$ modulo n. However, we have $((n-4)/2, n) = 2$ or 1 (as n is, or is not divisible by 4). So again we deduce that for each i, $d_i + n/2 \in D$. The final contradiction proceeds as in the case $m = -1$, and therefore $-1 + n/2$ is not a multiplier. ∎

Remark 1. Let D, $D + 1, \cdots, D + n - 1$ be the blocks of an (n, k, r) design (see Definition 2). Each of the blocks are a difference set. We say that two difference sets D_1 and D_2 are equivalent if they are blocks of the same design.

Let (n, k, r) be a 3-tuple of integers such that:

(1.21) $r(n-1) = k(k-1)$,
(1.22) there exists a difference set D modulo n with parameters (n, k, r) (note that 1.22) implies 1.21)) and,
(1.23) the group $G(D) = \{\sigma \in S_n$ (symmetric group on n letters) $\mid \sigma$ permutes the blocks of the design$\}$ is a doubly transitive permutation group.

We list some facts and observations about these conditions.

Fact 1. The subgroup $\mathfrak{M}$ of multipliers of the group $G(D)$ is not a transitive group.

Fact 2. (Conditions of Chowla and Ryser [3, Theorems 3, 4, 5]). If n is even, and a difference set modulo n with parameters (n, k, r) exists, then $k - r$ is a square. If n is odd, and a difference set with parameters (n, k, r) exists, then

(1.24) $z^2 = (k-r)x^2 + (-1)^{(n-1)/2}y^2$ has a non-trivial solution in integers x, y, z.

These conditions are believed to be both necessary and sufficient for the existence of a difference set modulo n with parameters (n, k, r). For the integers $n \leq 31$ such that there exists $\{k, r\}$ satisfying (1.21) (that is, $n - 1$ is not a power of a prime) with $1 < k < n - 1$ (these are the integers 7, 11, 13, 15, 16, 19, 21, 22, 23, 25, 27, 29, 31), $n = 22$ and $n = 23$, 27 do not satisfy (1.22).

Fact 3. Up to equivalence, the only difference sets modulo 7, 11, 13 are, respectively:

(1.25) $D = \{1, 2, 4\}; \{1, 2, 4, 9, 10\}; \{1, 2, 4, 10\}$ and $\{1, 2, 5, 7\}$, and their negatives.

Modulo 21 and 31, respectively, $D = \{1,2,7,9,19\}$ and $D = \{1,2,4,9,13,19\}$ are difference sets.

Fact 4. Let $l \geq 2$ be an integer, and $q = p^l$ where p is a prime. Let $D_l(q)$ be the design whose points are the points of l-dimensional projective space over the finite field of q elements and whose blocks are the hyperplanes of this space. The automorphism group of $D_l(q)$ is denoted $P\Gamma L_{l+1}(q)$. Then $D_l(q)$ is a

$$((q^{l+1}-1)/(q-1),\quad (q^l-1)/(q-1),\quad (q^{l-1}-1)/(q-1))$$

design, and $P\Gamma L_{l+1}(q)$ contains a $(q^{l+1}-1)/(q-1)$-cycle and is a doubly transitive group on the points of $D_l(q)$. Also, there exists an (11, 5, 2) design, denoted by $H(11)$ whose automorphism group is $PSL_2(11)$ for which (1.22) and (1.23) hold. It is *not known* if any other doubly transitive cyclic designs exist.

We add to these facts a theorem of W. Feit.

PROPOSITION 1. *Let $\mathfrak{D}$ be any symmetric, balanced, incomplete block design* [16, Chaper 11]. *Then any non-identity automorphism of $\mathfrak{D}$ moves at least half the points* [7, Theorem 3].

2. Reducibility of polynomials

Let K be some subfield of $\mathbf{C}$, and assume $f(x, y) \in K[x, y]$. Then we denote by Ω_f the splitting field of $f(x, y)$ over $K(x)$. We shall be primarily concerned with the case

$$f(x, y) = h_1(y) - h_2(y)x \tag{2.1}$$

where $h_1(y)$, $h_2(y) \in K[y]$ are relatively prime polynomials. As a matter of course, we use the ratio $h_1(y)/h_2(y) = h(y)$, and we sometimes abuse notation by writing $h(y) - x$ instead of $f(x, y)$ as in (2.1). The degree of h is the integer, max (degree h_1, degree h_2).

DEFINITION 3. Let $h(y) \in K(y)$. We say $h(y)$ is *decomposable* over K if $h(y) = h^{(1)}(h^{(2)}(y))$ where degree $h^{(i)}(y) > 1$ for $i = 1, 2$. If $h^{(1)}$ and $h^{(2)}$ do not exist, then $h(y)$ is *indecomposable* over K.

Question. When can there exist a pair of rational functions $h, g \in K(y)$ such that

$$\Omega_{h-x} = \Omega_{g-x}; \tag{2.2}$$

or such that

(2.3) $h(y) - g(z)$ is reducible as a rational function in two variables;

or such that

$$\bigcup_{y_i} G(\Omega_x/K(y_i)) = \bigcup_{z_j} G(\Omega_x/K(z_j)) \tag{2.4}$$

where $\Omega_x = \Omega_{h-x} \cdot \Omega_{g-x}$, $G(\Omega_x/K(x))$ is the Galois group of the field Ω_x over $K(x)$ and $\{y_1, \cdots, y_n\}$ (respectively $\{z_1, \cdots, z_m\}$) are the zeros of $h(y) - x$ (respectively $g(z) - x$)?

