ON A CONJECTURE OF SCHUR

Michael Fried

from the
MICHIGAN MATHEMATICAL JOURNAL
vol. 17 (1970)
pp. 41-55

ON A CONJECTURE OF SCHUR

Michael Fried

The main purpose of this paper is to prove a conjecture due to I. Schur [11, p. 125]. Let K be a number field, finite-dimensional over the rational field $\mathbb{Q}$. If f(x) denotes an element of the polynomial domain K[x], then we may reduce the polynomial, modulo any prime $\mathfrak{p}$ (of the ring of integers of K) that does not appear in the denominators of the coefficients of f(x). Let $V_{\mathfrak{p}}(f)$ denote the values assumed by f(x), modulo $\mathfrak{p}$. An inspection of $V_{\mathfrak{p}}(f)$ for only a few primes cannot be expected to contribute immensely to our knowledge of f(x). However, Schur conjectured that *if* $V_{\mathfrak{p}}(f)$ *consists of all cosets modulo* $\mathfrak{p}$, *for infinitely many primes* $\mathfrak{p}$ *of* K, *then* f(x) *is a composition of polynomials of two special types:*

(i) $ax^n + b$ (*cyclic polynomials*),

(ii) $T_n(x) = 2^{-n-1}\{(x + (x^2 + 4)^{1/2})^n + (x - (x^2 + 4)^{1/2})^n\}$ (*Chebychev polynomials*).

In the lemma at the end of Section 1, we shall show that if $f(x) \in \mathbb{Q}[x]$ is a composition of polynomials of type (i) and (ii) such that the degree of f is relatively prime to 6, then f is one-to-one (mod p) for infinitely many rational primes p. The condition (deg f, 6) = 1 will also be shown to be necessary. The elegant part of the argument is due to H. Davenport.

That Schur's conjecture is true is our Theorem 2, which follows from our Theorem 1. Theorem 1 is formulated over a fixed field of any characteristic. At the beginning of Section 2, we make certain calculations that have as one consequence our Theorem 3. Let $\mathfrak{k}$ be a finite field, and let $f(x) \in \mathfrak{k}[x]$ be a tame polynomial (see Definition 2). The gist of Theorem 3 is that the polynomial

$$\phi(x, y) = \frac{f(x) - f(y)}{x - y}$$

has an absolutely irreducible factor (as a polynomial in $\mathfrak{k}[x, y]$) in extremely general circumstances, unless f(x) is a composition of polynomials of type (i) and (ii). If the degree of f is small in comparison with the order of $\mathfrak{k}$, then the condition that $\phi(x, y)$ have no absolutely irreducible factors is equivalent to f being one-to-one. This can easily be seen from the proof of Theorem 2, in conjunction with a theorem of MacCluer (see the remarks following Theorem 3).

Actually, Schur himself made many contributions to the problem. In particular, by methods quite different from ours he was able to prove the conjecture for polynomials of prime degree, in the case where $K = \mathbb{Q}$. However, our Lemma 9, which will be used in subsequent work, strengthens even this result.

An analogue of the Schur conjecture is proved in [6]. Let $g_1(x), \cdots, g_\ell(x)$ be in K[x], and assume that $\bigcup_1^\ell V_{\mathfrak{p}}(g_i)$ fills out all cosets modulo $\mathfrak{p}$, for all but a finite

Received October 3, 1968.
This research was supported in part by the Army Research Office - Durham, grant ARO-D-21-124-G892.S1.

Michigan Math. J. 17 (1970).

number of primes p. Then one of $g_1, \cdots, g_\ell$ must be a linear polynomial. The proof requires the use of Chebatorev's density theorem and Hilbert's irreducibility theorem. Schur's conjecture will be seen to hinge on some rather difficult group-theoretic propositions and on the Riemann hypothesis for curves. Except for the use of some deep tools, however, these two theorems seem to have little in common besides their general formulation in terms of Riemann surfaces.

In Section 2, we state two conjectures related to the results of this paper.

1. PROOF OF SCHUR'S CONJECTURE

Suppose L is an arbitrary field and L^* is a fixed algebraic closure of L. A polynomial $f(x) \in L[x]$ is said to be *decomposable over* L if we can write $f(x) = f_1(f_2(x))$, where f_1 and f_2 are polynomials over L of degree greater than 1. We say merely that $f(x)$ is *decomposable* if it is decomposable over L^*. We call f_1 and f_2 *composition factors* of f. The following lemma shows that decomposability is in most cases independent of the field L.

LEMMA 1. *If* $f(x) \in L[x]$ *is decomposable over* L^*, *and if* (deg f, char L) = 1, *then* $f(x)$ *is decomposable over* L. (This lemma is Theorem 3.5 of [7].)

Let λ be an indeterminate over L^*, so that the zeros $\theta_1, \cdots, \theta_n$ of $f(x) - \lambda$ are also indeterminates over L^*. The integer n denotes the degree of f. Let

$$\Omega_{f-\lambda} = L(\theta_1, \cdots, \theta_n, \lambda) = L(\theta_1, \cdots, \theta_n),$$

and let $G(\Omega_{f-\lambda}/L(\lambda))$ denote the Galois group of $\Omega_{f-\lambda}$ over $L(\lambda)$. The group $G^* = G(L^* \cdot \Omega_{f-\lambda}/L^*(\lambda))$ is often referred to as the monodromy group of $f(x) - \lambda$, if char L = 0. The group G^* can be identified as the subgroup of G fixed on the absolute constants of $\Omega_{f-\lambda}$. ■

Definition 1. A permutation group G on the letters $\theta_1, \cdots, \theta_n$ is said to be *imprimitive* if there exists a subdivision of the set $\{\theta_1, \cdots, \theta_n\}$ into disjoint proper sets that are permuted among each other by each element of G. We say G is *primitive* if it is not imprimitive.

LEMMA 2. *Suppose* $f(x) \in L[x]$ *is indecomposable over* L. *Then, in the notation introduced above, the group* $G(\Omega_{f-\lambda}/L(\lambda))$ *is a primitive group when represented on the letters* $\theta_1, \cdots, \theta_n$.

Proof. In [7, Proposition 3.4], it is shown that the fields between $L(\theta_1)$ and $L(\lambda)$ are in one-to-one correspondence with the composition factors of $f(x)$. If $f(x)$ is indecomposable, there exists no proper group between $G(\Omega_{f-\lambda}/L(\lambda))$ and $G(\Omega_{f-\lambda}/L(\theta_1))$. However, if $G(\Omega_{f-\lambda}/L(\lambda))$ were imprimitive, the stabilizer of the set of imprimitivity containing θ_1 would be such a proper subgroup. ■

Definition 2. We shall say that a polynomial f is *tame* over L if either

(1) the characteristic of L is zero, or

(2) (deg f, char L) = 1 and (m + 1, char L) = 1 for all m that are multiplicities of a zero of $f'(x)$ (the derivative of $f(x)$).

