Journal für die reine und angewandte Mathematik

Herausgegeben von **Helmut Hasse** und **Hans Rohrbach**

Sonderdruck aus Band 264, Seite 40 bis 55

Verlag Walter de Gruyter · Berlin · New York 1973

On a theorem of Ritt and related Diophantine problems

By Michael Fried at Stony Brook

On a theorem of Ritt and related Diophantine problems

By *Michael Fried* at Stony Brook

Introduction

In [8], J. Ritt carried out certain computations which showed very precisely the lattice structure of the fields between $k(x)$ and $k(f(x))$ where $f(x) \in k[x]$ and $k = \mathbb{C}$ (the complex field). Our theorems 1 and 2 collect together Ritt's results. Theorem 3 (and Theorem 4) can be regarded as a generalization of Ritt's Theorem (and itself offers a simple proof of Ritt's Theorem). As a corollary we classify the set of irreducible curves represented in $\boldsymbol{P}^2(\mathbb{C})$ by the zeros of a factor of a polynomial of form $f(x) - g(y)$ where $f, g \in K[x]$ (K an algebraic number field) that have infinitely many K-integral points. This problem was considered in special cases by Davenport, Lewis, and Schinzel [1], LeVeque [7], and many others.

In [5] the author concerned himself with an arithmetic problem he called the 'generalized Schur conjecture.' Of importance was the phenomena: $f \in k(x)$ where $f = f_1(f_2)$ (composition of rational functions) with $f_i \in \hat{k}(x)$, $i = 1, 2$ (where $\hat{k}$ is an algebraic closure of k) but $f_i \notin k(x)$. Theorem 5 is a contribution to the investigation of this problem when f_1 is a polynomial.

Given a function field F in one variable over the field $\mathbb{C}$, Riemann's existence theorem provides a powerful tool for studying the field extensions of F. However, it is not so easy to investigate the lattice of subfields of F (defined over $\mathbb{C}$). A theorem due to Severi ([9], p. 68) implies that F contains but finitely many subfields of genus greater than 1. Since the coverings of genus 1 curves by genus 1 curves have a welldeveloped theory, as a first approximation to investigating the general problem it would seem reasonable to take F of genus zero. In this light, this paper may be regarded as a contribution to this problem.

This paper received its impetus from a large number of conversations between the author and other number theorists concerning certain arithmetic problems. A host of arithmetic problems *can* be attacked by the methods of this paper. However, one of the more intriguing (and undoubtedly difficult) problems in this area remains unsolved. Let G be a finite group with a given permutation representation $T\colon G \to S_n$ (where S_n is the symmetric group on n letters). Let L be a function field over $\mathbb{C}(x)$, L^* its Galois closure. For what integers g does there exist a function field $L/\mathbb{C}(x)$ such that L is of genus g and $G(L^*/\mathbb{C}(x))$ induces the representation T on the fields conjugate to L? In particular (related to this paper) investigate the case $g = 0$. The problem is much easier if we demand that $f(x) \in \mathbb{C}[x]$, and the problem can be shown by Theorem 2 to have a negative answer in many cases. Even without this restriction, the problem has a negative answer for

some pairs (G, T) (examples obtained by the author result from a generalization of techniques used by W. Feit in [2]). However, to date there are but finitely many examples where the problem is answered negatively, and no theory (known to the author) exists.

Section 1. Ritt's Theorem and the computation of genus

In [8], p. 51, Ritt proved a theorem which very precisely gave the decomposition pattern of a polynomial $f(x) \in \mathbb{C}[x]$. His theorem had two parts (Theorems 1 and 2 below). The author and MacRae gave two short, completely algebraic proofs of the first (and easier) part, in [3a]. In this section we introduce some concepts which enable us to simplify the combinatorial nature of part 2 of Ritt's theorem. Theorem 3 and the results of Section 2 can be regarded as generalizations of this result.

Lemma 1. *Let k be an arbitrary field and let $f(x) \in k[x]$ such that*

$$\text{g.c.d. } (\deg f(x), \text{char } k) = 1 \text{ or } \text{char } k = 0.$$

Let $\hat{k}$ be a fixed algebraic closure of k. Then the correspondence $M \to k \cdot M$ (composition of fields over k) establishes a relative degree preserving isomorphism of the lattice of fields intermediate between $k(x)$ and $k(f(x))$ onto the lattice of fields intermediate between $\hat{k}(x)$ and $\hat{k}(f(x))$. (Theorem 3. 5 of [3a].)

It has already been observed (p. 225 of [3b]; Section 1 of [5]) that neither of the assumptions ((deg $f(x)$, char k) = 1 or $f(x)$ is a polynomial) may be dropped.

Lemma 1 reduces the proof of the next theorem to the case where k is algebraically closed ($k = \hat{k}$). Ritt proved this result for $k = \mathbb{C}$.

Theorem 1. *Let k be an arbitrary field and let $z = f(x)$ be a polynomial in $k[x]$ such that* g.c.d. $(\text{char } k, \deg f(x)) = 1$ *or* $\text{char } (k) = 0$. *If M_1, M_2 are fields intermediate between $L = k(x)$ and $K = k(f(x))$, then $[M_1 \cap M_2 : K] =$* g.c.d. $([M_1 : K], [M_2 : K])$ *and* $[M_1 \cdot M_2 : K] =$ l.c.m. $([M_1 : K], [M_2 : K])$. (Theorem 3. 6 of [3a].)

Definition 1. Let k be any field and let $f(x)$, $g(x)$ be two rational functions. We say f, g, are *linearly equivalent* if there exist constants a, b, c, d such that $f(x) = \dfrac{ag(x) + b}{cg(x) + d}$.

Lemma 2. *With the notation above; there is a one-one correspondence between linear equivalence classes of rational functions $h_2(x)$ such that $h_1(h_2(x)) = f(x)$, and fields M between $k(x)$ and $k(f(x))$. This correspondence is given by: $h_2(x) \to k(h_2(x)) \subset k(x)$.* (Proposition 3. 4 of [3a].)

Theorem 1 combined with Lemma 2 yields a simple picture of the lattice structure of the fields between $k(x)$ and $k(f(x))$ when the assumptions of Theorem 1 hold.

Before stating the second half of Ritt's theorem we introduce a more general problem. Let $g_1, h_1 \in k(x)$ be rational functions. For z an indeterminate let $x_1, \ldots, x_n$ (respectively $y_1, \ldots, y_m$) be the zeros of $g_1(x) - z$ (respectively $h_1(y) - z$). Consider the *special assumption*:

(1. 1) $g_1(x) - h_1(y)$ is an irreducible rational function in two variables over $\hat{k}$.

Equivalently,

(1. 2) $\hat{k}(x_1, y_i)$ is isomorphic over $\hat{k}(x_1)$ to $\hat{k}(x_1, y_1)$ for $i = 1, \ldots, m$.

If $(\deg g_1, \deg h_1) = 1$, then (1. 1) is satisfied because the place $z = \infty$ of $\hat{k}(z)$ has ramification index equal to l.c.m. $(\deg g_1, \deg h_1) = \deg g_1 \cdot \deg h_1$ in $k(x_1, y_1)$. Thus

$[\hat{k}(x_1, y_1)\colon \hat{k}(x_1)] = \deg g_1$. See Lemma 7 for a method for investigating conditions implying (1. 1) in the general case.

Problem 1. For fixed integers n and m, characterize the rational function pairs g_1, h_1 ($\deg g_1 = n$, $\deg h_1 = m$) such that (1. 1) holds and

(1. 3) $\hat{k}(x_1, y_1)$ is a function field of genus zero.

Problem 2. Same as Problem 1, except we add the additional hypothesis that

(1. 4) g_1, h_1 are both polynomials.