DEFINITION 4. If $h(y)$ and $g(y)$ are related by

$$h(y) = g((ay + b)/(cy + d))$$

for some $a, d, c, d \in K$ we say, h and g are *linearly related.* When h and g are linearly related, then conditions (2.2), (2.3) and (2.4) are easily seen to be satisfied.

LEMMA 6. *With the preceding notation, if $h, g \in K(y)$, then h and g are linearly related if and only if there exists an integer i such that*

$$G(\Omega_x/K(y_1)) = G(\Omega_x/K(z_i)).$$

Proof. From the fundamental theorem of Galois theory,

$$G(\Omega_x/K(y_1)) = G(\Omega_x/K(z_i)) \quad \text{if and only if} \quad K(y_1) = K(z_i),$$

an equality between genus zero function fields. By simple field theory

$$z_i = (ay_1 + b)/(cy_1 + d)$$

for some $a, b, c, d \in K$. This is equivalent to the relation

$$h(y_1) = x = g((ay_1 + b)/(cy_1 + d)).$$

The lemma now follows easily. ∎

LEMMA 7 [8, Proposition 2.3]. *Let $h(y) \in K(y)$, and assume y_1 is any zero of $h(y) - x$. Then, there is a one-to-one association between subfields of $K(y_1)$ containing $K(x)$ and composition factors of $h(y)$. Namely, for*

$$K(x) \subset M \subset K(y_1), \quad M = K(h^{(2)}(y))$$

where $h^{(2)} \in K(y)$ and $h = h^{(1)}(h^{(2)})$.

PROPOSITION 2. *Let $h(y), g(y) \in K(y)$, where $h = h_1/h_2$, $g = g_1/g_2$ as in (2.1). Assume*

(2.5) *$(h(y) - g(z))h_2(y)g_2(z)$ is a reducible polynomial in $K[y, z]$.*

Then there exist rational functions $h^{(1)}, h^{(2)}, g^{(1)}, g^{(2)} \in K(y)$ such that

$$h = h^{(1)}(h^{(2)}), \quad g = g^{(1)}(g^{(2)}), \tag{2.6}$$

$$\Omega_{h^{(1)}-x} = \Omega_{g^{(1)}-x} \text{ denoted } \Omega_x^*, \tag{2.7}$$

and

(2.8) *the irreducible factors of $(h(y) - g(z))h_2(y)g_2(z)$ (over K) are in one-to-one correspondence with*

(2.9) *the transitivity classes of $G(\Omega_x^*/K(y_1^*))$ on the letters $z_1^*, \cdots, z_{m^*}^*$ where y_i^*, $i = 1, \cdots, n^*$ are the zeros of $h^{(1)}(y) - x$; z_j^*, $j = 1, \cdots, m^*$ the zeros of $g^{(1)}(z) - x$.*

Remark 2. The members of (2.9) will be shown to be in one-to-one correspondence with the irreducible factors of $h^{(1)}(y) - g^{(1)}(z)$ (over K). Also, if h and g are polynomials satisfying condition (2.2), the degree of h can be interpreted as the order of the inertial groups for places of Ω_{h-x} lying over the place at ∞ on the x-sphere. Proposition 2 therefore implies that in considering the reducibility of *polynomials* of the form $h(y) - g(z)$, we may assume without loss that $\deg h = \deg g$ and $\Omega_{h-x} = \Omega_{g-x}$.

Proof. Let $\Omega_x = \Omega_{h-x} \cdot \Omega_{g-x}$. Since y_1 is an indeterminate over K, the irreducible factors of $h(y) - g(z)$ are in one-to-one correspondence with the irreducible factors of $h(y_1) - g(z)$ over K. The latter are, as an immediate consequence of Galois theory, in one-to-one correspondence with

(2.10) the transitivity classes of $G(\Omega_x/K(y_1))$ on the letters $z_1, \cdots, z_m$.

We now show that the elements of (2.10) are in one-to-one correspondence

with the transitivity classes of $G(\Omega_{g-x}/K(y_1'))$ on $z_1, \cdots, z_m$, where $K(y_1') = K(y_1) \cap \Omega_{g-x}$. Use Lemma 7 to find h' such that $h'(y_1') = x$. From the theorem of natural irrationalities,

$$G(\Omega_{g-x}/K(y_1')) = G(K(y_1)\cdot\Omega_{g-x}/K(y_1)).$$

Since every automorphism of $K(y_1)\cdot\Omega_{g-x}/K(y_1)$ extends to an automorphism of Ω_x, $G(K(y_1)\cdot\Omega_{g-x}/K(y_1))$ has the same transitivity classes on $z_1, \cdots, z_m$ as does the group $G(\Omega_x/K(y_1))$.

Now let h' play the role of g, and g the role of h in the above argument. We conclude the existence of a rational function g' such that $\Omega_{g'-x} \subset \Omega_{h'-x}$, and the irreducible factors of $h(y) - g(z)$ are in one-to-one correspondence with the transitivity classes of $G(\Omega_{h'-x}/K(z_1'))$ on the letters $y_1', \cdots, y_n'$, where $h'(y_i') = x$, $i = 1, \cdots, n'$. Continuing this process we eventually obtain rational functions $h^{(1)}, g^{(1)}$ satisfying (2.7) and (2.8).

The next lemma is a consequence of the theorem of natural irrationalities, and the technique of proof is well known.