If f is tame, then the Riemann surface of $f(x) - \lambda$ over the λ-sphere is tamely ramified.

For the remainder of this section, we limit the discussion to tame polynomials $f(x) \in L[x]$.

We now list some lemmas that will be used in the proof of Theorem 1. These are well-known in the case where L is the field of complex numbers. For the sake of completeness, we shall outline the proof (or give convenient references) for this case. This case is all that we actually need for the Schur conjecture (Theorem 2). We shall comment on the general case after we have stated and proved our lemmas.

Consider the Riemann surface $\mathscr{R}$ for $f(x) - \lambda = 0$ as a branched covering of the λ-sphere, and let $\lambda_1, \cdots, \lambda_r$ be the finite branch points. For a description of the process by which the Riemann surface of $f(x) - \lambda = 0$ is formed, see [13, Chapter 3]. Fix a point λ^* of the λ-sphere different from $\lambda_1, \cdots, \lambda_r, \infty$. Let $\wp_1, \cdots, \wp_r$ denote the places in the fiber above λ^*. For each path $\mathfrak{P}$ starting and ending at λ^* and intersecting none of the branch points, we obtain a permutation of $\wp_1, \cdots, \wp_r$ by mapping $\wp_i$ into $\wp_j$, where $\wp_i$ is the starting point of a lift of the path to the Riemann surface $\mathscr{R}$, and $\wp_j$ is the end point of the same lifted path. By [13; Chapter 4, Theorem 4.1], the point $\wp_j$ is uniquely determined by $\mathfrak{P}$ and $\wp_i$. Similarly, by analytically continuing the zeros $\theta_1, \cdots, \theta_n$ of $f(x) - \lambda = 0$ about $\mathfrak{P}$, we obtain an automorphism of $\Omega_{f-\lambda}/\mathbb{C}(\lambda)$. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_r, \mathfrak{P}_\infty$ be nonintersecting paths on the λ-sphere having the properties that

(a) $\mathfrak{P}_i$ $(i = 1, \cdots, r)$ (respectively, $\mathfrak{P}_\infty$) starts and ends at λ^*, goes around λ_i (respectively, ∞), but goes around no other branch point, and

(b) $\mathfrak{P}_1, \cdots, \mathfrak{P}_r, \mathfrak{P}_\infty$ are pointwise nonintersecting.

Let $\sigma_1, \cdots, \sigma_r, \sigma_\infty$ denote the elements of $G(\Omega_{f-\lambda}/\mathbb{C}(\lambda))$ obtained from the paths $\mathfrak{P}_1, \cdots, \mathfrak{P}_r, \mathfrak{P}_\infty$. We call $\sigma_1, \cdots, \sigma_r, \sigma_\infty$ *branch cycles.*

LEMMA 3. *The surface $\mathscr{R}$ is totally ramified over $\lambda = \infty$. If we replace the letters $\theta_1, \cdots, \theta_n$ by 1, 2, $\cdots$, n, we may write $\sigma_\infty = (1, 2, \cdots, n)$ (that is, the element σ_∞ is an n-cycle).*

Proof. The lemma is an immediate consequence of the fact that the Puiseux expansions for $f(x) - \lambda = 0$ over $\lambda = \infty$ are of the form

$$\theta_1 = \alpha_{-1}\lambda^{1/n} + \alpha_0 + \alpha_1\lambda^{-1/n} + \cdots,$$

$$\theta_2 = \alpha_{-1}\zeta_n\lambda^{1/n} + \alpha_0 + \alpha_1\zeta_n^{-1}\lambda^{-1/n} + \cdots,$$

$$\theta_n = \alpha_{-1}\zeta_n^{n-1}\lambda^{1/n} + \alpha_0 + \alpha_1\zeta_n^{-(n-1)}\lambda^{-1/n} + \cdots,$$

where ζ_n is a primitive nth root of 1. ■

LEMMA 4. *There exists an ordering of $\sigma_1, \cdots, \sigma_r$ such that $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = \sigma_\infty$.*

Proof. For some ordering of the paths $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$, the path obtained by juxtaposition of these paths is homologous on the λ-sphere (minus the branch points $\lambda_1, \cdots, \lambda_r, \infty$) to the path $\mathfrak{P}_\infty$. The lemma is an immediate consequence of the fact that the automorphisms of $\Omega_{f-\lambda}/\mathbb{C}(\lambda)$, obtained from homologous paths, are the same (see [13, Theorem 4.4, p. 81]). ■

Definition 3. Let G be a permutation group. If σ is in G and $\sigma = \gamma_1 \cdots \gamma_s$, then

$$\text{ind } \sigma = \sum_{i=1}^{s} [\text{ord}(\gamma_i) - 1].$$

LEMMA 5. *Let* $\sigma_1, \cdots, \sigma_r$ *satisfy the conditions of the description preceding Lemma* 3. *Then* $\sum_1^r \text{ind } \sigma_i = n - 1$.

Proof. If x_0 is a zero of multiplicity m of $f(x) - f(x_0)$, then some place of the Riemann surface $\mathscr{R}$ is ramified over $x_0 = f(x_0)$ with ramification index m. We can see this most easily by computing the Puiseux expansions of $f(x) = \lambda$ about the value x_0. Of course, λ_0 must be one of the points $\lambda_1, \cdots, \lambda_r, \infty$. The ramification of this place over λ_0 contributes a disjoint cycle to $\sigma_{\lambda_0} = \gamma_1 \cdots \gamma_s$ (written as a product of disjoint cycles). Say that the corresponding disjoint cycle is γ_1. Then γ_1 is of order m, so that

$$|\gamma_1| - 1 = m - 1.$$

Since x_0 is a zero of $f'(x)$ of multiplicity $m - 1$, the sum of the multiplicities of the zeros of $f'(x)$ is the same as $\sum_1^r \text{ind } \sigma_i$. The lemma follows from the fact that the degree of $f'(x)$ is $n - 1$. ■

Definition 4. Let $\mathscr{R}$ and $\mathscr{S}$ be two Riemann surfaces over the λ-sphere. Suppose λ^* is a fixed point on the λ-sphere and is not a branch point for either $\mathscr{R}$ or $\mathscr{S}$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ (respectively, $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$) be the places in the fiber over λ^* in $\mathscr{R}$ (respectively, $\mathscr{S}$). We say that $\mathscr{R}$ *and* $\mathscr{S}$ *exhibit the same branching over the* λ-*sphere* if there exists a labeling of the fibers over λ^* on $\mathscr{R}$ and $\mathscr{S}$ such that the branch cycles for $\mathscr{R}$ and $\mathscr{S}$ are the same. The proof of the next lemma shows that when the branching for $\mathscr{R}$ and $\mathscr{S}$ is the same, then $\mathscr{R}$ and $\mathscr{S}$ are analytically isomorphic. The isomorphism is canonical when λ^* is fixed.