In the remainder of this section we assume that the reader is familiar with the facts used on pages 42—44 of [4]. The reader familiar with compact Riemann surfaces will have no difficulty. Let Ω_{g_1-z} denote the splitting field of $g_1(x) - z$ over $\hat{k}(z)$. *We now make the assumption that* char $\hat{k} = 0$. *However, we need only the condition that* $\hat{k}(x_1)$ *is tamely ramified over* $\hat{k}(z)$ (see [4], p. 45). We denote by

$$\sigma(1), \ldots, \sigma(r), \sigma(\infty) \in G(\Omega_{g_1-z} \cdot \Omega_{h_1-z}/\hat{k}(z))$$

branch cycles corresponding to the branch points $\lambda_1, \ldots, \lambda_r, \infty$ of $\Omega_{g_1-z} \cdot \Omega_{h_1-z}$ over $\hat{k}(z)$. Throughout $G(L/K)$ denotes the Galois group of the field L over the field K. It is desirable to view the action of the branch cycles on Ω_{g_1-z} and Ω_{h_1-z} respectively. For this purpose we denote by $\sigma(i, x)$ (respectively $\sigma(i, z)$) the permutation of $x_1, \ldots, x_n$ (respectively $y_1, \ldots, y_m$) obtained by restricting $\sigma(i)$ to Ω_{g_1-z} (respectively Ω_{h_1-z}). By abuse of notation we sometimes write: tr $\sigma(i, x) \overset{\text{def}}{=}$ the number of letters fixed by $\sigma(i, x)$, and

$$\begin{aligned} \sigma(i, x) &= (s(i, 1)) \cdots (s(i, k_i)) \\ \sigma(i, y) &= (t(i, 1)) \cdots (t(i, l_i)) \end{aligned} \tag{1. 5}$$

where $s(i, 1), \ldots, s(i, k_i)$ (respectively $t(i, 1), \ldots, t(i, l_i)$) are the lengths of the disjoints cycles of $\sigma(i, x)$ (respectively $\sigma(i, y)$). Also define ind $\sigma(i, x) \overset{\text{def}}{=} \sum_{j=1}^{k_i} (s(i, j) - 1)$.

Proposition 1. *Let* $g_1, h_1 \in \hat{k}(x)$ *and assume that* (1. 1) *holds. Then the genus of* $\hat{k}(x_1, y_1)$ *(in the previous notation) is given by* p *where*

$$\begin{aligned} 2(\deg g_1 + p - 1) = &\sum_{i=1}^{r} \sum_{j=1}^{l_i} \sum_{v=1}^{k_i} (s(i, v) - (s(i, v), t(i, j))) \\ &+ \sum_{j=1}^{l_\infty} \sum_{v=1}^{k_\infty} (s(\infty, v) - (s(\infty, v), t(\infty, v))). \end{aligned} \tag{1. 6}$$

In particular, if $g_1, h_1 \in \hat{k}[x]$, *then*

$$2(\deg g_1 + p - 1) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \sum_{v=1}^{k_i} (s(i, v) - (s(i, v), t(i, j))) + n - (n, m) \tag{1. 7}$$

where $n = \deg g_1$, $m = \deg h_1$.

Suppose g_1 *satisfies*:

$$\frac{g_1(x) - g_1(y)}{x - y} \text{ is absolutely irreducible.} \tag{1. 8}$$

Then, the genus of $\hat{k}(x_1, x_2)$ *is given by* p *where*

$$\begin{aligned} 2(\deg g_1 + p - 2) = &\sum_{i=1}^{r} \sum_{j=1}^{k_i} \sum_{v=1}^{k_i} (s(i, v) - (s(i, v), s(i, j))) \\ &+ \sum_{v=1}^{k_\infty} \sum_{j=1}^{k_\infty} (s(\infty, v) - (s(\infty, v), s(\infty, j))). \end{aligned} \tag{1. 9}$$

Proof. This is an application of the Riemann-Hurwitz formula. For details see [5], Prop. 2.

Lemma 3. *Let* $\sigma(1), \ldots, \sigma(r) \in S_n$ *(the symmetric group on n letters). Assume*

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

Then there exists a polynomial $f(x)$ *of degree n such that* $f(x) - z$ *has a description of its finite branch cycles given by* $\{\sigma(i)\}_{i=1}^{r}$ *iff* $\sigma(1), \ldots, \sigma(r)$ *generate a transitive subgroup of* S_n.

Proof. Let $\left(\prod_{i=1}^{r} \sigma(i)\right)^{-1} \stackrel{\text{def}}{=} \sigma(\infty)$. If $f(x)$ does exist with the properties described in the statement of the lemma, then the branch cycle over ∞ for the Riemann surface of $f(x) - z$ (over the z-sphere) is $\sigma(\infty)$. However $\sigma(\infty)$ must be an n-cycle, since $f(x)$ is a polynomial.

Conversely, if $\sigma(1), \ldots, \sigma(r)$ do generate a transitive subgroup of S_n, then (by a well-known construction) we can construct a connected Riemann surface over the z-sphere having $\sigma(1), \ldots, \sigma(r), \sigma(\infty)$ as branch cycles. By the Riemann-Hurwitz formula, the genus of this surface is given by p where

$$2(n + p - 1) = \sum_{i=1}^{r} \operatorname{ind} \sigma(i) + \operatorname{ind}(\sigma(\infty)). \tag{1.11}$$

Thus (from (1.10))

$$n - 1 + 2p = \operatorname{ind}(\sigma(\infty)). \tag{1.12}$$

Thus $\sigma(\infty)$ is an n-cycle and $p = 0$. This implies that the Riemann surface is the Riemann surface of $f(x) - z$, for some polynomial $f(x)$.

Lemma 4. *Let* $\langle\sigma(1)\rangle, \ldots, \langle\sigma(r)\rangle$ *represent r conjugacy classes of* S_n *such that*

$$\sum_{i=1}^{r} \operatorname{ind} \langle\sigma(i)\rangle = n - 1, \tag{1.13}$$

where $\operatorname{ind}\langle\sigma\rangle$ *denotes the index of a representative of* $\langle\sigma\rangle$. *Then there exist*

$$\tau(i) \in \langle\sigma(i)\rangle, \quad i = 1, \ldots, r$$

such that $\{\tau(i)\}_{i=1}^{r}$ *generate a transitive subgroup of* S_n.

Proof. For applications we need only the special case of Lemma 4 where $r = 2$, $\sigma(2)$ is of order 2, and $\sigma(1)$ fixes no letters. In this case, if

$$\sigma(1) = (1, 2, \ldots, s(1,1))(\ldots, s(1,1) + s(1,2)) \cdots \left(\ldots, \sum_{j=1}^{k_1} s(1,j)\right) \tag{1.14}$$

then we can take

$$\sigma(2) = (s(1,1), s(1,1) + 1) \cdots \left(\sum_{j=1}^{k_1 - 1} s(1,j), \sum_{j=1}^{k_1 - 1} s(1,j) + 1\right). \tag{1.15}$$

Note the use of the integer i to replace x_i in the representations of $\sigma(1)$ and $\sigma(2)$ on $x_1, \ldots, x_n$.

The general argument is of a similar nature and will be left to the reader.

We remind the reader of the definition of

$$f(x) = x^n, \tag{1.16}$$

the *normalized cyclic polynomial* of degree n, and

$$T_n(x) = 2^{-n-1}\{(x + (x^2 + 4)^{\frac{1}{2}})^n + (x - (x^2 + 4)^{\frac{1}{2}})^n\}, \tag{1.17}$$

the normalized *Chebychev polynomial* of degree n. A linear change of the variable x gives us the general cyclic and Chebychev polynomials of degree n.

Lemma 5. *Let $f(x) \in k[x]$. Then $f(x)$ is a cyclic polynomial iff the field $k(f(x))$ has only one finite ramified place in $k(x)$. Suppose now that $f(x)$ is not a cyclic polynomial. Then $f(x)$ is a Chebychev polynomial iff $k(f(x))$ has exactly two finite ramified places in $k(x)$, and the branch cycles $\sigma(1)$ and $\sigma(2)$ are both of order 2. This latter condition is satisfied if either:*

$$\text{(1. 18)} \qquad \mathbf{tr}\,\sigma(1) = \mathbf{tr}\,\sigma(2) = 1 \ (\deg f \text{ is odd}),$$

or

$$\text{(1. 19)} \qquad \mathbf{tr}\,\sigma(1) = 0 \text{ and } \mathbf{tr}\,\sigma(2) = 2 \text{ or } \mathbf{tr}\,\sigma(1) = 2 \text{ and } \mathbf{tr}\,\sigma(2) = 0$$

$(\deg f$ *is even*$)$ (p. 49 of [4]).