LEMMA 8. *Let $f(y) \in K[y]$ be an irreducible polynomial. Let Ω be the splitting field of f over K, and let M be any Galois subfield of Ω containing K. Also, let $y_1, \cdots, y_n$ be the zeros of $f(y)$. Then, any element of $G(M/K)$ which leaves $L = K(y_1) \cap M$ elementwise fixed, can be extended to an element of $G(\Omega/K(y_1))$. If, in addition $K(y_1) \cap M = K$, then*

$$(2.11)\quad G(\Omega/M) - \bigcup_1^n G(\Omega/M\cdot K(y_i)) \text{ is not empty.}$$

PROPOSITION 3. *Let $h(y), g(y) \in K[y]$ (that is, h and g are polynomials). Then condition (2.4) implies conditions (2.2) and (2.3). In fact, if $h = h^{(1)}(h^{(2)})$, then (2.4) implies there exist polynomials $g^{(1)}, g^{(2)} \in K[y]$ such that $g = g^{(1)}(g^{(2)})$ and*

$$(2.12)\quad \Omega_{h^{(1)}-x} = \Omega_{g^{(1)}-x};$$
$$(2.13)\quad \text{the pair } h^{(1)}, g^{(1)} \text{ satisfies (2.4); and}$$
$$(2.14)\quad h^{(1)}(y) - g^{(1)}(z) \text{ is reducible over } K.$$

Proof. Let $z_1, \cdots, z_m$ be the zeros of $g(z) - x$. From Lemma 7, there exists a polynomial $g^*(y) \in K[y]$ such that the zeros of $g^*(z) - x$ are exactly the quantities z_i^* obtained from the expression

$$K(z_i^*) = K(z_i) \cap \Omega_{h-x}.$$

From Lemma 8, $G(\Omega_{h-x}/K(z_i^*))$ is the group obtained by restricting the elements of $G(\Omega_x/K(z_i))$ to Ω_{h-x}. We thus obtain from (2.4)

$$(2.15)\qquad \bigcup_{y_i} G(\Omega_{h-x}/K(y_i)) = \bigcup_{z_j^*} G(\Omega_{h-x}/K(z_j^*)).$$

If the degree of g^* were less than the degree of h, then some power of σ_∞ (the branch cycle corresponding to the branch point $x = \infty$) would be fixed on all quantities z_j^*, but would not be fixed on the quantities y_i. This would con-

tradict (2.15). We therefore deduce that $\deg g^* > \deg h$, and

$$K(z_i) \cap \Omega_{h-x} = K(z_i) \quad \text{and} \quad \Omega_{g-x} \subset \Omega_{h-x}. \tag{2.16}$$

Interchanging the roles of h and g in this argument, we see that $\deg g = \deg h$ and $\Omega_{h-x} = \Omega_{g-x} = \Omega_x$. Thus, $G(\Omega_x/K(x))$ has two faithful permutation representations satisfying (1.7). From Lemma 3,

(2.17) $G(\Omega_x/K(y_1))$ is intransitive on $z_1, \cdots, z_n$.

Assume $h = h^{(1)}(h^{(2)})$. In order to obtain expressions (2.12), (2.13) and (2.14), apply the argument above after having restricted all elements of $G(\Omega_x/K(x))$ to $\Omega_{h^{(1)}-x}$. ∎

Proposition 4 when coupled with Proposition 2 gives necessary and sufficient conditions that a pair of rational functions h, g satisfy (2.3).

PROPOSITION 4. *Let G^* be a finite group with two inequivalent transitive permutation representations on the letters $y_1^*, \cdots, y_n^*$ and $z_1^*, \cdots, z_m^*$ respectively. If $\omega_1, \cdots, \omega_n$ are any set of letters on which it makes sense to represent G^*, for $\sigma^* \in G^*$, let σ_ω^* be the permutation of $\omega_1, \cdots, \omega_n$ corresponding to σ^*. Then there exist rational functions $h(y), g(y) \in \mathbf{C}(y)$ such that*

$$\Omega_{h-x} = \Omega_{g-x}, \tag{2.18}$$

$$G^* = G(\Omega_{h-x}/\mathbf{C}(x)) \text{ denoted } G, \tag{2.19}$$

and

(2.20) *the representation of G on the zeros $y_1, \cdots, y_n$ of $h(y) - x$ (respectively $z_1, \cdots, z_m$) is the same (up to a renaming of the letters) as the representation of G on $y_1^*, \cdots, y_n^*$ (resp. $z_1^*, \cdots, z_m^*$) if and only if there exist elements $\sigma^*(1), \cdots, \sigma^*(r) \in G^*$ such that*

(2.21) *$\sigma^*(1), \cdots, \sigma^*(r)$ generate G^*;*

(2.22) *if we let $(\sigma^*(\infty))^{-1} = \sigma^*(1) \cdots \sigma^*(r)$, then*

$$\sum_{j=1}^{r} \operatorname{ind} \sigma_{y^*}^*(j) + \operatorname{ind} \sigma_{y^*}^*(\infty) = 2(n-1)$$

and

$$\sum_{j=1}^{r} \operatorname{ind} \sigma_{z^*}^*(j) + \operatorname{ind} \sigma_{z^*}^*(\infty) = 2(m-1)$$

(see 1.2)).