LEMMA 6. *Suppose there exists* $g(x) \in L^*[x]$ *such that the Riemann surface* $\mathscr{R}$ *and the Riemann surface* $\mathscr{S}$ *of* $g(x) - \lambda$ *exhibit the same branching over the* λ-*sphere. Then there exist constants* $a, b \in L^*$ *such that* $g(ax + b) = f(x)$.

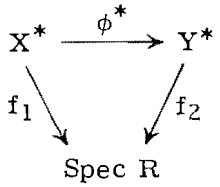
Proof. Let $\mathfrak{p}$ be a place on $\mathscr{R}$. Draw a simple path $\mathfrak{P}^*$ from $\mathfrak{p}$ to some $\mathfrak{p}_i$ (an element of the fiber above λ^*) so that $\mathfrak{P}^*$ intersects no ramified place. Project $\mathfrak{P}^*$ to a path $\mathfrak{P}$ on the λ-sphere. Lift $\mathfrak{P}$ (this may be done uniquely by [13, Chapter 4, Theorem 4.1]) to a path $\mathfrak{Q}^*$ on $\mathscr{S}$ starting at $\mathfrak{q}_i$. The end point of $\mathfrak{Q}^*$ is an analytic function of $\mathfrak{p}$ as we vary $\mathfrak{p}$. The fact that $\mathfrak{q}$ is uniquely determined by $\mathfrak{p}$ (independent of the path $\mathfrak{P}^*$) is a simple consequence of the fact that $\mathscr{R}$ and $\mathscr{S}$ exhibit the same branching.

We thus obtain an analytic isomorphism $\phi: \mathscr{R} \to \mathscr{S}$. If f is a meromorphic function on $\mathscr{S}$, we induce a meromorphic function on $\mathscr{R}$ by sending f into $f \circ \phi$. Thus we induce an isomorphism of the function fields of $\mathscr{R}$ and $\mathscr{S}$. By construction, this isomorphism is the identity on $\mathbb{C}(\lambda)$, the function field of the λ-sphere. The function field for $\mathscr{R}$ is given by $\mathbb{C}(\theta_i)$, where θ_i is any one of the zeros of $f(x) - \lambda$. Similarly, the function field for $\mathscr{S}$ is given by $\mathbb{C}(\alpha_j)$, where $\alpha_1, \cdots, \alpha_n$ are the zeros of $g(x) - \lambda$. Thus $\mathbb{C}(\theta_1)$ is isomorphic to $\mathbb{C}(\alpha_j)$, by an isomorphism fixed on $\mathbb{C}(\lambda)$. The only fields isomorphic to $\mathbb{C}(\alpha_j)$ over $\mathbb{C}(\lambda)$ are the fields $\mathbb{C}(\alpha_i)$ $(i = 1, \cdots, n)$. Hence, for some integer i, $\mathbb{C}(\theta_1) = \mathbb{C}(\alpha_i)$. By simple field theory, α_i is a linear fractional transformation of θ_1; therefore

$$f(\theta_1) = \lambda = g(\alpha_i) = g\left(\frac{\theta_1 + b}{c\theta_1 + d}\right).$$

Since θ_1 is an indeterminate, we conclude that $c = 0$, $d \neq 0$, and $f(x) = g(a'x + b')$ for some $a', b' \in \mathbb{C}$. ■

Remarks. In his thesis [8], W. Fulton gives a general procedure for proving properties such as those occurring in the preceding lemmas, over any field. Without appealing to the Lefschetz principle, he shows [8, Corollary 6.9, p. 6.7] that these results hold over any field with characteristic zero. If L^* is of positive characteristic, let R be the Witt vector ring with residue class field L^*. Suppose ϕ: $X \to Y$ is a tame cover of complete, irreducible, nonsingular curves defined over L^*. Then there exist schemes X^* and Y^* that fit into a diagram



(where f_1, f_2 are proper maps) whose reduction is ϕ: $X \to Y$, such that aut (X^*/Y^*) (the group of automorphisms of X^* over Y^*) is canonically isomorphic to aut (X/Y). Lemmas 3, 4, 5, 6 were concerned with the automorphisms of the Riemann surface of $\Omega_{f-\lambda}(X)$ over the λ-sphere (Y). The facts about aut (X^*/Y^*), where X^*, Y^* are the lifted schemes as given in the diagram above, then go over canonically to aut (X/Y). As a matter of fact, it is an easy application of the Riemann-Roch theorem to show that X^* is actually a model for the Riemann surface of some function field $\Omega_{f^*-\lambda^*}$, where $f^* \in R[x]$ reduces to f, modulo the maximal ideal of R, and λ^* is an indeterminate over the quotient field of R. A careful reading of [8] (especially pages 4.9 to 4.12) will make clear the proofs of these results and how they lead to proofs of Lemmas 3, 4, 5, and 6 in general. These and the remaining results of [8] were previously announced by A. Grothendieck in [9]. The proofs in [8] rely heavily on the work of Grothendieck; in particular, the elementary properties of formal schemes are used. It seems quite reasonable that an easier proof of the lifting can be found, at least in the special case required for the proof of Theorem 1, when char $L \neq 0$. However, in later applications these facts, as presented here, will be needed in their full generality.

We record now one important comment. Without the assumption that f(x) is tame, we *cannot* associate elements of $G(\Omega_{f-\lambda}/L(\lambda))$ with the branch points. This corresponds to the fact that Puiseux expansions exist only around tamely ramified places of the λ-sphere.

We are now ready for our main result. Consider the polynomial

$$\phi(x, y) = \frac{f(x) - f(y)}{x - y} \tag{3}$$

in two variables.

THEOREM 1. *If* $f(x) \in L[x]$ *is indecomposable, tame, and neither a cyclic nor a Chebychev polynomial, then* $\phi(x, y)$ *is absolutely irreducible.*

We need the following facts from group theory. The first is due to Schur [12]. The second originated with Burnside [2], but Schur gave an elegant alternate proof of it [3, p. 234].

LEMMA 7. *If a primitive permutation group* G *of degree* n *contains an* n*-cycle, then either* n *is prime or* G *is doubly transitive.*

LEMMA 8. *If* G *is a group of prime degree* p *and* G *is not doubly transitive, then* $|G|$ *divides* $p(p-1)$.

The following lemma almost immediately implies Theorem 1.

LEMMA 9. *Suppose* f *has degree* n *and* f *is indecomposable over* L^*, *tame, and neither a cyclic nor a Chebychev polynomial. Then the group*

$$G(L^* \cdot \Omega_{f-\lambda}/L^*(\theta_1))$$

is transitive on the letters $\theta_2, \cdots, \theta_n$.