Lemma 6. *Let $g_1(x) \in \hat{k}[x]$ and t a positive integer $(t > 1)$. Suppose that (in notation of* (1. 5)*):*

$$\text{(1. 20)} \qquad t \mid s(1, i) \quad \text{for } i = 2, \ldots, k_1.$$

By a linear change of variables (in z and x both) we may assume that $g_1(x) = x^{s(1,1)}h(x)$. Then:

$$\text{(1. 21)} \qquad h(x) = (r(x))^t,$$

for some polynomial $r(x)$.

Suppose $g_1, h_1 \in \hat{k}[x]$. Assume also that:

$$\text{(1. 22)} \qquad h_1(x) = x^t, \quad (\deg h_1, \deg g_1) = 1 \text{ or } 2, \quad \text{and (1. 3) holds.}$$

Then, either:

$$\text{(1. 23)} \qquad g_1(x) = x^{s(1,1)}\,(r(x))^t$$

for some integer $s(1, 1)$ and polynomials $r(x)$, or

$$\text{(1. 24)} \qquad g_1(x) = x^{s(1,1)}\,(x - \alpha)^{s(1,2)}\,(r(x))^t$$

where $(t, s(1, 1)) = \frac{t}{2}$ and $(t, s(1, 2)) = \frac{t}{2}$ for some integers $s(1, 1)$, $s(1, 2)$ and some constant α (so $2 \mid t$ in case (1. 24)*). In the case of* (1. 24), $(\deg g_1, \deg h_1) \geqq \frac{t}{2}$ *so $t = 2$ or 4.*

Suppose $g_1, h_1 \in k[x]$. Assume also that:

(1. 25) *$h_1(x)$ is a Chebychev polynomial,* $(\deg h_1, \deg g_1) = 1$ *or* 2, *and* (1. 3) *holds.*

Then, either:

$$\text{(1. 26)} \qquad \deg h_1 = 2$$

(and we have the above case), or

(1. 27) *g_1 is a Chebychev polynomial such that $g_1(x) - z$ has the same finite branch points as does $h_1(y) - z$, or*

(1. 28) $\deg h_1 = 4$, $\sigma(1, x) = (1)\,(1)\,(1)\,(3)\,(2)\,(2)\cdots(2)$, $\sigma(2, x) = (2)\,(2)\cdots(2)$

and $(\deg g_1, \deg h_1) = 2$ *and* $\mathbf{tr}\,\sigma(1, y) = 2$ *(in the notation of* 1. 5)).

Proof. By assumption, $z = 0$ corresponds to the branch cycle $\sigma(1, x)$. Thus (1. 20) implies that

$$g_1(x) = C \cdot x^{s(1,1)} \prod_{v=2}^{k_1} (x - \alpha_v)^{s(1,v)}$$

or,

$$g_1(x) = C \cdot x^{s(1,1)} \prod_{v=2}^{k_1} \left((x - \alpha_v)^{s(1,v)/t}\right)^t.$$

Expression (1. 21) follows easily from this.

Assume (1. 22) holds. We use Lemma 7 to check the irreducibility of $g_1(x) - y^t$ (see discussion below 1. 2). The reader can give an adhoc argument. We find: there exist polynomials $\bar{g}_1$, $\bar{g}_2$ such that $\bar{g}_1(\bar{g}_2(x)) = g_1(x)$ and $\Omega_{y^u - z} = \Omega_{g_1 - z}$ for some integer $u \mid t$. However, this implies that $\bar{g}_1 - z$ has exactly one finite branch point (or by a linear change of the variable x), $\bar{g}_1(x) = x^u$. The hypotheses of the lemma are satisfied with t replaced by $\frac{t}{u}$ and g_1 replaced by $\bar{g}_2(x)$. Therefore we may assume $g_1(x) - y^t$ is irreducible.

We use formula (1. 7) with the roles of g_1 and h_1 switched (and now we use $(\deg g_1, \deg h_1) = 1$ or 2) to obtain:

$$0 = \sum_{v=1}^{k_1} \left(t - (t, s(1, v))\right) - t - (l - 2) \quad \text{where} \quad l = 0 \quad \text{or} \quad 1. \tag{1.29}$$

Consider the expression

$$B(v) = \sum_{j=1}^{l_1} \left(s(1, v) - (t(1, j), s(1, v))\right) - s(1, v). \tag{1.30}$$

If $s(1, v) \mid t(1, j)$, then $s(1, v) - \left(t(1, j), s(1, v)\right) > \frac{s(1, v)}{2}$, with equality in the last expression iff $\frac{s(1, v)}{2}$ divides $t(1, j)$.

Let $I \overset{\text{def}}{=} \{1, \ldots, k_1\} = I_1 \cup I_2 \cup I_3 \cup I_4$ where

$$I_1 = \{j \in I \mid s(1, v) \text{ divides } t(1, j)\},$$

$$I_2 = \{j \in I - I_1 \mid s(1, v)/2 \text{ divides } t(1, j)\},$$

$$I_4 = \{j \in I - I_1 - I_2 \mid \left(s(1, v), t(1, j)\right) = 1\} \quad \text{and}$$

$$I_3 = I - I_1 - I_2 - I_4.$$

Then (1. 30) becomes:

$$B(v) = (|\, I_2 \,| - 2)\left(\frac{s(1, v)}{2}\right) + \sum_{j \in I_3 \cup I_4} \left(s(1, v) - (t(1, j), s(1, v))\right) \tag{1.31}$$

and

$$B(v) \geqq (|\, I_2 \,| - 2)\left(\frac{s(1, v)}{2}\right) + |\, I_3 \,|\left(\frac{2s(1, v)}{3}\right) + |\, I_4 \,|\, (s(1, v) - 1).$$

If we substitute $s(1, v)$ for t and $t(1, j)$ for $s(1, j)$ in (1. 29) we obtain

$$0 = B(v) - (l - 2) \quad \text{where} \quad l = 1 \quad \text{or} \quad 2, \tag{1.32}$$

or

$$(|\, I_2 \,| - 2)\left(\frac{t}{2}\right) + |\, I_3 \,|\left(\frac{2t}{3}\right) + |\, I_4 \,|\, (t - 1) \leqq l - 2.$$

Thus, either $|\, I_2 \,| = 0$ and $|\, I_3 \,| + |\, I_4 \,| \leqq 1$ (which implies that (1. 20) holds, and therefore (1. 23) holds), or $|\, I_2 \,| = 1$ and $|\, I_3 \,| = |\, I_4 \,| = 0$ (again (1. 23) results), or $|\, I_2 \,| = 2$ and $|\, I_3 \,| = |\, I_4 \,| = 0$ (and (1. 24) results).

Now assume that (1. 25) holds. From Lemma 5 we have two cases for $h_1(y)$ to consider. They are handled similarly. So we assume $\operatorname{tr} \sigma(1, y) = 2$, $\operatorname{tr} \sigma(2, y) = 0$, and leave to the reader the remaining cases. In switching the roles of h_1 and g_1 in formula (1. 7) we obtain:

$$(1.33) \qquad 2(\deg h_1 - 1) \geqq \operatorname{tr} \sigma(1, x)\frac{m-2}{2} + \operatorname{tr} \sigma(2, x)\frac{m}{2} + m - (n, m)$$

where $n = \deg g_1$, $m = \deg h_1$, and (by assumption) $(n, m) = 1$ or 2. In this case we also have m even and $\geqq 3$ (by assumption). In terms of the characterization of Chebychev polynomials at the end of the statement of Lemma 5, if g_1 is not a Chebychev polynomial, then, in order for (1. 32) to hold we must have n even, and $m = 6$ or $m = 4$, $\operatorname{tr} \sigma(2, x) = 0$ and $\operatorname{tr} \sigma(1, x) = 3$. Now, since n is even and $\sum_{i=1}^{r} \operatorname{ind} \sigma(i, x) = n - 1$, we must have (after suitable ordering of $s(1, v)$ for $v = 1, \ldots, k_1$) that:

(1. 34) $s(1, 1) = s(1, 2) = s(1, 3) = 1$, $s(1, 4) = 3$, $s(1, v) = 2$ for $v = 5, \ldots, k_1$, and $s(2, v) = 2$ for $v = 1, \ldots, k_2$. Returning now to formula (1. 7) we find that with $p = 0$, $m = 6$ is not possible, but $m = 4$ is possible and (1. 28) results.

