Table des matières du tome XV, fascicule 2

	Page
M. Fried, Arithmetical properties of value sets of polynomials	91
I. Sh. Slavutsky, The simplest proof of Vandiver's theorem	117
R. J. Miech, A number-theoretic constant	119
T. Storer, On the arithmetic structure of Galois Domains	139
K. K. Norton, Upper bounds for k-th coset representatives modulo n	161
J. Lehner and M. Newman, Sums involving Farey fractions	181
M. Mendès France, Nombres transcendants et ensembles normaux	189
J. Wójcik, A refinement of a theorem of Schur on primes in arithmetic progressions III	193
W. M. Schmidt, A problem of Schinzel on lattice points	199

La revue est consacrée à toutes les branches de *l'Arithmétique* et de la *Théorie des Nombres*, ainsi qu'aux *fonctions ayant de l'importance dans ces domaines.*

Prière d'adresser les textes dactylographiés à l'un des rédacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa 1 (Pologne), ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l'échange de Acta Arithmetica.

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 1 (Pologne), Krakowskie Przedmieście 7.

Prix de ce fascicule 4.00 $.

Les volumes I-III (reédits) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XV (1969)

Arithmetical properties of value sets of polynomials

by

M. FRIED (Princeton, N. J.)

Introduction. The extent to which the value sets of a polynomial determine the polynomial depends on many things. Most important of these are the domain and range of the polynomial. Little can be discovered about a polynomial in $\boldsymbol{Z}[x]$ by knowing its value set mod p for only one rational prime p. The object of this paper is to show that if we let p run over almost all rational primes p (i.e. for all but a finite number of primes p — henceforth abbreviated a.a.p.), the value sets mod p of a polynomial yield significant information about the nature of the polynomial. For $h(x) \in \boldsymbol{Z}[x]$ let $V_p(h)$ denote those cosets mod p taken on by $h(x)$. Primarily we devote our attention to:

THE POLYNOMIAL CONJECTURE. *Let* $h(x), g_1(x), \ldots, g_l(x) \in \boldsymbol{Z}[x]$, *and assume* $V_p(h) \subset \bigcup_{i=1}^{l} V_p(g_i)$ *for a.a.p. Then there exists an index* i, *and a polynomial* $r(x) \in \overline{\boldsymbol{Q}}[x]$ (*where* $\overline{\boldsymbol{Q}}$ *is the algebraic closure of* $\boldsymbol{Q}$) *such that* $h(x) = g_i(r(x))$.

Section I is the technical key to the results relating to the polynomial conjecture, which are found in Section II. In Section I we assume that $h(x), g_1(x), \ldots, g_l(x) \in \boldsymbol{Z}[x]$ are all irreducible, and that the set of primes p for which $h(x) \equiv 0 \bmod p$ has a solution is (with finitely many exceptions) contained in the set of primes p for which there exists an index i_p such that $g_{i_p}(x) \equiv 0 \bmod p$ has a solution. We dignify this statement with the title, *local polynomial hypothesis* so that we may refer to it in Section I. We now describe those instances in which we have been able to resolve the polynomial conjecture.

CASE A. If, in the polynomial conjecture, we assume h is linear, then the hypothesis is reduced to the condition

$$\bigcup_{1}^{l} V_p(g_i) = \{0, 1, \ldots, p-1\} \quad \text{for a.a.p.}$$

The conclusion that there exists an index i such that $g_i(x)$ is linear is an immediate consequence of Corollary 2, which states, under the hypo-

thesis of the polynomial conjecture, that there exists an index i such that $\deg g_i$ divides $\deg h$.

CASE B. For the purpose of this work a polynomial $h(x) \in \boldsymbol{Q}[x]$ will be called *cyclic* if $h(x) = a(x-b)^n + c$ for some $a, b, c \in \boldsymbol{Q}$. The terminology is suggested by the fact that the galois group of the splitting field of $h(x) - \lambda$ (the group of monodromy) over $\overline{\boldsymbol{Q}}(\lambda)$ (where λ is an indeterminate) is cyclic. We show in Theorem 3 that the polynomial conjecture is true if the polynomials $g_i(x), i = 1, \ldots, l$, are all cyclic.