Also, h and g can be chosen to be polynomials if and only if $\sigma^*(1), \cdots, \sigma^*(r)$ can be chosen so that

$$\sum_{j=1}^{r} \operatorname{ind} \sigma_{y^*}^*(j) = n-1 \quad \text{and} \quad \sum_{j=1}^{r} \operatorname{ind} \sigma_{z^*}^*(j) = m-1 \tag{2.23}$$

(here $n = m$ by Remark 2).

Proof. If there exist $h(y), g(y) \in \mathbf{C}(y)$ satisfying (2.18), (2.19), and (2.20), then the branch cycles $\sigma_1, \cdots, \sigma_r, \sigma_\infty$ for Ω_{h-x} over $\mathbf{C}(x)$, satisfy (2.21) and (2.22) when represented on $\{y_1, \cdots, y_n\}$ and $\{z_1, \cdots, z_m\}$ (see [9, p. 43] for more details on this and the rest of the argument, in relation to the use of

Riemann surfaces). The fact that (2.21) and (2.22) yield (2.18), (2.19), and (2.20) follows from the well-known scissors and paste construction of a Riemann surface having finite branch cycles (as a cover of the sphere) $\{\sigma_{z^*}^*(i)\}_{i=1}^r$ (respectively $\{\sigma_{z^*}^*(i)\}_{i=1}^r$). Riemann's existence theorem implies that these surfaces have an algebraic structure, and from the Riemann-Hurwitz formula the genus of these surfaces is 0. Thus, these Riemann surfaces described above are the Riemann surfaces corresponding to $h(y) - x$ and $g(z) - x$ for two rational functions h and g.

Then h and g are polynomials, if σ_∞ (the branch cycle for $x = \infty$) is an n-cycle on both sets $\{y_1, \cdots, y_n\}$ and $\{z_1, \cdots, z_m\}$. This implies (2.23) must hold if we choose $\sigma^*(1), \cdots, \sigma^*(r)$ to represent finite branch cycles in the construction alluded to above. ∎

The next two propositions are important for applications where $h(y)$ is decomposable and the hypotheses of Theorem 1 are not satisfied. See [10, p. 83].

PROPOSITION 5. *Let $h(y), g(y) \in K(y)$. We denote the zeros of $h(y) - x$ by $y_1, \cdots, y_m$; the zeros of $g(z) - x$ by $z_1, \cdots, z_m$. Suppose*

(2.24) *$h(y) - g(z)$ is reducible over K,*

but

(2.25) *$h^{(1)}(y) - g^{(1)}(z)$ is not reducible for any rational functions $h^{(1)}$, $g^{(1)}$ which are composition factors of h, g respectively such that either* $\deg h^{(1)} < \deg h$ *or* $\deg g^{(1)} < \deg g$.

If $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$ are the conjugates of z_1 over $K(y_1)$, let F be the field obtained by adjoining to K the symmetric functions in $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$. Then

$$F = K(y_1). \tag{2.26}$$

Proof. From Proposition 2 we must have $\Omega_{h-x} = \Omega_{g-x}$. Let Ω^* be a fixed algebraic closure of Ω_{h-x}. If $\sigma \in G(\Omega_{h-x}/K(y_i))$, then σ permutes the field elements $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$. Therefore σ is elementwise fixed on F and by the fundamental theorem of Galois theory, $F \subset K(y_1)$.

Conversely, any isomorphism σ of Ω_{h-x} into Ω^*, fixed on F, must permute the elements $z_1, z_{\alpha(2)}, \cdots, Z_{\alpha(k)}$. Therefore

$$\sigma(g(z_1)) = \sigma(x) = g(\sigma(z_1)) = g(z_{\alpha(i)}) = x \quad \text{for some integer } i. \tag{2.27}$$

By Galois theory this implies

$$K(x) \subset F \subset K(y_1). \tag{2.28}$$

From Lemma 7, $F = K(r(y_1))$ where r, $h^{(1)} \in K[y]$ are polynomials such that $h^{(1)}(r(y_1)) = h(y_1)$. If ω is one of the symmetric functions in $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$, then ω is a rational function in $r(y_1)$. Also, ω is a sum of products of elements integral over $K[x]$. As $K[r(y_1)]$ is the integral closure of $K[x]$ in F,

we have $K[x, \omega] \subseteq K[r(y_1)]$. Thus, ω is a polynomial in $r(y_1)$ and we deduce that

$$h^{(1)}(r(y)) - g(z) = \phi_1(r(y), z) \cdot \phi_2(y, z) \tag{2.29}$$

where $\phi_1, \phi_2 \in K[y, z]$ and the coefficients of ϕ_i are symmetric functions in $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$. Now, if $\phi_2(y, z)$ were contained in $K[r(y), z]$, then $h^{(1)}(y) - g(z)$ would be a reducible polynomial in two variables, contrary to (2.25). More generally, suppose $S(r(y), z)$ divides $T(r(y), z)$ as polynomials in two variables. We claim that the quotient

$$T(r(y), z)/S(r(y), z) = R(y, z)$$

is in $K[r(y), z]$. The rational function $T(u, z)/S(u, z)$ is not a polynomial in u, z if and only if there exists finite $(u_0, z_0) \in \mathbf{C}^2$ such that $T(u_0, z_0) \neq 0$, $S(u_0, z_0) = 0$. Let y_0 be such that $r(y_0) = u_0$. Then $R(y_0, z_0) = \infty$, contrary to the fact that the polynomial $R(y, z)$ takes finite values at finite places (y_0, z_0). ∎

PROPOSITION 6. *Let $h(y), g(y) \in K[y]$ (that is, h and g are polynomials). Assume that (2.24) and (2.25) of Proposition 5 holds. Assume, in addition,*

(2.30) *there exists $x_0 \in \mathbf{C} \cup \{\infty\}$ such that $g(z) - x_0$ has a zero of multiplicity p^u (that is, some power of a prime integer) and p^u does not divide the multiplicity of any other zero of $g(z) - x_0$.*

In particular, (2.30) holds if $x_0 = \infty$ and deg *g is a prime power.*

Then there exist constants $a \neq 0$, $b \in \mathbf{C}$ such that,

$$ay_1 + b = z_1 + z_{\alpha(2)} + \cdots z_{\alpha(k)} \tag{2.31}$$

where $z_1, \cdots, z_{\alpha(k)}$ are the conjugates of z_1 over $K(y_1)$.