Let $f(x) \in \hat{k}[x]$, and suppose that $f(x)$ has two distinct decompositions

$$(1.35) \qquad f(x) = g_1(g_2),\ f(x) = h_1(h_2).$$

From Theorem 1 there exist polynomials $\bar{g}$, $\bar{g}_1$, $\bar{h}_1$, $\bar{\bar{g}}$, $\bar{\bar{g}}_2$, $\bar{\bar{h}}_2$ such that

$$(1.36) \quad g_1 = \bar{g}(\bar{g}_1),\ h_1 = \bar{g}(h_1),\ g_2 = \bar{g}_2(\bar{\bar{g}}), \quad \text{and} \quad \bar{h}_2 = \bar{\bar{h}}_2(\bar{\bar{g}})$$

where $(\deg \bar{g}_1, \deg \bar{h}_1) = 1$ and $(\deg \bar{\bar{g}}_2, \deg \bar{\bar{h}}_2) = 1$. Thus, in order to investigate the decompositions of the polynomial $f(x)$ we are reduced to the case

(1. 37) $(\deg g_1, \deg h_1) = 1$ in expression (1. 18), and (1. 1) holds

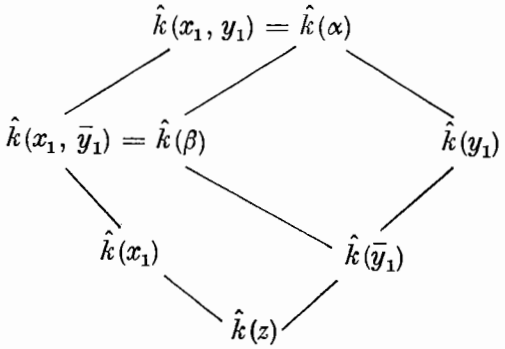
(see discussion following (1. 2)).

Cyclic Factor Reduction Diagram

Suppose $h_1 = (h_2)^t$ for some integer $t > 1$ and polynomial h_2. Let $\bar{y}_1$ be a variable such that $(\bar{y}_1)^t = z$. Assume $g_1, h_1 \in \hat{k}[x]$ satisfy:

(1. 38) $(t, \deg g_1) = 1$, and $\hat{k}(x_1, y_1)$ is of genus 0.

Then we obtain the following diagram of fields after applying expression (1. 23):



where (in the notation of Lemma 6) $h_2(y_1) = \bar{y}_1 = \beta^{s(1,1)}\, r(\beta^t)$, $\beta^t = x_1$ and $x_1^{s(1,1)}\, r(x_1)^t = z$. We call the polynomial pair $x^{s(1,1)}\, r(x^t)$, $h_2(x)$ *the cyclic reduced pair* (obtained from g_1, h_1).

Ritt (p. 61, [8]) proved the next theorem in the case where g_1 and h_1 have no non-trivial decomposition (are indecomposable).

Theorem 2. *Let* $f(x) \in \hat{k}[x]$ *have decompositions* (*we assume* $\deg g_1$ *and* $\deg h_1 > 1$)

(1. 39) $\qquad f(x) = g_1(g_2(x)) = h_1(h_2(x))$ *where* $(\deg g_1, \deg h_1) = 1$

(*see* (1. 35)). *Then there exists a chain of polynomial pairs*

$$\{g_1, h_1\} = \{g_1^{(1)}, h_1^{(1)}\}, \ldots, \{g_1^{(w)}, h_1^{(w)}\}$$

such that:

(1. 40) $\{g_1^{(i)}, h_1^{(i)}\}$ *is a cyclic reduced pair obtained from* $\{g_1^{(i-1)}, h_1^{(i-1)}\}$, $i = 2, \ldots, w$;

(1. 41) *for each* $i = 1, \ldots, w-1$, *there exists a constant* $\alpha(i)$ *and integers* $s(i) > 1$, $t(i) > 1$ *such that* $g_1^{(i)} - \alpha(i) = (\bar{g}^{(i)})^{s(i)}$, $h_1^{(i)} - \alpha(i) = (\bar{h}_1^{(i)})^{t(i)}$ *for some polynomials* $\bar{g}^{(i)}$ *and* $\bar{h}^{(i)}$;

and

(1. 42) *either* $h_1^{(w)}$ *is cyclic* (*or* $g_1^{(w)}$ *is cyclic*) *and* (1. 23) *holds, or* $\{g_1^{(w)}, h_1^{(w)}\}$ *is a pair of Chebychev polynomials having the same finite branch points.*

Theorem 2 is a special case of Theorem 3, and Theorem 4 is still a further generalization. The reader can see for himself that the assumption $(\deg g_1, \deg h_1) = 1$ greatly reduces the work of both Lemma 6 and Theorem 3.

Theorem 3. *Let* $g_1, h_1 \in \hat{k}[x]$. *Suppose that* $g_1(x) - h_1(y)$ *is irreducible, and defines a curve of genus zero over* $\hat{k}$. *Assume also that*

(1. 43) $\qquad (\deg g_1, \deg h_1) = 1$ *or* 2.

Then, either:

(1. 44) *the conclusion of Theorem* 2 *holds for* $\{g_1, h_1\}$ (*expressions* (1. 41), (1. 42));

or (*with* g_1 *and* h_1 *possibly switched*)

(1. 45) $(\deg g_1, \deg h_1) = 2$ *and* $\deg h_1 = 2$, $g_1 = (x-\alpha)(x-\beta)(r(x))^2$ *for some constants* α *and* β, *and some polynomial* $r(x)$ (*expression* (1. 24)); *or* (1. 28) *holds*;

or

(1. 46) $\deg h_1 = 4$, $\deg g_1 = 6$ *and* $t(1, 1) = 1$, $t(1, 2) = 3$, $s(1, 1) = s(1, 2) = 3$

(*in the notation of* (1. 5)).

Corollary. *Let* $g_1, h_1 \in K[x]$ *where* K *is a number field. Suppose that* $g_1(x) - h_1(y)$ *has an irreducible factor which defines a curve having infinitely many* K*-integrals points* (x_0, y_0) *on the curve with* x_0 *and* y_0 *in the ring of integers of* K). *Then, either*;

(1. 47) $g_1(x) - h_1(y)$ *is irreducible and the conclusion of Theorem* 3 *holds for* $\{g_1, h_1\}$;

or

(1. 48) *there exist polynomials* $\bar{g}_1, \bar{g}_2, \bar{h}_1, \bar{h}_2$ *such that* $\deg \bar{g}_1 > 1$;

$$\bar{g}_1(\bar{g}_2) = g_1, \bar{h}_1(\bar{h}_2) = h_1; \deg \bar{g}_1 = \deg \bar{h}_1,$$

and

(1. 49) $\bar{g}_1(x) - \bar{h}_1(y)$ *has an irreducible factor of degree* 2 *or* 1.