CASE C. In Theorem 4 we show that the polynomial conjecture is true in the case where $l = 1$ and $g_1(x) = g(x)$ is of prime degree, or if the group of monodromy of $g(x) - \lambda$ over $\boldsymbol{Q}(\lambda)$ is the symmetric group or alternating group (as a permutation group acting on the zeros of $g(x) - \lambda$), or if $g(x)$ is a composite of polynomials of this type.

We say that $g(x) = s_1(s_2(\ldots(s_r(x))$ is a *prime decomposition* of $g(x)$ if each of the s_i's cannot be written as a composite of polynomials of strictly smaller degree. Even if we specialize the hypothesis of the polynomial conjecture to assume $V_p(h) = V_p(g)$ for a.a.p., we are not able to show the expected conclusion (i.e. that $r(x)$ is linear). However, we are able to conclude (Theorem 5) that each prime decomposition of $h(x)$ corresponds to a prime decomposition of $g(x)$ where the degrees of the prime components of $h(x)$ are the same, in the given order, as the degrees of the prime components in the respective decomposition of $g(x)$.

We include in Section III an application to the Hilbert irreducibility theorem. There we give a condition on a polynomial in two variables insuring that there exists an arithmetic progression of integers with prime modulus such that specialization of one of the variables from the integers of this set leaves the polynomial irreducible in one variable.

Additional comments. The hypothesis $V_p(h) \subset V_p(g)$ for a.a.p. is seen to imply that either g is linear, or else the polynomial $h(x) - g(y)$ is reducible in $\boldsymbol{Z}[x, y]$. We outline this. By Gauss' lemma a factorization of $h(x) - g(y)$ may be assumed to be in $\boldsymbol{Z}[x, y]$. If $h(x) - g(y)$ is irreducible, the Hilbert irreducibility theorem would imply that there exists an integer $x_0 \in \boldsymbol{Z}$ such that $h(x_0) - g(y)$ is irreducible (and non-linear by assumption). From algebraic number theory we know that a non-linear polynomial which is irreducible over the rationals has no zero mod p for infinitely many primes p. This contradicts $V_p(h) \subset V_p(g)$ for a.a.p. In light of this we make a definition.

Let $h(x), g(x)$ be elements of $L[x]$ where L is any field. If there exist polynomials F, h_1, g_1 in $L[x]$ such that $\deg F > 1$, and $F(h_1) = h$, $F(g_1) = g$, we say that h, g are a *composite pair over* L. If $L = \boldsymbol{C}$, we say that h, g are a composite pair. For a time it was conjectured that $h(x) - g(y)$ reducible in $\boldsymbol{C}[x, y]$ implies that h, g are a composite pair.

The truth of this would obviously give some information toward the further resolution of the polynomial conjecture. In fact though, $h(x) - g(y)$ reducible in $\boldsymbol{Z}[x, y]$ does not imply that h, g are a composite pair over $\boldsymbol{C}$, as the following example shows:

$$(x^2 + 2xy + 2y^2 + 1)(x^2 - 2xy + 2y^2 + 1) = x^4 + x^2 + 4y^4 + 4y^2 + 1.$$

This example is obtained by a linear change of homogeneous variables in an example from Davenport, Lewis, and Schinzel [2]. For further information on $h(x) - g(y)$ see this last cited paper and Fried and MacRae [4] where it is shown in particular that if $h_1(x) - g_1(y)$ divides $h(x) - g(y)$, then there exists $F(x)$ such that $h(x) - g(y) = F\big(h_1(x)\big) - F\big(g_1(y)\big)$. It is pertinent to notice that the last cited reference inadvertently has some lemmas and an example similar to those appearing in a paper by Schinzel [12]. Here Schinzel has shown that if the degree of h is a prime, $h(x) - g(y)$ factorizable in $\boldsymbol{Z}[x, y]$ does indeed imply h, g a composite pair. This fact will be used in Theorem 4 (Section II) where a large list of polynomials $h(x)$ is displayed for which the polynomial conjecture is true in the case when $l = 1$. The analog over $\boldsymbol{Z}$ of our polynomial conjecture may be established in a straightforward manner using the Hilbert irreducibility theorem. For completeness we record it here.