Proof of Theorem 1. To see that Lemma 9 implies Theorem 1, note that $\phi(\theta_1, y)$ has exactly the zeros $\theta_2, \cdots, \theta_n$. By simple Galois theory, $\phi(\theta_1, y)$ is irreducible over $L^*(\theta_1)$ if and only if $G(L^* \cdot \Omega_{f-\lambda}/L^*(\theta_1))$ is transitive on $\theta_2, \cdots, \theta_n$. Since θ_1 is an indeterminate, the irreducibility of $\phi(\theta_1, y)$ over $L^*(\theta_1)$ is equivalent to the absolute irreducibility of $\phi(x, y)$ over L. Of course, transitivity of $G(L^* \cdot \Omega_{f-\lambda}/L^*(\theta_1))$ on the letters $\theta_2, \cdots, \theta_n$ is equivalent to double transitivity of $G(L^* \cdot \Omega_{f-\lambda}/L(\lambda)) = G^*$. We now show the double transitivity of G^*, under the conditions of Lemma 9. We note that G^* is a subgroup of $G(L \cdot \Omega_{f-\lambda}/L(\lambda))$, and this latter group is sometimes more useful than G^*, when special information is available.

Proof of Lemma 9. Lemmas 2 and 3 imply that G^* is a primitive permutation group on the letters $\theta_1, \cdots, \theta_n$, and also that G^* contains an n-cycle, where $n = \deg f$. If n is composite, then Lemma 7 implies that G^* is doubly transitive, and Lemma 9 is established. Now suppose that n is a prime p and that G^* is not doubly transitive. Then, by Sylow's theorem, Lemma 8 implies that the group generated by $\sigma_\infty = (1, 2, \cdots, p)$ is a normal subgroup. We shall prove that if f is tame, then f is either a cyclic or a Chebychev polynomial. We now divide the argument into three steps.

Step 1. *With the notation preceding Lemma* 3, σ_i $(i = 1, \cdots, r)$ *fixes at most one letter.*

Suppose σ_i fixes two letters. We may rename the branches so that these letters are 1 and a. The operation of renaming the branches is algebraically achieved by conjugating all elements of the group by some power of σ_∞.

Since σ_∞ generates a normal subgroup of G^*, we have that $\sigma_i \sigma_\infty \sigma_i^{-1} = \sigma_\infty^s$ for some integer s. But in this case,

$$\sigma_i \sigma_\infty \sigma_i^{-1} = (1, \cdots, a, \cdots) = \sigma_\infty^s = (1, 1+s, 1+as, \cdots) \tag{4}$$

(where a is in the ath position in the second member). Thus $a \equiv 1 + (a-1)s \pmod p$. By solving this congruence, we see that s must be 1. Equation (4) implies that

$$\sigma_i \sigma_\infty \sigma_i^{-1} = \sigma_\infty. \tag{5}$$

By comparing the two sides of equation (5), we see that if $\sigma_i: 1 \to t$, then

$$\sigma_i^{-1}: t+1 \to 2 \quad \text{or} \quad \sigma_i: 2 \to t+1.$$

In general, σ_i: $u \to u + t - 1$, which implies that σ_i is a power of σ_∞. By definition, σ_i is not the identity (that is, $t \neq 1$ in the discussion above); hence σ_i fixes no letters, contrary to the assumption that it fixed two letters.

Step 2. *Description of the two possible types of branching of* $f(x) - \lambda$.

For each i, σ_i leaves at most one letter fixed. If we write σ_i as a product of disjoint cycles, we see easily that $\operatorname{ind} \sigma_i \geq (p - 1)/2$, with equality if and only if σ_i consists of a product of $(p - 1)/2$ two-cycles. By Lemma 5, $\sum_1^r \operatorname{ind} \sigma_i = p - 1$. There are only two possible cases, namely $r = 1$ and $r = 2$. If $r = 1$, then $\operatorname{ind} \sigma_1 = p - 1$. Thus $f'(x) = b(x - a)^{p-1}$, and $f(x)$ is a cyclic polynomial. If $r = 2$, then

$$\operatorname{ind} \sigma_1 = \operatorname{ind} \sigma_2 = (p - 1)/2,$$

and σ_1 and σ_2 both consist of $(p - 1)/2$ disjoint two-cycles.

Step 3. *Explicit description of the case* $r = 2$.

We now show that up to a relabeling of the branches of $f(x) - \lambda$, the branching type is determined by the conditions that $\sigma_1 \sigma_2 = \sigma_\infty$ and that σ_1 and σ_2 both consist of $(p - 1)/2$ disjoint two-cycles. By relabeling the branches of $f(x) - \lambda$, we may assume σ_1 contains the two-cycle (1, 2). Thus σ_2 contains the cycle (1, 3); therefore σ_1 contains (3, p) and σ_2 contains (p, 4); hence σ_1 contains (p - 1, 4) and σ_2 contains (p - 1, 5); it follows that σ_1 contains (p - 2, 5) and σ_2 contains (p - 2, 6), and so forth.

By Lemma 6, we may conclude that (up to a linear change of variable) there exists at most one polynomial $f(x)$ such that $f(x) - \lambda$ has this type of branching. We may move the branch points $\lambda_1, \lambda_2, \infty$ at will to $\lambda_1', \lambda_2', \infty$, by a linear change of λ. This amounts to changing $f(x)$ to $af(x) + b$, for some $a, b \in L^*$. If the characteristic of L is 2 or p, then, by Definition 2, no such *tame* polynomial $f(x)$ exists. However, if (char L, 2p) = 1, the Chebychev polynomials $T_p(x)$ have this branching (see Lemmas 12 and 13 for more explicit information on the Chebychev polynomials). ■

Let K be an algebraic number field. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we denote the order of the residue class field $\mathcal{O}_K/\mathfrak{p}$ by $N(\mathfrak{p})$. If $f(x) \in K[X]$ has its coefficients in the ring of integers $\mathcal{O}_K$ localized at the prime ideal $\mathfrak{p}$, we say that $f(x)$ has *good reduction* modulo $\mathfrak{p}$. This means that we may reduce the coefficients of f modulo $\mathfrak{p}$. If $f(x)$ is decomposable over K, say $f = f_1(f_2)$, then good reduction of $f(x)$ modulo a prime $\mathfrak{p}$ does not imply good reduction of f_1 or f_2. Although the next lemma is sometimes useful in this connection, it is not needed for the arguments of this paper. We remark only that Lemma 10 may be proved in exactly the same manner as Lemma 1.

LEMMA 10. *Suppose* $f(x) \in K[X]$ *and* $\deg f = n$. *Suppose further that* $f = f_1(f_2)$ *is decomposable over* K *and has good reduction modulo* $\mathfrak{p}$. *If* $(n, N(\mathfrak{p})) = 1$, *then there exist* $g_1, g_2 \in K[X]$ *such that* $f_2 = a g_2 + b$ *for some* $a, b \in K$, *and such that* $f = g_1(g_2)$, *where* g_1 *and* g_2 *have good reduction modulo* $\mathfrak{p}$.