Proof. By Siegel's Theorem (p. 244, [10]) if $\varphi(x, y)$ (an irreducible factor of $g_1(x) - h_1(y)$) defines a curve with infinitely many K-integral points, then $K(x_1, y_1)$

defines a curve of genus zero (where (x_1, y_1) is a generic point for $\varphi(x, y) = 0$). Also, for some quadratic extension K' of K, there exists $\alpha \in K'(x_1, y_1)$ such that

$$K'(\alpha) = K'(x_1, y_1) \text{ and } z = \frac{f(\alpha)}{\alpha^r}$$

where

$$z = g_1(x_1) = h_1(y_1)$$

for some polynomial f, and some integer $r \geqq 0$. If the ring of integers of K' contains only finitely many units (so that $K' = \mathbb{Q}$, or some complex quadratic extension of $\mathbb{Q}$), then we can take $r = 0$. In this latter case $K'(x_1, y_1)$ has one place over $z = \infty$; while if $t > 0$, then $K'(x_1, y_1)$ has at most two places over $z = \infty$. On the other hand, if $g_1(x) - h_1(y)$ is irreducible, then (deg g_1, deg h_1) is the number of places of $K'(x_1, y_1)$ over $z = \infty$. Thus we obtain (1. 47), since the hypotheses of Theorem 3 hold. If $g_1(x) - h_1(y)$ is reducible, then Lemma 7 implies the existance of polynomials satisfying (1. 48), and such that $\bar{g}_1(x) - \bar{h}_1(y)$ is reducible and has a factor $\bar{\varphi}(x, y)$ with infinitely many K-integral points. Letting $(\bar{x}_1, \bar{y}_1)$ be a generic point for $\bar{\varphi}(x, y) = 0$, since

$$\deg \bar{h}_1 = \deg \bar{g}_1, \deg {}_x\bar{\varphi}(x, y) = \deg {}_y\bar{\varphi}(x, y) = \text{number of places of } K(\bar{x}_1, \bar{y}_1) \text{ over } z = \infty.$$

From $K(z) \subset K(\bar{x}_1, \bar{y}_1) \subset K(x_1, y_1)$ we must have 1 or 2 places of $K(\bar{x}_1, \bar{y}_1)$ over $z = \infty$. Thus, deg ${}_x\bar{\varphi}(x, y) = 1$ or 2. If the former, then (by a linear change of the polynomials $\bar{g}_2(x)$) we may assume that $\bar{g}_1(x) = \bar{h}_1(x)$. Thus (1. 48) and the concluding statement of the corollary holds.

Remark 1. It is not difficult to classify the polynomial pairs $\bar{g}_1, \bar{h}_1$ such that $\bar{g}_1(x) - \bar{h}_1(y)$ has a factor of degree 2. The techniques for doing this are contained in [6]. Essentially the only such pair is given by:

(1. 50) deg $\bar{g}_1 = \deg \bar{h}_1 = 4$, and $\bar{g}_1$ and $\bar{h}_1$ are both Chebychev polynomials (with the same finite branch points) where (in the notation of (1. 5)) with g_1 replaced by $\bar{g}_1$, h_1 replaced by $\bar{h}_1$; $\sigma(1, x) = (1)\,(1)\,(2)$, $\sigma(1, y) = (2)\,(2)$, $\sigma(2, x) = (2)\,(2)$, $\sigma(2, y) = (1)\,(1)\,(2)$.

With this type branching $\bar{g}_1(x) - \bar{h}_1(y)$ must be reducible: for if irreducible we could apply formula (1. 7). However, an application of that formula, in this case, results in a negative genus for $K(\bar{x}_1, \bar{y}_1)$.

Proof of *Theorem* 3. Let $l = (\deg g_1, \deg h_1)$ ($l = 1$ or 2). Suppose first that (in the notation of (1. 5));

$$\text{tr } \sigma(1, x) = 0 = \text{tr } \sigma(1, y), \tag{1. 51}$$

and

$$\underset{1 \leqq j \leqq l_1}{\text{g.c.d.}} \, (t(1, j)) = 1. \tag{1. 52}$$

Since $g_1(x) - h_1(y)$ is irreducible we may apply formula (1. 7). If, in formula (1. 7), we replace $\sigma(2, x)$ (resp. $\sigma(2, y)$) by an element of form $\tau(2, x) = \underbrace{(2)\,(2)\cdots(2)}_{k_1 - 1}\,(1)\cdots(1)$ (resp. $\gamma(2, y) = \underbrace{(2)\,(2)\cdots(2)}_{k_1 - 1}\,(1)\cdots(1)$) we obtain

$$2(\deg g_1 - 1) \geqq \sum_{j=1}^{l_1} \sum_{v=1}^{k_1} (s(1, v) - (s(1, v), t(1, j))) + \deg g_1 - l + (k_1 - 1)(m - 2(l_1 - 1)) \tag{1. 53}$$

with equality iff $\sigma(2, x)$ (resp. $\sigma(1, y)$) is similar to $\tau(2, x)$ (resp. $\gamma(2, y)$).

Simplifying (and using (1. 30)) we obtain

$$(1.54) \qquad 0 \geqq \sum_{v=1}^{k_1} B(v) + (k_1 - 1)\,(m - 2(l_1 - 1)) + 2 - l.$$

In order for the right side to be $\leqq 0$, we must have either

$$(1.55) \qquad B(v) < 0 \quad \text{for same } v,$$

or

(1. 56) $k_1 = 1$ (so g_1 is cyclic), or $m = 2(l_1 - 1)$ (so h_1 is Chebychev).

From Lemma 6, (1. 56) leads to cases included in the conclusion of Theorem 3. Thus we assume (1. 55) holds.

From (1. 51), $s(1, v) > 0$. From the argument following expression (1. 32) we conclude there exists an integer $c > 1$ such that $c \mid t(1, j)$ for $j = 1, \ldots, l_1$. This contradicts (1. 52).

Now we must show that with no loss of generality both (1. 51) and (1. 52) hold. Suppose $\operatorname{tr} \sigma(1, y) \geqq 1$ and $\operatorname{tr} \sigma(i, y) \geqq 2$ for $i = 2, \ldots, r$. In applying formula (1. 7) we obtain

$$(1.57) \qquad 2(\deg g_1 - 1) \geqq g_1 - k_1 + 2(k_1 - 1) + g_1 - l$$

with equality iff $\operatorname{tr} \sigma(1, y) = 1$, $\operatorname{tr} \sigma(2, y) = 2$, $l = 2$, $k_1 = 2$ (since we are assuming $k_1 > 1$) and

$$s(1, 1) \mid t(1, j),\ s(1, 2) \mid t(1, j), \quad \text{for } j = 1, \ldots, l_1.$$

If $s(1, 1) = s(1, 2) = 2$, then g_1 is Chebychev of degree 4 (thus by Lemma 6, (1. 44) holds). If $s(1, 1) > 2$, then in order for $\operatorname{tr} \sigma(1, y) = 1$, $\operatorname{tr} \sigma(2, y) = 2$ we must have

$$(1.58) \qquad l_1 = 2,\ t(1, 1) = 1,\ t(1, 2) = 3,\ 3 = s(1, 1) = s(1, 2),$$

so expression (1. 46) holds. Thus, with no loss we may assume

$$(1.59) \qquad \operatorname{tr} \sigma(1, y) = 0 \quad \text{and} \quad \operatorname{tr} \sigma(i, x) = 0 \quad \text{for some } i = 1, \ldots, r.$$

Suppose the index i in (1. 59) is different from 1. Since we are assuming that h_1 is not a Chebychev polynomial, by Lemma 6 (last line) $\operatorname{tr} \sigma(i, y) > 3$. Therefore the right hand side of (1. 7) is at least $3(n - k_i) + n - l$ (since $\operatorname{tr} \sigma(i, x) = 0$). This is greater than $5/2\, n - l$. This contradicts (1. 7).

Therefore we may assume (1. 51) holds. Let

$$s = \underset{1 \leq v \leq k_1}{\text{g.c.d.}}\,(s(1, v)), \quad t = \underset{1 \leq j \leq l_1}{\text{g.c.d.}}\,(t(1, j)).$$

If $t = 1$, or $s = 1$ (by switching the roles of g_1 and h_1 if necessary) we may assume (1. 52) holds. If $(t, s) > 1$, then Lemma 6 shows that there exists polynomials $\bar{g}_1$, $\bar{g}_2$, $\bar{h}_2$ such that $\bar{g}_1$ is cyclic of degree (t, s) and $\bar{g}_1(\bar{g}_2) = g_1$, $\bar{g}_1(\bar{h}_2) = h_1$, so that $g_1(x) - h_1(y)$ is reducible (contrary to assumption of Theorem 3). Thus $(t, s) = 1$, and we assume $2 \nmid t$. We are now in position to apply the cyclic factor reduction diagram to $\{g_1, h_1\}$ to get $\{g_1, {}^{(2)}\, h_1^{(2)}\}$ where $\deg h_1^{(2)} < \deg h_1$. Continue until (1. 52) is satisfied as described above.