THEOREM. *Let* $h(x), g_1(x), \ldots, g_l(x) \in \boldsymbol{Z}[x]$. *Let*

$$X = \Big\{x_0 \in \boldsymbol{Z} \mid h(x_0) \in \bigcup_1^l V_{\boldsymbol{Z}}(g_i)\Big\}.$$

where $V_{\boldsymbol{Z}}(g_i)$ *denotes the set of values of* g_i *at the integers. If* X *has positive lower density, then there exists a polynomial* $r(x) \in \boldsymbol{Q}[x]$ *and an index* i *such that* $g_i\big(r(x)\big) = h(x)$.

Note that the polynomial $r(x)$ in this last theorem is shown to be an element of $\boldsymbol{Q}[x]$, while the polynomial conjecture asserts only that $r(x) \in \overline{\boldsymbol{Q}}[x]$. A simple example will illustrate the need for this. Suppose $h(x) = 2 \cdot 3 \cdot 5x^2$, $g_1(x) = 2x^2$, $g_2(x) = 3x^2$, $g_3(x) = 5x^2$. Then we have

$$V_p(h) \subset \bigcup_1^3 V_p(g_i) \quad \text{for all } p.$$

However, no $g_i(x)$ and $h(x)$ form a composite pair over $\boldsymbol{Q}$. In connection with this, see Proposition 3 and its use in Theorem 4 (comments).

If $h(x), g_1(x), \ldots, g_l(x)$ are cyclic polynomials all of the same prime degree, it is possible to give necessary and sufficient conditions in terms of the arithmetic properties of the coefficients of these polynomials in order that $V_p(h) \subset \bigcup_1^l V_p(g_i)$ for a.a.p. We do this in the case that all the polynomials are quadratic in Section III. Thus, in this case we have a finite process for determining whether or not the hypothesis of the poly-

nomial conjecture is satisfied. Ax, in a paper that will appear in Annals of Mathematics [1], has given a very general theorem which has as a particular consequence the existence of a decision procedure for the hypothesis of the polynomial conjecture, given a fixed set of polynomials $h(x), g_1(x), \ldots, g_l(x)$. There is obviously a very simple decision procedure for the conclusion of the polynomial conjecture to be true.

Since the polynomial conjecture in its entirety is not known to be true, we have inserted several counterexamples to plausible conjectures that would have partially resolved the polynomial conjecture had they been correct. These have been placed at the end of Section III.

Slightly more sophisticated techniques (using Riemann surfaces) than those used in Section II may be used on the polynomial conjecture. These are capable of resolving quite a bit more of the case where $l = 1$, and with some additional hypotheses the case where $g_1, \ldots, g_l$ are all composites of cyclic polynomials. It seems best to put these results into a separate paper because of their extreme technical nature. However, we do include one computation of a geometrical nature in Theorem 4 (comments).

Professor Lewis has suggested the following modification of the hypothesis of the polynomial conjecture in order that it and the hypothesis of Theorem 2 will be equivalent.

MODIFIED POLYNOMIAL CONJECTURE HYPOTHESIS. *Let* $h(x), g_1(x), \ldots, g_l(x) \in \boldsymbol{Z}[x]$. *Let*

$$V_p^s(h) = \{\textit{cosets mod } p \textit{ assumed by } h \textit{ with multiplicity one}\}.$$

Assume

$$V_p^s(h) \subset \bigcup_1^l V_p^s(g_i).$$

This is one of many ways in which we could weaken the hypothesis of the polynomial conjecture without changing the conclusion of Theorem 2. Most such changes call for trivial modifications of the arguments presented in the text and cumbersome rewordings of the theorems. Therefore it has been felt best not to alter the hypothesis of the polynomial conjecture for this greater generality.

Nevertheless, we would like to insert here a conjecture which has as a particular consequence the equivalence of the hypothesis of the polynomial conjecture and the conclusion of Theorem 2.