Remark 3. From Proposition 2, (2.24) and (2.25) imply that $\Omega_{h-x} = \Omega_{g-x}$. Thus (2.31) implies that the representations of $G(\Omega_{h-x}/K(x))$ on the letters $\{y_1, \cdots, y_n\}$ and $\{z_1, \cdots, z_n\}$ are equivalent. In particular (2.4) holds.

Proof. First we recall that if a_0 is a zero of $g(z) - x_0$ of multiplicity m, then the Puiseux expansions for $g(z) - x$ about x_0, corresponding to the center (a_0, x_0), are of form

$$\begin{aligned}
z_{r(1)} &= a_0 + a_1(x - x_0)^{1/m} + a_2(x - x_0)^{2/m} + \cdots \\
z_{r(2)} &= a_0 + a_1\zeta_m(x - x_0)^{1/m} + a_2\,\zeta_m^2(x - x_0)^{2/m} + \cdots \\
&\vdots \\
z_{r(m)} &= a_0 + a_1\,\zeta_m^{m-1}(x - x_0)^{1/m} + \cdots
\end{aligned} \tag{2.32}$$

where $a_1 \neq 0$ and ζ_m is a primitive m-th root of 1. This holds only for $a_0 \neq \infty$, but corresponding expansions are easily obtained for $a_0 = \infty$. From Proposition 5, $K(y_1) = F$ (statement (2.26)). Using Remark 3, we have $\Omega_{h-x} =$

Ω_{g-x}, so that the orders of the inertial groups for primes over x_0 in both Ω_{h-x} and Ω_{g-x} are the same. Therefore, we may without loss assume that y_1 has a Puiseux expansion for x_0 of ramification order divisible by p^u.

Let $h(y_1) - g(z)$ have a factorization of the form $\pi_1^t \phi_i(y_1, z)$ into irreducible factors over $K(y_1)$. We assume that z_1 is a zero of $\phi_1(y_1, z)$. The complete set of zeros of $\phi_1(y_1, z)$ is therefore $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$; and the coefficient of z^{k-1} is

$$z_1 + z_{\alpha(2)} + \cdots + z_{\alpha(k)} = y^*.$$

However, the coefficient of z^{k-1} in $\phi_1(y_1, z)$ is linear in y_1. Therefore we have established the proposition if we show that y^* is not a constant.

Let $m = p^u$ in (2.32). Let c be the coefficient of $(x - x_0)^{1/p^u}$ in y^*. Then c is actually a_1 times a sum of p^u-th roots of 1. Some, but not necessarily all, of the elements $z_{r(1)}, \cdots, z_{r(m)}$ appear among $z_1, \cdots, z_{\alpha(k)}$. Suppose $c = 0$. Then the expression for c results in an equation

$$f(\zeta_{p^u}) = 0 \tag{2.33}$$

where f is a polynomial whose coefficients are 0's or 1's. However, $f(x)$ is divisible by $(x^{p^u} - 1)/(x^{p^{u-1}} - 1)$, so

$$f(x) = g(x)((x^{p^u} - 1)/(x^{p^{u-1}} - 1)) \tag{2.34}$$

where $g(x)$ is a polynomial of degree $\leq p^{u-1} - 1$. From this expression we see that if

$$f(x) = \sum_{i=0}^{p^u} a_i x^i \quad \text{and} \quad A = \{i \text{ modulo } p^u \mid a_i \neq 0\},$$

then $B = \{i + p^{u-1} \bmod p^u \mid i \in A\}$ is identically the same set as A. Consider σ to be any extension to Ω_{h-x} of the automorphism obtained from

$$(x - x_0)^{1/p^u} \to \zeta_p (x - x_0)^{1/p^u} \tag{2.35}$$

where ζ_p is a primitive p-th root of 1. Then the preceding discussion shows that the symmetric function in $z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}$ are fixed by σ because the set

$$\{z_1, z_{\alpha(2)}, \cdots, z_{\alpha(k)}\}$$

is invariant under transformation by σ. However, y_1 is not fixed by σ. This contradicts $K(y_1) = F$. Thus y^* is not a constant. ∎

Our next theorem goes a long way toward characterizing polynomial pairs h, g such that h is indecomposable and $h(y) - g(z)$ is reducible. For the applications it would be of interest to consider the case where h is an indecomposable polynomial and g is a rational function (rather than a polynomial).