The following lemma in its most general form is usually attributed to E. Noether. For the reader's convenience, we provide a simple proof of the lemma. A reader familiar with ultraproducts should have no trouble giving an even shorter proof. We suspect that neither proof is new.

LEMMA 11. *Let* K *be a number field. If* $\phi(x, y) \in K[x, y]$ *is an absolutely irreducible polynomial in two variables over* K, *then* $\phi(x, y)$ *modulo* $\mathfrak{p}$ *is absolutely irreducible over* $\mathcal{O}_{K/\mathfrak{p}}$, *for almost all primes* $\mathfrak{p}$ *of the ring of integers* $\mathcal{O}_K$ *of* K.

Proof. Let L be any field (char $L \geq 0$) over which it makes sense to consider $\phi(x, y)$. Let $r = \deg \phi - 1$. Then $\phi(x, y)$ is reducible over L^* if and only if there exist polynomials

$$h_1 = \sum_{i+j \leq r} a_{i,j} x^i y^j, \qquad h_2 = \sum_{i+j \leq r} b_{i,j} x^i y^j$$

such that

$$h_1 h_2 - \phi(x, y) \equiv 0, \tag{6}$$

where $h_1, h_2 \in L^*[x, y]$. Treat the a's and b's as indeterminates over L^*. The coefficients of (6) (quadratic polynomials in the a's and b's with coefficients in L) are a basis for an ideal $\mathfrak{A}(L)$ of the ring

$$R(L) = L[a_{1,1}, \cdots, a_{r,r}; b_{1,1}, \cdots, b_{r,r}].$$

By Hilbert's Nullstellensatz, $\mathfrak{A}(L) = R(L)$ if and only if $\mathfrak{A}(L)$ has no zero over L^*, and this is equivalent to the absolute irreducibility of $\phi(x, y)$ over L. If, as is the case by hypothesis, $\mathfrak{A}(K) = R(K)$, then $1 = \sum s_i t_i$, where $s_i, t_i \in R(K)$ and $\{t_i\}$ is the basis of $\mathfrak{A}(K)$ described above. Then, for all primes $\mathfrak{p}$ for which we may reduce s_i, t_i $(i = 1, \cdots, \ell)$, we obtain $\mathfrak{A}(\mathcal{O}_{K/\mathfrak{p}}) = R(\mathcal{O}_{K/\mathfrak{p}})$. Thus $\phi(x, y)$ is absolutely irreducible modulo $\mathfrak{p}$. ■

THEOREM 2. *Suppose* $f(x) \in K[x]$ *is a polynomial (not necessarily indecomposable) whose value set* $V_{\mathfrak{p}}(f)$ *consists of all cosets module* $\mathfrak{p}$, *for infinitely many primes* $\mathfrak{p}$ *of* K. *Then* f(x) *is a composite of cyclic and Chebychev polynomials.*

Proof. If f(x) is decomposable over K^*, then by Lemma 1, f(x) is decomposable over K. If $f = f_1(f_2)$, then, excluding the finite number of primes for which either f_1 or f_2 has bad reduction, we see that f is one-to-one modulo $\mathfrak{p}$ if and only if both f_1 and f_2 are one-to-one modulo $\mathfrak{p}$. A simple induction shows that we may assume that f(x) is indecomposable over K^*. Since char K is zero, f(x) is tame. If f(x) is neither a cyclic nor a Chebychev polynomial, then Theorem 1 implies that

$$\phi(x, y) = \frac{f(x) - f(y)}{x - y}$$

is absolutely irreducible over K. By Lemma 11, $\phi(x, y)$ is absolutely irreducible modulo $\mathfrak{p}$ for all but a finite number of primes $\mathfrak{p}$ of K. If $\deg \phi$ is less than the characteristic of $\mathcal{O}_{K/\mathfrak{p}}$, then $\phi(x, x) = f'(x)$ is not identically zero modulo $\mathfrak{p}$; hence $\phi(x, x)$ has no more than $\deg \phi$ zeros modulo $\mathfrak{p}$. The multiplicity of each point (x, y) on the curve $\phi(x, y) \equiv 0 \pmod{\mathfrak{p}}$ is bounded by $\deg f' = \deg \phi$.

Weil [14, p. 71] has shown that if $\phi(x, y)$ is an absolutely irreducible polynomial (modulo $\mathfrak{p}$), then $\phi(x, y) = 0$ has $N(\mathfrak{p}) + O((N(\mathfrak{p}))^{1/2})$ zeros in $\mathcal{O}_{K/\mathfrak{p}}$. As was shown above, if $N(\mathfrak{p}) > \deg f$, then the polynomial $\phi \equiv 0 \pmod{\mathfrak{p}}$ has less than $\deg f$ zeros with $x \equiv y \pmod{\mathfrak{p}}$. Hence it follows that for all but a finite number of $\mathfrak{p}$, $\phi(x, y) \equiv 0 \pmod{\mathfrak{p}}$ has a solution with $x \not\equiv y \pmod{\mathfrak{p}}$. This would imply in addition that $f(x) \equiv f(y) \pmod{\mathfrak{p}}$, which would be a contradiction to the assumption that $V_{\mathfrak{p}}(f)$ consists of all cosets modulo $\mathfrak{p}$. ■

We conclude this section with some lemmas about Chebychev polynomials. These results are known in principle, but we include them for the sake of completeness. If in the expression for $T_n(x)$ (formula (ii)), we let $2z = x + (x^2 - 4)^{1/2}$, then $T_n(x) = (z^n + z^{-n})/2$, where $x = (z + z^{-1})/2$.

LEMMA 12. *If* (n, char L) = 1, *then the Riemann surface for* $T_n(x) - \lambda$ *is branched over* $\lambda = 1, -1, \infty$. *At* $\lambda = -1$ *and* $\lambda = +1$, $(n - 1)/2$ *places have ramification index* 2.

Proof. We can express T_n' in terms of z by the formula

$$T_n' = n\frac{z^{2n} - 1}{(z^2 - 1)z^{n-2}}.$$

Each x different from 1 or -1 occurs for two distinct values of z. Therefore, the $2n - 2$ zeros of $(z^{2n} - 1)/(z^2 - 1)$ correspond to exactly $n - 1$ distinct values of x, which are the zeros of $T_n'(x)$. Since the values of z are $2n$th roots of 1, the values of λ for which there is branching are ± 1. Thus, over each of the finite branch points, the places have ramification as indicated in the statement of the lemma. ■

LEMMA 13. *If* K *is a number field and* $\mathfrak{p}$ *is a prime ideal of* K, *then* $T_n(x)$ *is one-to-one modulo* $\mathfrak{p}$ *if* $(n, N(\mathfrak{p}) - 1) = 1$. *If in addition* $K = \mathbb{Q}$, *then every composition of cyclic and Chebychev polynomials of degrees relatively prime to* 6 *is one-to-one modulo* p, *for infinitely many primes* p.