CONJECTURE. *Let* $f(x) \in \boldsymbol{Z}[x]$, P_k *the polynomials of* $\boldsymbol{Z}[x]$ *of degree* k, *and* l *a positive integer. Then there exists an integer* $N = N(l, k)$ *such that if* p *is any rational prime with* $p > N$, *the following is true; if* $g \in P_k$ *satisfies* $|V_p(f) \div V_p(g)| \leqslant l$, *(i.e. the symmetric difference of the value sets of* f *and* g *has order* $\leqslant l$), *then* $V_p(f) = V_p(g)$ *(i.e. the value sets are actually the same).*

Note. The equivalence described above results from replacing the set P_k by a single polynomial $g(x)$.

We are able to prove this conjecture only in the case where $f(x)$ is a cyclic polynomial, and we give now a quick outline of the case where $f(x)$ is linear. When $f(x)$ is linear the hypothesis is reduced to showing that if $p > N$ and $g(x)$ of degree k takes on all but l values mod p, then $g(x)$ takes on all values mod p.

MacCluer [9] has shown that a polynomial $g(x)$ is one-one mod p (equivalent to $g(x)$ taking on all values mod p) where $\deg g < p$ if and only if $\dfrac{g(x)-g(y)}{x-y}$ as a polynomial in two variables has no absolutely irreducible factors over $\boldsymbol{Z}/(p)$.

Let $n(a)$ be the number of times a is taken on by g (without multiplicity). Then

$$\sum_{a=0}^{p-1} n(a) = p;$$

thus if

$$\tau(a) = \begin{cases} n(a)-1 & \text{for} \quad n(a) \geqslant 1, \\ 0 & \text{otherwise}, \end{cases}$$

then $\sum \tau(a) \geqslant l+1$ implies that g excludes at least $l+1$ values mod p. Assume $p > k$. From MacCluer's result we need only show that

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

has no absolutely irreducible factors mod p. So assume $\varphi(x, y)$ is such an absolutely irreducible factor of $h(x, y)$. If $\varphi(x, y)$ has distinct zeros $S = \{(x_i, y_i) \mid i = 1, \ldots, l+1\}$ where $x_i \neq y_i$, and (y_i, x_i) is not in the set, then we see that g excludes at least $l+1$ values mod p. Each zero of $\varphi(x, y)$ appears with multiplicity at most k. Also, since $(x-y)^2 \nmid g(x)-g(y)$ (just take the partial derivative with respect to x and use the assumption $k < p$) by Bezout's $\varphi(x, y)$ has no more than k zeros (x_0, y_0) where $x_0 = y_0$. By Weil's Riemann Hypothesis for curves [14], since $\varphi(x, y)$ is absolutely irreducible, $\varphi(x, y)$ has $p + O(p^{1/2})$ zeros mod p, and the constant in the O relation is dependent only on the degree of φ and therefore on k. Thus, if $p + O(p^{1/2}) \geqslant 2k(l+1)+k$, we get a set S of zeros of $\varphi(x, y)$ as described above, and a contradiction to our assumption on g.

With pleasure we would now like to thank Professor Lewis for his many helpful comments, and Professors Lewis and LeVeque for their contributions toward the preparation of this manuscript.

I. We reproduce below, without separate references, some notation and theorems all of which can be found in Hasse [5].

Assume $L \subset M$ are two number fields; O_L and O_M their respective rings of integers. If $\mathfrak{z}$ is a prime ideal of O_L, $O_M \cdot \mathfrak{z} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, we say that $\mathfrak{z}$ has g primes over it in M with ramification indices $e_i = e(\mathfrak{p}_i/\mathfrak{z})$ and degrees $f_i = f(\mathfrak{p}_i/\mathfrak{z}) = [O_M/\mathfrak{p}_i : O_L/\mathfrak{z}]$. The symbol $|\mathfrak{z}|$ designates the *norm of* $\mathfrak{z}$, which is the cardinality of the residue class field $O_L/\mathfrak{z}$.