THEOREM 1. *Let $h(y) \in K[y]$ be an indecomposable polynomial. If $g(y) \in K[y]$ is a polynomial such that*

(2.36) *$h(y) - g(z)$ is reducible as a polynomial in two variables, then Proposition 2 implies (by replacing g by a composition factor of g) that we may assume*

$$\deg g = \deg h = n \quad \text{and} \quad \Omega_{h-x} = \Omega_{g-x}. \tag{2.37}$$

Let $h(y) - g(z) = \pi_1^t \phi_i(y, z)$ *where* $\phi_i(y, z)$ *are absolutely irreducible polynomials. Then:*

(2.38) $g(y)$ *is indecomposable;*

(2.39) $t = 2$, *so that* $h(y) - g(z)$ *has exactly two irreducible factors, unless* h *and* g *are linearly related (see Definition* 4) *and* h *is a cyclic or Chebychev polynomial* [9, p. 41];

(2.40) *if* $\deg \phi_1 = k$, *then* $n - 1 \mid k(k-1)$ *and there exists a difference set* $\{1, \alpha(2), \cdots, \alpha(k)\}$ *modulo* n *whose automorphism group is doubly transitive;*

and

(2.41) *the Riemann surface for* $h(y) - x$ *over the* x*-sphere has at most three finite branch points.*

In addition, suppose that K *is a field such that*

(2.42) $K \cap Q(\zeta_n) \subset M$ *where* M *is the totally real subfield of* $Q(\zeta_n)$.

Then

(2.43) h *and* g *must be linearly related. In particular if* $K = \mathbf{Q}$ (*that is,* h, $g \in \mathbf{Q}[y]$) *and* (2.36) *holds* (*assuming* (2.37)), *then* h *and* g *are linearly related.*

Proof. From Lemma 9 of [9], since h is indecomposable $G(\Omega_{h-x}/K(x))$ is doubly transitive as a permutation group on $y_1, \cdots, y_n$ (the zeros of $h(y) - x$), unless h is a cyclic or Chebychev polynomial. In the case that h is a cyclic or Chebychev polynomial, Lemma 11 of [9] shows that h and g are linearly related. Assume (2.36), and therefore (2.37) holds. If $\deg \phi_1(y, z) = k$, the coefficient of y^{k-1} in $\phi_1(y, z_1)$ is linear in z_1, where $z_1, \cdots, z_n$ are the zeros of $g(z) - x$. Then we obtain

$$az_1 + b = y_1 + y_{\alpha(2)} + \cdots + y_{\alpha(k)} .$$

As already noted in the proof of Lemma 2, a doubly transitive permutation representation is the direct sum of an irreducible representation and the identity representation. Thus, the subspace of relations

$$\{\sum a_i y_i = b \text{ with } a_1, \cdots, a_n, b \in K\}$$

is of dimension 1, generated by $\sum_{i=1}^n y_i - c = 0$ for some $c \in K$. In particular we deduce that $y_1 + y_{\alpha(2)} + \cdots + y_{\alpha(k)}$ is not constant. From this we see that the representations of $G(\Omega_{h-x}/K(x))$ on $\{y_1, \cdots, y_n\}$ and on $\{z_1, \cdots, z_n\}$ are equivalent.

From Proposition 3 we conclude that $g(y)$ is indecomposable. Thus we have two doubly transitive representations of $G(\Omega_{h-x}/K(x))$. Therefore (2.39) and (2.40) follow from Lemma 4 (since the branch cycle for $x = \infty$ is an n-cycle in both representations).

The hypotheses for Proposition 1 now hold. Thus, each of the finite branch cycles $\sigma_y(1), \cdots, \sigma_y(r)$, for the Riemann surface of $h(y) - x$, moves

at least half the letters. It is easy to see that this implies

$$\text{ind } \sigma_y(i) \geq n/4 \quad \text{for} \quad i = 1, \cdots, r. \tag{2.44}$$

However, since $\sum_{i=1}^{r} \sigma_y(i) = n - 1$, we must have $r \leq 3$. This demonstrates (2.41). The remainder of the theorem, expression (2.42), is a consequence (special case) of Theorem 2 applied to the function fields of $h(y) - x$ and $g(z) - x$. ∎

Remark 4. Let $h, g \in \mathbf{C}[y]$ be two polynomials such that $\Omega_{h-x} = \Omega_{g-y}$. If $\deg h$ is a prime, then Lemma 3 implies that $h(y) - g(z)$ is reducible. Indeed, this also can be shown if $\deg h$ is $2 \cdot p$ for p a prime. In fact, there do not *seem* to be known any examples of pairs (G, T_i), $i = 1, 2$ where T_1 and T_2 are inequivalent doubly transitive representations of the same degree such that there exists $\sigma \in G$ with $T_1(\sigma)$ and $T_2(\sigma)$ both n-cycles. If there were no such examples, then, combining Proposition 2 and Proposition 4, there would be essentially an equivalence between the relations $\Omega_{h-x} = \Omega_{g-x}$ and $h(y) - g(z)$ reducible, for h and g *both polynomials.*

PROPOSITION 7. *Suppose* $h(y) - g(z) = \pi_1^t \phi_i(y, z)$ *where* h *and* g *are polynomials and* $\deg h = p$ *(a prime integer). From Theorem* 1, *we may assume* $\deg g = \deg h$ *and* $t = 2$ *(where* ϕ_1 *and* ϕ_2 *are absolutely irreducible). Assume* $\deg_y \phi_1$ *and* $\deg_y \phi_2 > 1$. *Then, there exist polynomials* h^* *and* g^* *such that:*

$$\deg h^* = \deg g^* = p; \tag{2.45}$$

$h^*(y) - g^*(z)$ *is reducible (or equivalently from Lemma* 3, $\Omega_{h^*-x} = \Omega_{g^*-x}$) *but has no linear factors; and* (2.46)

the Riemann surface for $h^*(y) - x$ *has exactly two finite branch points over the* x*-sphere.* (2.47)