Example 1. Consider (as in [7] where $g(x)$ was assumed a polynomial) the question: when does $y^n = g(x)$ have infinitely many integral solutions over a number field K. When $g(x)$ is a polynomial Lemma 6 suffices to give the complete answer, since the proof of the Lemma shows that we are reduced to the case

$$h_1(y) = y^n,\ g(x) = g_1(x) \quad \text{and} \quad h_1(y) - g_1(x)$$

is irreducible. The case where $g(x)$ is a rational function is no more difficult to handle (using the proof of the Corollary to Theorem 3).

Example 2. Consider (as in [1]) the question: when does

$$f_n(x) \stackrel{\text{def}}{=} x^n + x^{n-1} + \cdots + x = y^m + y^m + \cdots + y$$

have infinitely many K-integral solutions. We exclude the trivial case $n = m$. If $n > m$, then the Corollary to Theorem 3 shows that $f_n(x) - f_m(y)$ must be reducible. From Lemma 7 this implies that $f_n(x)$ is decomposable. However, a simple computation shows that $f_n(x) - z$ has $n - 1$ distinct finite branch cycles (of type $(2)(1)\cdots(1)$). If $f_n(x) = g_1(g_2(x))$ where $\deg g_i > 1$, $i = 1, 2$, then none of the branch cycles corresponding to branch points of $g_1(x) - z$ could be of this type.

Section 2. Polynomials of almost relatively prime degree

In this section we concern ourselves with $g_1, h_1 \in \hat{k}[x]$ (retain the notation of (1. 1) through (1. 5)) where:

(2. 1) $$\deg g_1 = n, \ \deg h_1 = m, \quad \text{and } (n, m) = 1.$$

Lemma 7. *Let $g_1, h_1 \in \hat{k}(x)$ (not necessarily in $\hat{k}[x]$) and assume that*

(2. 2) *$g_1(x) - h_1(y)$ is reducible as a rational function in two variables.*

Then, there exist $\bar{g}_1, \bar{g}_2, \bar{h}_1, \bar{h}_2, \in \hat{k}(x)$ such that

(2. 3) $$\bar{g}_1(\bar{g}_2(x)) = g_1(x), \ \bar{h}_1(\bar{h}_2(x)) = h_1(x),$$

(2. 4) *$\bar{g}_1(x) - \bar{h}_1(y)$ is reducible,*

and

(2. 5) $$\Omega_{\bar{g}_1 - z} = \Omega_{\bar{h}_1 - z}.$$

Suppose g_1, h_1 are polynomials and $\bar{g}_1$, $\bar{h}_1$ are not linearly equivalent (see Definition 1). Then,

(2. 6) $\deg \bar{g}_1 = \deg \bar{h}_1$ *(equality of the order of inertial groups over $z = \infty$ in $\Omega_{\bar{g}_1 - z} = \Omega_{\bar{h}_1 - z}$).*

If, in addition, $\bar{g}_1(x)$ is indecomposable, then so is $\bar{h}_1(x)$, and

(2. 7) $$\bar{g}_1(x) - \bar{h}_1(y) = \prod_{i=1}^{2} \varphi_i(x, y) \text{ where } \varphi_1, \varphi_2 \text{ are irreducible,}$$

and $n - 1 \mid (\deg_x(\varphi_1))(\deg_x(\varphi_1) - 1)$ (see Theorem 1 of [6]).

Lemma 8. *Let $g_1, h_1 \in \hat{k}(x)$ and assume that condition (1. 1) holds ($g_1(x) - h_1(y)$ is irreducible). If*

(2. 8) *$\hat{k}(x_1, y_1)$ is of genus zero,*

then there exists finite indices i and j such that

(2. 9) $\operatorname{tr}(\sigma(i, x)) = 0$ *or* 1 *and* $\operatorname{tr}(\sigma(j, y)) = 0$ *or* 1

(excluding the cases where $\deg g_1$ and $\deg h_1$ are 4, 6, or 8).

Now assume that g_1 and h_1 are polynomials. Then, we may assume

(2. 10) *$i = j$ where i, j satisfy (2. 9) (with no exceptions).*

Proof. The computation showing (2. 9) is worked out in [5], Section 2, but the technique is included in the proof of the remainder of the Lemma. In order to prove (2. 10),

assume that $i = 1$, $j = 2$ (that is, $i \neq j$). By renaming g_1 and h_1 (if necessary) we may assume that

$$m - 2(l_2 - 1) \geqq n - 2(k_1 - 1). \tag{2.11}$$

From (1.7)

$$2(n-1) \geqq \operatorname{tr}(\sigma(1, y))(n - k_1) + n - (n, m). \tag{2.12}$$

However, since h_1 is a polynomial

$$\operatorname{tr}(\sigma(1, y)) \geqq m - 2(l_2 - 1) \tag{2.13}$$

with equality iff $\sigma(2, y)$ is of order 2, $\sigma(j, y)$ is of order 1 for $j = 3, \ldots, r$.

Thus,

$$2(n-1) \geqq (n - 2(k_1 - 1))(n - k_1) + n - (n, m) \text{ (using expression (2.11))}. \tag{2.14}$$

For fixed n the right side of this expression is decreasing as a function of k_1, and therefore we must have $k_1 \geqq \frac{n-1}{2}$. Since $\operatorname{tr}\sigma(1, x) = 0$ or 1, we also note that $n \geqq 1 + 2(k_1 - 1)$. Therefore;

$$k_1 = \frac{n}{2} \text{ or } \frac{n-1}{2} \text{ (depending on } n \text{ even or odd)}. \tag{2.15}$$

Returning to (2.12) we obtain either

$$2(n-1) \geqq \operatorname{tr}(\sigma(1, y))\frac{n}{2} + n - (n, m) \text{ (for } n \text{ even)}, \tag{2.16}$$

or

$$2(n-1) \geqq \operatorname{tr}(\sigma(1, y))\frac{n+1}{2} + n - (n, m) \text{ (for } n \text{ odd)}. \tag{2.17}$$

Thus, if $(n, m) = n$, $\operatorname{tr}(\sigma(1, y)) \leqq 3$ and if $(n, m) < n$, then $\operatorname{tr}(\sigma(1, y)) \leqq 2$. From (2.13):

$$l_2 \geqq \frac{m-1}{2} \text{ and } (\text{since } \operatorname{tr}\sigma(2, y) = 0 \text{ or } 1) \tag{2.18}$$

we have $l_2 = \frac{m}{2}$ or $\frac{m-1}{2}$. If we show that $\sigma(1)$ and $\sigma(2)$ are of order 2, then the characterization of Lemma 5 shows that g_1 and h_1 are both Chebychev polynomials. If $k_1 = \frac{n}{2}$, since $\operatorname{tr}(\sigma(1, x)) = 0$ or 1, we must have $\sigma(1, x)$ of order 2. However, suppose $k_1 = \frac{n-1}{2}$. Since $\operatorname{tr}\sigma(2, y) \leqq 1$, $\operatorname{ind}\sigma(2, y) \geqq \frac{m-1}{2}$. Thus, from $\operatorname{ind}\sigma(1, y) + \operatorname{ind}\sigma(2, y) \leqq m - 1$, we conclude that $\operatorname{ind}\sigma(1, y) \leqq \frac{m-1}{2}$, $\operatorname{tr}\sigma(1, y) \leqq 3$, and we find that either:

$$t(1, v) = 1 \text{ for } v = 1, 2, 3;\ t(1, 4) = 3;\ t(1, v) = 2 \text{ for } v = 5, \ldots, l_1; \tag{2.20}$$

or

$$t(1, v) = 1 \text{ for } v = 1, 2;\ t(1, 3) = 3;\ t(1, v) = 2 \text{ for } v = 4, \ldots, l_1; \tag{2.21}$$

or

$$t(1, v) = 1 \text{ for } v = 1, 2, 3;\ t(1, v) = 3 \text{ for } 4, 5;\ t(1, v) = 2 \text{ for } v = 6, \ldots, l_1; \tag{2.22}$$

or

$$t(1, 1) = 1;\ t(1, 2) = 3;\ t(1, v) = 2 \text{ for } v = 3, \ldots, l_1. \tag{2.23}$$

Consider the contribution to the right side of (1.7) obtained from just the term corresponding to $\sigma(1)$ in the above cases. Computation shows that this contribution

exceeds $2(n-1)$ (left side of (1. 7)) unless (2. 21) or (2. 23) holds. In the case of (2. 21) we explicitly compute the right side of (1. 7) to be no smaller than

$$2\left(\frac{n+1}{2}\right)+\left(\frac{n-3}{2}\right)+2(l_1-3)+n-(n,m). \tag{2. 24}$$

In order for (2. 24) to be $\leqq 2(n-1)$ we must have $l_1=3$ (or $m=6$) and $n \mid m$. But n is odd in this case, so we have disposed of case (2. 21). In the case of (2. 23), $\mathrm{tr}(\sigma(1,y))=1$, and (2. 9) already holds.