Now assume M/L is galois with group $G(M/L)$. For a prime $\mathfrak{p}$, unramified over L, $\left[\frac{M/L}{\mathfrak{p}}\right]$ is an element of $G(M/L)$ called the Frobenius symbol of $\mathfrak{p}$ over L. It is uniquely determined by the congruence condition

$$\left[\frac{M/L}{\mathfrak{p}}\right] x \equiv x^{|\mathfrak{z}|} \bmod \mathfrak{p} \quad \text{for each } x \in O_M.$$

If U is a subset of $G(M/L)$ which is closed under conjugation (i.e. a class of $G(M/L)$), then the set of primes $\mathfrak{z}$ of L such that $\left[\frac{M}{\mathfrak{p}}\right] \in U$ for $\mathfrak{p} \mid \mathfrak{z}$ has a Dirichlet density and that density is $\frac{\operatorname{card} U}{\operatorname{card} G}$. This is the content of the Čebotarev density theorem.

Let K be any number field containing L, M the galois closure of K, and $G = G(M/L)$. If $L(\alpha) = K$, the group G can be considered as a transitive permutation group acting on the conjugates of α over L. Let $\mathfrak{p}$ be a prime of M, $\sigma = \left[\frac{M/L}{\mathfrak{p}}\right]$. Then σ can be written as $\pi_1 \dots \pi_r$ where π_i are disjoint cycles formed by representing σ as a permutation on the conjugates of α. If $\mathfrak{z} = O_L \cap \mathfrak{p}$, then $\mathfrak{z}$ factors into $\mathfrak{z} \cdot O_K = \prod_{1}^{r} \mathfrak{q}_i$ where the $\mathfrak{q}_i$ $(i = 1, \dots, r)$ are distinct prime ideals of degree $f_i = f(\mathfrak{q}_i/\mathfrak{z})$ = length of π_i. This theorem is due to Artin.

As usual, if L_1/L and L_2/L are two galois extensions we look upon $G(L_1 \cdot L_2/L)$ as a subgroup of $G(L_1/L) \times G(L_2/L)$.

Preparation for Theorem 1. Let L be a number field. We will use the following notation:

p = primes (finite of $\boldsymbol{Q}$),

$P'(L) = \{p \in P \mid p$ has a prime factor of degree one in $L\}$.

If A, B are two sets of primes, we let $A \subset B$ denote the fact that $\operatorname{card}(A - B) < \infty$.

Kummer's theorem implies that a polynomial $h(x) \in \boldsymbol{Z}[x]$ has a zero mod p for a prime p not dividing the discriminant of $h(x)$, if and only if p has a prime ideal factor of degree one in $\boldsymbol{Q}(\theta_h)$, where θ_h is a zero of $h(x)$. This allows us to translate the *local polynomial hypothesis* (see the introduction) to the relation

$$P'\big(\boldsymbol{Q}(\theta_h)\big) \subset \bigcup_{1}^{l} P'\big(\boldsymbol{Q}(\theta_{g_i})\big).$$

Let Ω be the composite of the fields $\Omega_h, \Omega_{g_1}, \dots, \Omega_{g_l}$ which are respectively the splitting fields of the polynomials $h, g_1, \dots, g_l$ over $\boldsymbol{Q}$.

THEOREM 1. *Let $h, g_1, \dots, g_l$ be irreducible polynomials of $\boldsymbol{Z}[x]$. Then*

$$P'\big(\boldsymbol{Q}(\theta_h)\big) \subset \bigcup_{1}^{l} P'\big(\boldsymbol{Q}(\theta_{g_i})\big) \tag{1}$$

holds if and only if

$$\bigcup_{\theta_h} G\big(\Omega/\boldsymbol{Q}(\theta_h)\big) \subset \bigcup_{1}^{l} \bigcup_{\theta_{g_i}} G\big(\Omega/\boldsymbol{Q}(\theta_{g_i})\big). \tag{2}$$

Remark. One can easily deduce from this theorem a theorem of Schinzel [11].