Proof. From Theorem 1 (expression (2.41)) we may assume that the Riemann surface for $h(y) - x$ has no more than three finite branch points over the x-sphere. Actually using (2.41) is not essential to this proposition, and it could be replaced by an induction process. Let $\sigma_y(1)$, $\sigma_y(2)$, and σ_y (3) be branch cycles corresponding to these points. If σ_y (1) and σ_y (3) both fixed at most one letter, then h would be a cyclic or a Chebychev polynomial (Lemma 9 of [9]). Thus we assume $\sigma_y(1)$ fixes at least 2 letters among $y_1, \cdots, y_n$. Consider the subgroup H of $G(\Omega_{h-x}/\mathbf{C}(x))$ generated by $\sigma(1) = \sigma^*(1)$ and $\sigma(2) \cdot \sigma(3) = \sigma^*(2)$. Then if we replace G^* by H in Proposition 4, we conclude that there exist polynomials h^* and g^* of degree p such that $h^*(y) - g^*(z)$ is reducible, the Riemann surface for $h^*(y) - x$ over the x-sphere has finite branch cycles $\sigma_y^*(1)$ and $\sigma_y^*(2)$, and the irreducible factors of $h^*(y) - g^*(z)$ are in one-to-one correspondence with the orbits of H_1 on $z_1, \cdots, z_p$ where H_1 is the stabilizer of y_1 in the subgroup H of $G(\Omega_{h-x}/\mathbf{C}(x))$. The number of such orbits is at least 2, and must be 3 if one of these orbits is of length 1 (that is, $h^*(y) - g^*(z)$ has an irreducible factor of degree 1).

However, if $h^*(y) - g^*(z)$ has three irreducible factors, then (2.39) implies that $h^*(y)$ is a cyclic or Chebychev polynomials. This is impossible (Lemma 9 of [9]) because $\sigma_y^*(1)$ fixes two letters. This contradiction concludes the Proposition since h^* and g^* cannot be linearly related. ∎

3. Fields of definition of function fields

Let K be a number field, and let Z be a projective curve equipped with a morphism $\phi : Z \to \mathbf{P}'(\mathbf{C})$ such that Z and ϕ are both defined over K. Let $\Omega_{K(Z)}$ be the normal closure of $K(Z)$ (the field of K-rational functions on Z) over $K(\mathbf{P}'(\mathbf{C}))$. The field $\Omega_{K(Z)}$ was called $K(Z)\hat{}$ in the introduction of this paper. Let T be the permutation representation of $G(\Omega_{K(Z)}/K(\mathbf{P}'))$ obtained from the action of G on the set of conjugates of some primitive generator of $K(Z)$ over $K(\mathbf{P}')$. Suppose also that

(3.1) G is equipped with two (permutation inequivalent) doubly transitive permutation representations $T_1 = T$ and T_2 which are equivalent as group representations.

Let ζ_n be a primitive n-th root of 1. Then, $G(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ can be identified with the invertible elements $\mathfrak{g}$ of the ring $\mathbf{Z}/(n)$. From Lemma 4, the situation (3.1) yields a difference set modulo n, and the multipliers of this difference set, $\mathfrak{M}$ (see Definition 2), form a non-empty subgroup of $\mathfrak{g}$ such that $\mathfrak{g}/\mathfrak{M}$ is not the trivial group (Lemma 5). Let $M(\mathfrak{M})$ denote the fixed field in $\mathbf{Q}(\zeta_n)$ of $\mathfrak{M}$, so $M(\mathfrak{M}) \neq \mathbf{Q}$.

THEOREM 2. *With the above assumptions, assume also that*

(3.2) *there exists a place (which we may assume to be ∞) of $\mathbf{P}'(\mathbf{C})$ which is totally ramified in Z.*

Then,

$$K \supseteq M(\mathfrak{M}). \tag{3.3}$$

Proof. The permutation representation T_2 (of (3.1)) yields a curve

$$\psi : Y \to \mathbf{P}'(\mathbf{C})$$

such that Y and ψ are also defined over K. Let y_1 be a primitive generator of $K(Y)$ over $K(\mathbf{P}'(\mathbf{C}))$, $\{y_i\}_1^n$ the conjugates of y_1 and $y_1, y_{\alpha(2)}, \cdots, y_{\alpha(k)}$ the conjugates of y_1 over $K(Z)$.

Let $z_1 = y_1 + y_{\alpha(2)} + \cdots + y_{\alpha(k)}$ and

$$z_i = \sigma_\infty^{i-1}(z_1) = y_{1+i-1} + y_{\alpha(2)+i-1} + \cdots + y_{\alpha(k)+i-1} \quad \text{for } i = 1, \cdots, n,$$

where σ_∞ is the branch cycle corresponding to the totally ramified place ∞. For Theorem 2 we may replace K by $K \cap \mathbf{Q}(\zeta_n)$. Assume that

$$\tau \in G(M(\mathfrak{M})/K \cap M(\mathfrak{M}))$$

so that τ is represented by a non-multiplier of the difference set. Since Z (respectively Y) is defined over K, and ∞ is totally ramified in Z (respectively Y), we may assume that y_1 and z_1 are fixed by the action of τ on their Puiseux expansions about ∞, while