Proof. If x is a coset modulo $\mathfrak{p}$, associate with x one of the solutions z (it doesn't make any difference which solution) of $x = (z + z^{-1})/2$. All such z lie in the unique quadratic extension F of $\mathcal{O}_{K/\mathfrak{p}}$. If x_1 and x_2 represent distinct cosets modulo $\mathfrak{p}$ such that $T_n(x_1) = T_n(x_2)$, then either $z_1^n = z_2^n$ or $z_1^n = z_2^{-n}$, since we have $z_1^n + z_1^{-n} = z_2^n + z_2^{-n}$. The multiplicative group $F - \{0\}$ is cyclic and of order $N(\mathfrak{p}) - 1$. Since we have assumed $(n, N(\mathfrak{p}) - 1) = 1$, it follows that $z_1 = z_2$ or $z_1 = z_2^{-1}$. Thus $x_1 = x_2$, and therefore $T_n(x)$ is one-to-one modulo $\mathfrak{p}$. Of course, a cyclic polynomial of degree n is one-to-one (mod $\mathfrak{p}$) if and only if $(n, N(\mathfrak{p}) - 1) = 1$.

Let $f(x) = f_1(f_2(\cdots(f_r(x)))$ be a composition of cyclic and Chebychev polynomials of degree $n_1, \cdots, n_r$. If p is a prime such that $(n_i, p^2 - 1) = 1$ for $i = 1, \cdots, r$, then the first part of this lemma, applied to $K = \mathbb{Q}$, shows that f(x) is one-to-one modulo p. Let $n_1 \cdots n_r = N$. We have therefore established the second part of the lemma if we show that there exist infinitely many primes p such that $(N, p \pm 1) = 1$. However, there are infinitely many primes in the arithmetic progression $\{jN + 2\}$, because $(N, 2) = 1$. We have that $((jN + 2) \pm 1, N) = 1$, because $(N, 3) = 1$, and hence we are done. ■

It is important to observe that if f(x) is a composite of cyclic and Chebychev polynomials for which $(\deg f, 6) \neq 1$, then f is not necessarily one-to-one modulo p for infinitely many primes p. First of all, by the simple properties of cyclic and Chebychev polynomials, f is a composition of cyclic and Chebychev polynomials of prime degree. If $(\deg f, 6) \neq 1$, then f could be one-to-one only if its composition factors of degrees 2 and 3 are one-to-one modulo p. However, polynomials of degree 2 are never one-to-one for large primes p. Certainly x^3 is one-to-one for infinitely many p. However,

$$\frac{T_3(x) - T_3(y)}{x - y}$$

has an absolutely irreducible factor of degree 2 over $\mathbb{Q}$. The argument of Theorem 2 shows that $T_3(x)$ is not one-to-one for large primes p.

2. FURTHER RESULTS AND CONJECTURES

For any finite field F, Davenport and Lewis [4] called $f(x) \in F[x]$ *exceptional relative to* F if $\phi(x, y) = [f(x) - f(y)]/[x - y]$ has no absolutely irreducible factor over F. They conjectured that such polynomials are one-to-one on F. MacCluer [10] showed that this is true if f is tame. The following corollary is an immediate consequence of Theorem 1.

COROLLARY 1. *If* $f(x) \in F[x]$ *is indecomposable and tame, then* f *is exceptional relative to* F *only if* f *is a cyclic or a Chebychev polynomial.*

We now introduce techniques that will allow us to handle some problems where f(x) is decomposable. We remind the reader that we are, as always, restricting ourselves to consideration of tame polynomials.

Suppose $f(x) = h(g(x)) \in L[x]$ (L is arbitrary again), where deg h = n and deg g = m. Let x(i) (i = 1, ⋯, n) denote the zeros of $h(x) - \lambda$, and let x(i, j) (j = 1, ⋯, m) denote the zeros of g(x) - x(i). We choose a primitive mn^{th} root of 1, say ζ_{nm}, in order to identify x(i, j) by its Puiseux expansion over $\lambda = \infty$. We then may label x(i, j) (i = 1, ⋯, n; j = 1, ⋯, m) so that

$$x(i, j) = \alpha_{-1} \zeta_{nm}^{i-1+n(j-1)} \lambda^{\frac{1}{nm}} + \alpha_0 + \alpha_1 \zeta_{nm}^{-(i-1+n(j-1))} \lambda^{-\frac{1}{nm}} + \cdots . \tag{7}$$

With these choices, we can describe the action of the branch cycle over $\lambda = \infty$ by

$$\sigma_\infty = (x(1, 1), x(2, 1), \cdots, x(n, 1), x(1, 2), x(2, 2), \cdots, x(n, m)) . \tag{8}$$

Our biggest concern is to examine when

$$G(\Omega_{f-\lambda}/L(x(1, 1))) \text{ is transitive on the letters } x(i, j) \text{ for } i \neq 1 . \tag{9}$$

LEMMA 14. *Condition* (9) *is equivalent to*

$$\psi(x, y) = \frac{f(x) - f(y)}{g(x) - g(y)}$$

being irreducible as a polynomial in K[x, y].

Proof. Since x(1, 1) is an indeterminate over K, $\psi(x, y)$ is irreducible over K if and only if $\psi(x(1, 1), y)$ is irreducible (as a polynomial in y) over K(x(1, 1)). The zeros of $\psi(x(1, 1), y)$ are exactly the indeterminates x(i, j) (j = 2, ⋯, m; i = 1, ⋯, n), because g(x(1, 1)) = x(1), and the zeros of g(y) - g(x(1, 1)) are exactly the indeterminates x(1, j) (j = 1, ⋯, m). By Galois theory, $\psi(x(1, 1), y)$ is irreducible over K(x(1, 1)) if and only if $G(\Omega_{f-\lambda/K(x(1,1))})$ is transitive on x(i, j) (j = 2, ⋯, m; i = 1, ⋯, n). ■

We need a simple concept to explain what we may describe as the best situation.

Let G be a permutation group on the letters x(1, 1), ⋯, x(n, m), where the sets $X(i) = \{x(i, 1), \cdots, x(i, m)\}$ form a system of imprimitivity. Let H be the subgroup

of G that leaves each of the sets $X(i)$ $(i = 1, \cdots, n)$ fixed as sets. Let H_i $(i = 1, \cdots, n)$ be the permutation group operating on $X(i)$ obtained by restricting to H_i each element of G that maps $X(i)$ into itself.

Let S_n be the symmetric group on n letters. We obtain a group T (isomorphic to S_n) by letting $\sigma \to \sigma_T$ $(\sigma \in S_n)$, where σ_T is the permutation on $x(1, 1), \cdots, x(n, m)$ obtained by setting

$$\sigma_T(x(i, j)) = x(\sigma(i), j). \tag{10}$$

Let T_G be the image in T of G obtained by representing $\sigma \in G$ on the sets $X(i)$ $(i = 1, \cdots, n)$. That is, we forget what σ does on the elements of the sets $X(i)$. We form a map

$$\alpha: G \to T_G \times H_1 \times \cdots \times H_n \quad \text{by} \quad \sigma \to \sigma_T \times [(\sigma_T^{-1}\sigma), \cdots, (\sigma_T^{-1}\sigma)_n]. \tag{11}$$

The map α is easily seen to be a group homomorphism that is injective.