Proof. Let $\mathfrak{a}$ be a prime of Ω over $\mathfrak{p}$, $\mathfrak{p}$ a prime of Ω_h over $p \in P$, and assume $e(\mathfrak{a}/p) = 1$. Since $h(x)$ is irreducible, Artin's theorem implies that p has a prime ideal factor of degree one in $\boldsymbol{Q}(\theta_h)$ if and only if $\left[\frac{\Omega_h}{\mathfrak{p}}\right]$ is in $\bigcup_{\theta_h} G\big(\Omega_h/\boldsymbol{Q}(\theta_h)\big)$. Since $\left[\frac{\Omega}{\mathfrak{a}}\right]\Big|_{\Omega_h} = \left[\frac{\Omega_h}{\mathfrak{p}}\right]$, we conclude that $p \in P'\big(\boldsymbol{Q}(\theta_h)\big)$ if and only if $\left[\frac{\Omega}{\mathfrak{a}}\right] \in \bigcup_{\theta_h} G\big(\Omega/\boldsymbol{Q}(\theta_h)\big)$.

Similarly, $p \in P'\big(\boldsymbol{Q}(\theta_{g_i})\big)$ for some i, is equivalent to

$$\left[\frac{\Omega}{\mathfrak{a}}\right] \in \bigcup_{1}^{l} \bigcup_{\theta_{g_i}} G\big(\Omega/\boldsymbol{Q}(\theta_{g_i})\big).$$

From (1) and the Čebotarev density theorem if $\sigma \in \bigcup_{\theta_h} G\big(\Omega/\boldsymbol{Q}(\theta_h)\big)$, then $\sigma = \left[\frac{\Omega}{\mathfrak{a}}\right]$ for infinitely many primes $\mathfrak{a}$ of Ω and so $\sigma \in \bigcup_{1}^{l} \bigcup_{\theta_{g_i}} G\big(\Omega/\boldsymbol{Q}(\theta_{g_i})\big)$.

Conversely, the hypothesis (2) implies that if p is not one of finitely many primes, then $p \in P'\big(\boldsymbol{Q}(\theta_h)\big)$ is equivalent to $\left[\frac{\Omega}{\mathfrak{a}}\right] \in \bigcup_{\theta_h} G\big(\Omega/\boldsymbol{Q}(\theta_h)\big)$. Thus $\left[\frac{\Omega}{\mathfrak{a}}\right] \in G\big(\Omega/\boldsymbol{Q}(\theta_{g_i})\big)$ for some index i, and this is equivalent to $p \in P'\big(\boldsymbol{Q}(\theta_{g_i})\big)$.

The following two lemmas of galois theory will be used several times. The techniques for proving them are well known and we merely mention

that the first is a simple consequence of the theorem of natural irrationalities while the second is a corollary of the first.

LEMMA 1. *Let $f(x)\epsilon L[x]$ be an irreducible polynomial, where L is any perfect field. Let $\Omega = L(x_1, \dots, x_n)$ be the splitting field of f over L, and $x_1, \dots, x_n$ the zeros of f. If M is any galois subfield of Ω containing L, then any automorphism of $G(M/L)$ which leaves $K = L(x_1) \cap M$ elementwise fixed can be extended to an element of $G\big(\Omega/L(x_1)\big)$.*

LEMMA 2. *With the notation of Lemma 1, suppose $L(x_1) \cap M = L$. Then*

$$G(\Omega/M) - \bigcup_1^n G\big(\Omega/M\cdot L(x_i)\big)$$

is not empty.

We are now in a position to show that Theorem 1 implies a strong relation between the splitting fields of the polynomials $h, g_1, \dots, g_l$ over $\boldsymbol{Q}$. For simplicity we assume $l = 2$.

PROPOSITION 1. *Let h, g_1, g_2 be irreducible over $\boldsymbol{Q}$. If*

$$P'\big(\boldsymbol{Q}(\theta_h)\big) \subset \bigcup_1^2 P'\big(\boldsymbol{Q}(\theta_{g_i})\big)$$

then either

$$\boldsymbol{Q}(\theta_{g_1}) \cap (\Omega_{g_2}\cdot\Omega_h) \neq \boldsymbol{Q}$$

or

$$\boldsymbol{Q}(\theta_{g_2}) \cap (\Omega_{g_1}\cdot\Omega_h) \neq \boldsymbol{Q}.$$