$$\tau(y_{\alpha(i)}) = y_{\tau(\alpha(i)-1)+1} \tag{3.4}$$

where $\tau(\alpha(i) - 1)$ is the action of τ (as a multiplier modulo n) on $(\alpha(i) - 1)$ modulo n. Since τ is not a multiplier, the sets $\{\tau(\alpha(i) - 1)\}_{i=1}^{k}$ and $\{\alpha(i) - 1\}_{i=1}^{k}$ are distinct. Therefore (since $\tau(z_1) = z_1$), we have two representations of z_1 as a sum of elements $\{y_i\}_1^n$ which yields a relationship

$$y_1 + y_{\alpha(2)} + \cdots + y_{\alpha(k)} = y_1 + y_{\tau(\alpha(2)-1)+1} + \cdots + y_{\tau(\alpha(k)-1)+1}, \tag{3.5}$$

a non-trivial relationship among the $\{y_i\}_1^n$. As noted in the proof of Theorem 1, this contradicts the double transitivity of the representation T_1. ∎

An easy generalization of the theorem of [10, p. 83] yields the next proposition. The proof is quite combinatorial and utilizes Propositions 5 and 6.

PROPOSITION 8. *Let $\phi : Z \to \mathbf{P}'(\mathbf{C})$ be a covering morphism such that ϕ and the (projective) curve Z are defined over K. Suppose for the pair (G, T) (notation as above), there exist two representations of the same degree; $T_1 = T$ and T_2 of G which are permutation inequivalent, but $G(K(Z)^{\wedge}/K(Z))$ is not transitive in the restriction of T_2 to this group. Suppose also that there exists a place $\mathfrak{p}$ of $\mathbf{P}'(\mathbf{C})$ such that the branch cycle $\sigma_{\mathfrak{p}}$ corresponding to $\mathfrak{p}$ (and the representation T_1) has a decomposition into disjoint cycles of the form*

$$\sigma_{\mathfrak{p}} = (s(1, \sigma_{\mathfrak{p}}))(s(2, \sigma_{\mathfrak{p}})) \cdots (s(k(_{\mathfrak{p}}), \sigma_{\mathfrak{p}})) \tag{3.6}$$

(as in (1.2)), where

$$s(1, \sigma_{\mathfrak{p}}) = p^u \quad \text{for some prime } p \neq 2 \text{ and integer } u \geq 1, \tag{3.7}$$

and

$$p^u \nmid s(i, \sigma_{\mathfrak{p}}) \quad \text{for } i \neq 1. \tag{3.8}$$

Then

$$K \cap \mathbf{Q}(\zeta_{p^u}) \neq \mathbf{Q}. \tag{3.9}$$

We do not know to what extent the condition (3.2) can be removed from Theorem 2 (except where Proposition 8 is applicable). However, we suspect that the removal of (3.2) requires a fairly deep contribution to arithmetic (if it can be done). General principles (as in [12]) allow us to revert to the case where all ramified places of Z (in $\phi : Z \to \mathbf{P}'(\mathbf{C})$) are defined over K.

BIBLIOGRAPHY

1. R. D. CHARMICHAEL, *Introduction to the theory of groups of finite order*, Ginn, Boston, 1967.

2. J. W. S. Cassels, *Factorization of polynomials in several variables*, Proc. 15th Scandinavian Congress, Oslo, 1968, Springer Lecture Notes in Mathematics, pp. 1–17.
3. S. Chowla and H. Ryser, *Combinatorial problems*, Canadian J. Math., vol. 2 (1950), pp. 93–99.
4. H. Davenport and A. Schinzel, *Two problems concerning polynomials*, J. Riene Angew Math., vol. 214 (1964), pp. 386–391.
5. H. Davenport, D. J. Lewis, and A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math Oxford (2), vol. 12 (1961), pp. 304–312.
6. L. Ehrenfucht, *Kryterium absolutnej nierokladnósci wielominów*, Prace Mat., vol. 2 (1958), pp. 167–169.
7. W. Feit. *Automorphisms of balanced incomplete block designs*, Math. Zeitschr., vol. 118 (1970), pp. 40–49.
8. M. Fried and R. MacRae, *On the invariance of chains of fields*, Illinois J. Math., vol. 13 (1969), pp. 165–171.
9. M. Fried, *On a conjecture of Schur*, Michigan Math. J., vol. 17 (1970), pp. 41–55.
10. ———, *On the diophantine equation* $f(y) = x$, Acta Arith., vol. XIX (1971), pp. 79–87.
11. ———, *On Hilbert's irreducibility theorem*, J. Number Theory, June, 1972.
12. M. Fried and D. Lewis, *Solution spaces to Diophantine problems*, Invited talk, Bull. Amer. Math. Soc., to appear.
13. M. Fried and A. Schinzel, *On the reducibility of quadrinomials*, Acta Arithm. (Serpinski Volume, 1972).
14. M. Fried and J. A. Smith, *Primitive groups, Moore graphs, and rational curves*, Michigan Math, J., to appear.
15. M. Hall, Jr., *The theory of groups*. MacMillan, New York, 1963.
16. H. Ryser, *Combinatorial mathematics*, Wiley, New York, 1963.
17. A. Schinzel, *Some unsolved problems on polynomials*, Mathematička Biblioteka, vol. 25 (1963), pp. 63–70.

Institute for Advanced Study
Princeton, New Jersey
The University of Michigan
Ann Arbor, Michigan
State University of New York at Stony Brook
Stony Brook, New York