Definition 2. Let H be a subgroup of the symmetric group on n letters (denoted S_n). Let d_1 be an integer, such that $\{1,2,\ldots,n\}=\bigcup_{i=1}^{d_1} X_i$ where the X_i's are disjoint sets (of the same order) that are permuted among each other by the elements of H. Then we say, we have *decomposed* $\{1,2,\ldots,n\}$ *into* d_1 sets of *imprimitivity* for H.

Lemma 9. *Assume that* g_1 *and* h_1 *are polynomials, and* (1. 1) *and* (2. 8) *hold as in Lemma* 8. *From Lemma* 8 *we may assume that* $\mathrm{tr}(\sigma(1,x))$ *and* $\mathrm{tr}(\sigma(1,y))$ *are* $\leqq 1$. *Both* $\sigma(1,x)$ *and* $\sigma(1,y)$ *may be regarded as (distinct) elements of* S_n. *Suppose there exist* $\tau(2)$ *and* $\gamma(2)\in S_n$, $\bar{\sigma}(1,x)\in\langle\sigma(1,x)\rangle$ *and* $\bar{\sigma}(1,y)\in\langle\sigma(1,y)\rangle$ *(see Lemma* 4), *such that*

$$\bar{\sigma}(1,x)\cdot\tau(2)=(1,2,\ldots,n) \quad \textit{and} \quad \bar{\sigma}(1,y)\cdot\gamma(2)=(1,2,\ldots,m), \tag{2. 25}$$

and

(2. 26) *if* $d_1(x)$ *(respectively* $d_1(y)$*) is the number of sets of imprimitivity of* H_x, *the group generated by* $\bar{\sigma}(1,x)$ *and* $\tau(2)$ *(respectively* H_y*) on* $\{1,2,\ldots,n\}$ *(respectively* $\{1,2,\ldots,m\}$*), then* $d_1(x)\neq d_1(y)$.

Then we conclude that

$$\sigma(2,x) \quad \textit{and} \quad \sigma(2,y) \quad \textit{are of order } 2, \tag{2. 27}$$

and

(2. 28) $\sigma(j,x)$ *and* $\sigma(j,y)$ *are of order* 1 *for* $j>2$ *(that is,* $r=2$).

In particular, (2. 27) *and* (2. 28) *hold if either*

$$\deg g_1>(\deg g_1,\deg h_1)=d \textit{ and } \mathrm{tr}(\sigma(1,x))=1, \tag{2. 29}$$

or

(2. 30) $\deg g_1$ *and* $\deg h_1>d$, *and there exist* i *and* j *such that* g.c.d. $(d, s(1,i), t(1,j))=1$ *and* $u\neq i$, $v\neq j$ *such that* $s(1,u)>2$, $t(1,v)>2$.

Proof. The argument between expressions (1. 52) and (1. 55) suffices to prove that (2. 25) implies (2. 27) and (2. 28), once we have shown that $\bar{g}_1(x)-\bar{h}_1(y)$ is irreducible, where $\bar{g}_1$ and $\bar{h}_1$ are polynomials with a description of their branch cycles over the z-sphere given respectively by $\sigma(1,x)$, $\tau(2)$ and $\sigma(1,y)$, $\gamma(2)$. However, from Lemma 7 this implies that $\bar{g}_1$ and $\bar{h}_1$ have decomposition factors of the same degree. By Lemma 2 decomposition factors of $\bar{g}_1(x)$ are (up to linear relatedness; definition 1) in one-one correspondence with subfields of $\hat{k}(\bar{x}_1)$ containing $\hat{k}(z)$ (where $\bar{g}_1(\bar{x}_1)=z$). In turn, by the fundamental theorem of Galois theory such subfields are in one-one correspondence with subgroups of $G(\Omega_{\bar{g}_1-z}/\hat{k}(z))$ containing $G(\Omega_{\bar{g}_1-z}/\hat{k}(\bar{x}_1))$. Such subgroups are in one-one correspondence with systems of imprimitivity of $G(\Omega_{\bar{g}_1-z}/\hat{k}(z))$ on $\{x_i\}_{i=1}^{\deg\bar{g}_1}$. Thus condition (2. 26) is violated if $\bar{g}_1$ and $\bar{h}_1$ have decomposition factors of the same degree.

Now we show that (2. 29) and (2. 30) imply the existence of $\tau(2)$ and $\gamma(2)$ satisfying (2. 25) and (2. 26). For this argument alone, let $s(1, i) \overset{\text{def}}{=} s(i)$. If $\operatorname{tr}(\bar{\sigma}(1, x)) = 1$, let

$$(2.31)\quad \tau(2) = (1, 2)\,(a(1) + 1, n - b(1))\,(a(1) + a(2) + 1, n - b(1) - b(2)) \cdots$$

and $\bar{\sigma}(1, x) = (1, 2, \ldots, n) \cdot (\tau(2))^{-1}$ where $a(i) + b(i) = s(i)$ for $i = 1, \ldots, k_1 - 1$. Otherwise, let (similarly)

$$(2.32)\quad \tau(2) = (a(1), n - b(1))\,(a(1) + a(2), n - b(1) - b(2)) \cdots.$$

Since $\bar{\sigma}(1, x) \cdot \tau(2) = (1, 2, \ldots, n)$ each system of imprimitivity consists of a decomposition of $\{1, 2, \ldots, n\}$ into sets $\left\{1, 1 + d_1, \ldots, 1 + \left(\frac{n}{d_1} - 1\right) d_1\right\}$, $\{2, 2 + d_1, \ldots\}$, ... where d_1 is a divisor of n. Such a collection is a system of imprimitivity iff $\tau(2)$ maps the sets of the collection among themselves. For example, suppose

$$(2.33)\qquad \tau(2)(i) = j \quad \text{where } j - i \not\equiv 0 \bmod d_1,$$

and $\tau(2)(i + cd_1) = i + cd_1$ for some integer c. Then there is no decomposition of $\{1, 2, \ldots, n\}$ into d_1 sets of imprimitivity with respect to H_x.

First we consider the situation of (2. 31). Suppose $\bar{\sigma}(1, x)$ is not of order 2. Then we order $s(1), \ldots, s(k_1)$ so that $1 + d \to 2 + d$ in the cycle corresponding to $s(u)$ where $s(u) > 2$. Then $1 + d$ is not moved by $\tau(2)$ and (2. 33) is satisfied. On the other hand, if $\sigma(1, x)$ is of order 2 then we compute the genus of $\hat{k}(x_1, y_1)$ using formula (1. 7). Let $A = \{\#$ of j such that $2 \nmid t(1, j)\}$. Then

$$(2.34)\qquad 2(n-1) \geqq A \cdot \left(\frac{n-1}{2}\right) + (m - 2(l_1 - 1))\left(\frac{n-1}{2}\right) + n - (n, m)$$

where the second last term is a lower bound on the contributions from $\sigma(2), \ldots, \sigma(r)$ (with equality of this estimate to the actual contributions iff $r = 2$ and $\sigma(2, x)$ and $\sigma(2, y)$ are of order 2). Since $(n, m) \leqq \frac{n}{2}$ (from (2. 29)) we obtain

$$(2.35)\qquad A + (m - 2(l_1 - 1)) \leqq 2.$$

However, since $m \leqq 2 \cdot l_1$, we obtain $\sigma(1, y)$ is of order 2. If we switch the roles of g_1 and h_1 in formula (1. 7), then

$$(2.36)\quad 2(m-1) \geqq \frac{m-1}{2} + w\left(\frac{m}{2} - 1\right) \text{ where } w = \min_{i \neq 1} \operatorname{tr}(\sigma(i, x)).$$

Thus, $1 \leqq w \leqq 3$. If $w = 1$, then g_1 is (by Lemma 5) a Chebychev polynomial, and an explicit calculation of the genus $\hat{k}(x_1, y_1)$ now shows that (under assumption (2. 8)) h_1 is also a Chebychev polynomial. If $w = 2$ or 3, then we must check out cases similar to (2. 20) through (2. 23). This we leave to the reader. This shows that (2. 29) implies (2. 27) and (2. 28).