Definition 5. We say that a permutation group G, as described above, is *fully imprimitive* if the homomorphism α of (11) is onto (that is, α is an isomorphism).

We now return to the case where $G = G(\Omega_{f-\lambda}/L(\lambda))$ and the sets of imprimitivity are the sets $X(1), \cdots, X(n)$.

LEMMA 15. *The group* $G(\Omega_{f-\lambda}/L^*(\lambda))$ *is fully primitive on the letters* $x(1, 1), \cdots, x(n, m)$ *with respect to the sets* $X(1), \cdots, X(n)$ *of imprimitivity if*

$$\begin{aligned} &\textit{for each } \lambda \neq \infty, \textit{ at most one of the values } x(i)(\lambda_0) \ (i = 1, \cdots, n) \\ &\textit{is a branch point of } g(x) - y. \end{aligned} \tag{12}$$

Note. Two situations negating (12) can occur. That is, the set

$$x(1)(\lambda_0), \cdots, x(n)(\lambda_0)$$

may contain a given branch point of $g(x) - y$ twice, or this set may contain two distinct branch points of $g(x) - y$.

Proof. Let λ^* be a nonbranch point for $f(x) - \lambda$ on the λ-sphere. Let $\{y_i = x(i)(\lambda^*)\}_1^n$ be the fiber above λ^* on the Riemann surface for $h(x) - \lambda$, and let

$$\{y_{i,j} = x(i, j)(\lambda^*)\}_{i=1,j=1}^{m,n}$$

be the fiber above λ^* on the Riemann surface for $f(x) - \lambda$. Starting at y_1, draw simple paths (call these P^*), in the manner of the paths drawn in the discussion preceding Lemma 3, around branch points for $g(x) - y$. Here we refer to the Riemann surface for $h(x) - \lambda$ as the λ-sphere. In addition, assume that the projections P on the λ-sphere of the paths P^* enclose no additional branch points of $f(x) - \lambda$. The fact that paths P for finite branch points encircle one branch point exactly once is a consequence of (12). In addition to the paths P, draw paths Q on the λ-sphere so as to obtain branch cycles for $h(x) - \lambda$. Again this is to be done in the manner of the discussion preceding Lemma 3.

We denote by $\sigma(P^*)$ the automorphism obtained from P^* of the fiber above y_1 (say $z_1, \cdots, z_m$) on the Riemann surface for $g(x) - y$. If $\sigma(P^*)$: $z_i \to z_j$, then

$$\sigma(P^*)\sigma(P_\infty^*)^{i-j}: z_i \to z_i.$$

By projecting these paths on the λ-sphere we obtain, using $\sigma(Q_\infty^n) = \sigma(P_\infty)$, that

$$\sigma(P)\,\sigma(Q_\infty^n)^{i-j}: y_{i,k} \to y_{i,k}, \tag{13}$$

where k is the unique integer such that $\sigma(P)$ moves $y_{i,k}$. By (12), k is unique. Thus,

$$\sigma(P): y_{i,k} \to y_{j,k}. \tag{14}$$

Also from (12), for $j \neq k$ and all ℓ, we find that

$$\sigma(P): y_{\ell,j} \to y_{\ell,j}. \tag{15}$$

By conjugating the branch cycles of $f(x) - \lambda$ of form $\sigma(P)$ by powers of $\sigma(P)$, it is now easy to see that the image of α in (11) contains $\{1\} \times H_1 \times \cdots \times H_n$. The surjectivity of α follows from the fact that (12) also implies that the image of the group generated by the branch cycles of form $\sigma(Q)$ is exactly $T_G \times \{1\} \times \cdots \times \{1\}$. ■

THEOREM 3. *Let* $h, g \in L^*[x]$, *and let* $f(x) = h(g(x))$. *Using the notation following Corollary* 1, *if* (12) *holds and* $h(x)$ *is indecomposable and neither a cyclic nor Chebychev polynomial, then*

$$\psi(x, y) = \frac{f(x) - f(y)}{g(x) - g(y)} \tag{16}$$

is irreducible.

Proof. By Lemma 14, we must show that $G(\Omega_{f-\lambda}/L^*(x(1, 1)))$ is transitive on the letters $x(i, j)$ for $j \neq 1$. By Lemma 15, $G(\Omega_{f-\lambda/L^*(\lambda)})$ is fully primitive. Therefore our result follows from the fact that $G(\Omega_{h-\lambda/L^*(\lambda)})$ is doubly transitive on $x(1), \cdots, x(n)$ and $G(\Omega_{g-y/L^*(y)})$ is transitive on $z(1), \cdots, z(m)$ (the zeros of $g(x) - y$). ■

We do not know necessary and sufficient conditions for either Lemma 15 or Theorem 3. Such conditions would be useful for many arithmetic questions. We point out that without condition (12), Lemma 15 is false. Counterexamples that deny the conclusions of both Lemma 15 and Theorem 3 can be obtained from computations with monodromy groups of small order. However, we give only the simple examples

$$h(x) = x^2, \qquad g(x) = T_4(x) \quad \text{(see (ii))}. \tag{17}$$

As is noted in [5, p. 304],

$$\frac{f(x) - f(y)}{g(x) - g(y)} = T_4(x) + T_4(y)$$

is reducible. This contradicts the conclusion of Lemma 15 by the technique of proof of Theorem 3.

The author has incorrectly announced (on at least one occasion) that *if a tame polynomial* f *is exceptional, then* f *is a composition of cyclic and Chebychev polynomials.* As a matter of fact, Theorem 3 is the closest the author has come to proving this conjecture. The author's attempted proof seems to fail because of the possibility that there could exist a polynomial f(x) such that

(18) $f(x) \in K[x]$, where K is a number field,

(19) f is exceptional relative to K, but

(20) f modulo p is exceptional relative to the residue class field of the prime ideal p for only finitely many primes p of the ring of integers of K.

We now make a conjecture that may be regarded as a generalization of MacCluer's result. It is not simple to state; but if it is true, it has many useful consequences. We give one of these as Corollary 3. The procedure around which we base our statement of the conjecture is similar to a method used by Birch and Swinnerton-Dyer [1] to discuss the number of values assumed by a polynomial over a finite field.

Assume $f(x), g(x) \in F[x]$. Eventually, we shall also assume that f and g are tame polynomials. However, the following discussion remains valid without that assumption. Our conjecture will be that the condition

$$V_F(f) \subset V_F(g) \tag{21}$$

is a consequence of a certain condition placed on $G = G(\Omega_{f-\lambda} \cdot \Omega_{g-\lambda}/F(\lambda))$. Because this condition is difficult to describe, we shall state it indirectly.