Now we assume that (2. 30) holds. By an argument similar to that above (upon returning to (2. 32)) we have only to show that if:

$$(2.37)\qquad (s(1, 1), t(1, 1), d) = 1,$$

then we can choose $\tau(2)$ such that

(2. 38) $\qquad a(1) + cd$ is left fixed by $\tau(2)$ for some integer c.

Suppose that $d_1(x) = d_1(y) = e$ where $d_1(x)$ and $d_1(y)$ are the orders of systems of imprimitivity for $G(\Omega_{\bar{g}_1-z}/\hat{k}(z))$ and $G(\Omega_{\bar{h}_1-z}/\hat{k}(z))$. By a previous argument $e \mid d$. Then (2. 38) implies that the set $\{a(1), a(1) + e, a(1) + 2e, \ldots\}$ is mapped into itself by $\tau(2)$. However, since $\tau(2)$ maps $a(1)$ into $n - s(1, 1) + a(1)$, we must have $e \mid s(1, 1)$. Similarly, if we establish (2. 38) then by analogy we obtain a similar expression with $\tau(2)$ replaced by $\gamma(2)$ and we must have $e \mid t(1, 1)$. Since $e \mid d$, (2. 37) implies $e = 1$; contrary to the assumption $d_1(x) > 1$. If there exists $u \neq 1$ such that $s(1, u) > 2$ (as our hypothesis (2. 30) grants) then we may order $s(1, 2), \ldots, s(1, k_1)$ so that

$$a_1 + d \to a_1 + d + 1 \quad \text{by} \quad \bar{\sigma}(1, x).$$

Thus $\tau(2)$ leaves $a_1 + d$ fixed. This shows (2. 38) and finishes the lemma.

A proof of the next theorem is similar to the proof of Theorem 3 (which it generalizes). The main combinatorial tools are the proof of Theorem 3 and the analysis of Lemma 8 (in particular assumption (2. 11) and its consequence, expression (2. 14)). The proliferation of special cases, however, makes it untenable to include the proof in this paper.

Theorem 4. *Let $d > 0$ be fixed. Then there exist an integer $N(d)$ such that if $g_1, h_1 \in \hat{k}[x]$ satisfy*:

(2. 39) $\qquad (\deg g_1, \deg h_1) = d, \quad \deg g_1$ *and* $\deg h_1 > N(d)$

and

(2. 40) $\quad g_1(x) - h_1(y)$ *is irreducible, and defines a curve of genus zero*;

then

(2. 41) *the conclusion of Theorem* 2 *holds.*

For our last result we investigate a situation that arises for instance when g_1 and h_1 are polynomials that are conjugate by the action of $G(\mathbb{C}/\mathbb{Q})$ on their coefficients (see [5]).

Theorem 5. *Let $g_1, h_1 \in \hat{k}[x]$ satisfy* (2. 40). *By Lemma* 8 *we may assume* (*as in the notation of* (1. 5)) *that* $\operatorname{tr} \sigma(1, x) = 0$ *or* 1 *and* $\operatorname{tr} \sigma(1, y) = 0$ *or* 1. *Also assume*

(2. 42) $\qquad s(1, v) = t(1, v), \ v = 1, \cdots k_1$

for some ordering of $t(1, j), j = 1, \ldots l_1$ (where $l_1 = k_1$). So in particular $\deg h_1 = \deg g_1$. *Assume that $s(1, 1) \geqq s(1, j)$ for $j = 1, \ldots, k_1$, and let*

(2. 43) $\quad t = \{$*number of integers j such that* $s(1, 1) = s(1, j)\}$.

Then, either the conclusion of Theorem 2 *holds or*

$$(2.\ 44) \qquad \sum_{j=1}^{k_1} (s(1, j) - (s(1, j), s(1, 1))) < \frac{n}{t} - s(1, 1).$$

Proof. We merely indicate a proof, noting that the condition (2. 44) is a strong limitation on g_1 and h_1, but by no means does it exclude their existance. We do not know if there exist infinitely many polynomial pairs satisfying these hypotheses.

As at the beginning of the proof of Theorem 3 we assume that $\sigma(2, x)$ and $\sigma(2, y)$ are of order 2 to obtain the inequality:

$$(2.45) \quad 2(n-1) \geqq \sum_{j=1}^{k_1} \sum_{v=1}^{k_1} \big(s(1, v) - (s(1, v), s(1, j))\big) + (k_1 - 1)(n-2)(k_1 - 1).$$

From Lemma 6 and expression (1. 31) (and the elimination of a few wayward cases) we deduce that if (2. 44) does not hold:

$$\sum_{j=1}^{k_1} \sum_{v=1}^{k_1} \big(s(1, v) - (s(1, v), s(1, j))\big) \geqq n - ts(1, 1) + t(k_1 - t)\frac{s(1, 1)}{2}.$$

By noting that $s(1, 1) > \frac{k_1}{n}$, upon simplifying (2. 45) we obtain $2k_1 \geqq n$. We see that this implies $g_1(x)$ is a Chebychev polynomial.

Remark 2. In [5] (especially examples 3—5) the author has included many examples relevant to this paper. In particular, the hypothesis that $g_1(x)$ and $h_1(y)$ (expression (1. 1)) is irreducible is shown to be essential. Also we remark that a reduction to the case where $g_1(x)$ and $h_1(x)$ are indecomposable, is often possible (if $g_1 = \bar{g}_1(\bar{g}_2)$ and $h_1 = \bar{h}_1(\bar{h}_2)$ and $g_1(x) - h_1(y)$ has a genus zero factor, then so does $\bar{g}_1(x) - \bar{h}_1(y)$) and in this case Lemma 7 gives additional information regarding the possibility that $g_1(x) - h_1(y)$ is reducible. See [2] for an explicit description of all cases known (and in fact, the only cases believed to be possible).

Bibliography

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

[2] *W. Feit*, Automorphisms of symmetric balanced incomplete block designs, Math. Zeitschr. **118** (1970), 40—49.

[3] *M. Fried* and *R. MacRae*, a) On the Invariance of Chains of Fields, Illinois J. Math. **13** (1969), 165—171. b) On Curves with Separated Variables, Math. Ann. **180** (1969), 220—226.

[4] *M. Fried*, On a Conjecture of Schur, Mich. Math. Journal **17** (1970), 41—55.

[5] *M. Fried*, Arithmetic of Function Fields. II, Acta Arithmetica (to appear).

[6] *M. Fried*, Field of Definition of Function Fields and a Problem in the Reducibility of Polynomials, Illinois Journal Math. **17** (1973), 128—146.

[7] *W. J. LeVeque*, On the Equation $y^m = f(x)$, Acta Arithmetica **9** (1964), 209—219.

[8] *J. F. Ritt*, Prime and Composite polynomials, Trans. AMS **23** (1922), 51—66.

[9] *P. Samuel*, Lectures on Old and New Results on Algebraic Curves, Tata Institute of Fundamental Research, Bombay 1966.

[10] *C. L. Siegel*, Über einige Anwendungen diophantischer Approximationen, Abhandlungen der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse 1929, No. 1, 14—67.

Stony Brook and Massachusetts Institute of Technology.

Eingegangen 15. November 1971