For $i = 0, 1, \cdots, \deg f$ and $j = 0, 1, \cdots, \deg g$, let m_{ij} denote the number of elements $\lambda_0 \in F$ for which $f(x) = \lambda_0$ has exactly i distinct solutions x_0 and $g(y) = \lambda_0$ has exactly j distinct solutions y_0. Then, if

$$\sum_{i=1}^{n} m_{i0} = 0, \tag{22}$$

condition (21) is also satisfied. Each of the quantities m_{ij} may be computed roughly from G in the following way.

Consider the affine variety S_{ij} given by the condition

$$f(x_1) = f(x_2) = \cdots = f(x_i) = g(y_1) = g(y_2) = \cdots = g(y_j) = z. \tag{23}$$

This algebraic set consists of a finite number of curves irreducible over F. Let $\theta_1, \cdots, \theta_n$ be the zeros of $f(x) = \lambda$, and let $\alpha_1, \cdots, \alpha_m$ be the zeros of $g(y) = \lambda$. We consider the curves T that are not entirely contained in any of the hyperplanes $x_s = x_t$ for $s \neq t$ or $y_u = y_v$ for $u \neq v$. Each such irreducible curve can be described by a generic point of the form $(\theta_1, \theta_2, \cdots, \theta_i; \alpha_1, \cdots, \alpha_j; \lambda)$, where $\theta_1, \cdots, \theta_i$ are distinct and $\alpha_1, \cdots, \alpha_j$ are distinct. Two such generic points describe the same absolutely irreducible curve if there is an element of $G(F^* \cdot \Omega_{f-\lambda} \cdot \Omega_{g-\lambda}/F^*(\lambda)) = G^*$ sending one of the points coordinatewise into the other. A curve T is not absolutely irreducible if one of its generic points is sent into some other point by G, but not into this latter point by G^*. By the Riemann hypothesis for curves [14, p. 71], each of the curves T that is absolutely irreducible has $|F| + O(|F|^{1/2})$ rational points. By Bezout's theorem, any two of these curves have a bounded number of common points. Also, a bounded number of these points lie on any of the hyperplanes $x_s = x_t$ and $y_u = y_v$, since T is contained in none of these hyperplanes. Again by Bezout's theorem, the curves that are not absolutely irreducible have only a bounded number of F-rational points. Clearly, the number N_{ij} of absolutely irreducible curves T on S_{ij} that are contained in none of the hyperplanes $x_s = x_t$ or $y_u = y_v$ is computable from G.

Let m'_{ij} be the number of rational points on S_{ij} whose first i coordinates are distinct and whose next j coordinates are also distinct. The discussion above shows that

$$m'_{ij} = N|F| + O(|F|^{1/2}).$$

Although the problem is combinatorially difficult, we can theoretically solve for m_{ij} in terms of the quantities $m'_{\ell k}$ ($\ell = 1, \cdots, n$; $k = 1, \cdots, m$) and $|F|$. Let the solution be given by

$$L_{ij}(m'_{11}, \cdots, m'_{nm}, |F|) = m_{ij} \quad (i = 1, \cdots, n;\ j = 1, \cdots, m). \tag{24}$$

Let $m''_{ij} = N_{ij}|F|$, and let $m^*_{ij} = L_{ij}(m''_{11}, \cdots, m''_{nm}, |F|)$.

CONJECTURE 1. *If* $f, g \in F[x]$ *are tame polynomials and* $\sum_{i=1}^{n} m^*_{i0} = 0$, *then* $V(f) \subset V(g)$.

Using the procedure above on the special case where f is linear, we would find that $\sum_{i=1}^{n} m^*_{i0} = 0$ if and only if g(x) is exceptional. MacCluer's result [10] implies the truth of Conjecture 1 in the case where f is linear. The reader should be warned that MacCluer stated his result for polynomials of degree less than the characteristic of F, but proved it for tame polynomials.

COROLLARY 2. *If Conjecture* 1 *is true, and* n *and* ℓ *are positive integers, then there exists an integer* $N(n, \ell)$ *with the following property. Assume* $f, g \in \mathbb{Q}[x]$ *and* p *is a rational prime greater than* $N(n, \ell)$ *satisfying the inequalities*

$$\deg f \leq n \quad \textit{and} \quad \deg g \leq n \tag{25}$$

and

$$|V_p(f) - V_p(g)| \leq \ell \tag{26}$$

(in other words, let the values of f *be contained in the values of* g, *with at most* ℓ *exceptions). Then* $V_p(f) \subset V_p(g)$.

Proof. With f and g reduced modulo p, in the notation of the argument preceding Conjecture 1, $\sum_{i=1}^{n} m^*_{i0} \neq 0$ implies that $|V_p(f) - V_p(g)| > \ell$, for large primes p. It follows that $\sum_{i=1}^{n} m^*_{i0} = 0$ for all f, g, and primes p larger than some $N(n, \ell)$, where f and g satisfy (25) and (26). Conjecture 1 now gives the result. ■

Practically nothing is known about the situation where $f(x) \in F[x]$ is not assumed to be tame. Any analogues for nontame polynomials, similar to the results obtained in this paper, should be valuable.

REFERENCES

1. B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla.* Acta Arith. 5 (1959), 417-423.

2. W. Burnside, *On simply transitive groups of prime degree.* Quart. J. Math. 37 (1906), 215-221.

3. R. D. Carmichael, *Introduction to the theory of groups of finite order.* Ginn, Boston, 1937.

4. H. Davenport and D. J. Lewis, *Notes on congruences.* I. Quart. J. Math. Oxford Ser. (2) 14 (1963), 51-60.

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

6. M. Fried, *Arithmetical properties of value sets of polynomials.* Acta Arith. 15 (1969), 91-115.

7. M. D. Fried and R. E. MacRae, *On the invariance of chains of fields.* Illinois J. Math. 13 (1969), 165-171.

8. W. Fulton, *Fundamental group of a curve.* Archives of the Princeton University Mathematics Library, 1966.

9. A. Grothendieck, *Géométrie formelle et géométrie algébrique.* Séminaire Bourbaki, t. 11, no. 182, 1958/59.

10. C. R. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials.* Acta Arith. 12 (1966/67), 289-299.

11. I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen.* S.-B. Preuss. Akad. Wiss., Phys. - Math. Kl. (1923), 123-134.

12. ———, *Zur Theorie der einfach transitiven Permutationsgruppen.* S.-B. Preuss. Akad. Wiss., Phys. - Math. Kl. (1933), 598-623.

13. G. Springer, *Introduction to Riemann surfaces.* Addison-Wesley Publishing Co., Reading, Mass., 1957.

14. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind. no. 1041. Hermann et Cie., Paris, 1948.

Institute for Advanced Study
Princeton, New Jersey 08540
and
State University of New York at Stony Brook
Stony Brook, Long Island, New York 11790