Proof. If the conclusion of the proposition is false, then we may take $\Omega = \Omega_{g_1}$, $M = \Omega_{g_1} \cap (\Omega_{g_2}\cdot\Omega_h)$ in Lemma 2 to conclude that there exists

$$\sigma_1 \epsilon G(\Omega_{g_1}/\boldsymbol{Q}) - \bigcup_{\theta_{g_1}} G\big(\Omega_{g_1}/\boldsymbol{Q}(\theta_{g_1})\big), \tag{3}$$

such that

$$\sigma_1|_{\Omega_{g_1}\cap(\Omega_{g_2}\cdot\Omega_h)} = \text{identity}.$$

Similarly, there exists

$$\sigma_2 \epsilon G(\Omega_{g_2}/\boldsymbol{Q}) - \bigcup_{\theta_{g_2}} G\big(\Omega_{g_2}/\boldsymbol{Q}(\theta_{g_2})\big) \tag{4}$$

such that

$$\sigma_2|_{\Omega_{g_2}\cap(\Omega_{g_1}\cdot\Omega_h)} = \text{identity}.$$

Let $\Omega = \Omega_h\cdot\Omega_{g_2}\cdot\Omega_{g_1}$ as in Theorem 1, so that our hypotheses imply

$$\bigcup_{\theta_h} G\big(\Omega/\boldsymbol{Q}(\theta_h)\big) \subset \bigcup_1^2 \bigcup_{\theta_{g_i}} G\big(\Omega/\boldsymbol{Q}(\theta_{g_i})\big). \tag{5}$$

If

$$(\sigma_1, \sigma_2, 1) \epsilon G(\Omega_{g_1}/\boldsymbol{Q}) \times G(\Omega_{g_2}/\boldsymbol{Q}) \times G(\Omega_{g_3}/\boldsymbol{Q})$$

is an element of $G(\Omega/\boldsymbol{Q})$ we obtain a contradiction as follows. Since $(\sigma_1, \sigma_2, 1)|_{\Omega_h}$ is the identity, $(\sigma_1, \sigma_2, 1) \epsilon G\big(\Omega/\boldsymbol{Q}(\theta_h)\big)$ for each θ_h.

However, $(\sigma_1, \sigma_2, 1)|_{\Omega_{g_i}} = \sigma_i$ for $i = 1, 2$ and this contradicts (5).

In order to show that $(\sigma_1, \sigma_2, 1) \epsilon G(\Omega/\boldsymbol{Q})$ we must show

$$(\sigma_1, \sigma_2)|_{\Omega_h\cap(\Omega_{g_1}\cdot\Omega_{g_2})} = \text{identity}. \tag{6}$$

By the definition of σ_1 and σ_2, (σ_1, σ_2) is the identity on the field T equal to

$$\{\Omega_{g_1} \cap (\Omega_{g_2}\cdot\Omega_h)\}\cdot\{\Omega_{g_2} \cap (\Omega_{g_1}\cdot\Omega_h)\}.$$

To show that T contains $\Omega_h\cdot(\Omega_{g_1}\cdot\Omega_{g_2})$, we may without loss assume that $\Omega_h \subset \Omega_{g_1}\cdot\Omega_{g_2} = \Omega'$ and from the fundamental theorem of galois theory we must demonstrate that

$$G(\Omega'/T) \subset G(\Omega'/\Omega_h). \tag{7}$$

Let

$$A = G(\Omega'/\Omega_h), \qquad B = G(\Omega'/\Omega_{g_1}), \qquad C = G(\Omega'/\Omega_{g_2})$$

so that

$$B \cap C = G(\Omega'/\Omega_{g_1}\cdot\Omega_{g_2}) = \{1\}.$$

From galois theory we easily see that (7) is reduced to

$$\{B\cdot(A \cap C)\} \cap \{C\cdot(A \cap B)\} \subset A. \tag{8}$$

If $cb = c'b'$ where $b\epsilon B$, $b'\epsilon A \cap B$, $c\epsilon A \cap C$, and $c'\epsilon C$, then $c^{-1}c' = b(b')^{-1}\epsilon C \cap B = \{1\}$. Thus $cb\epsilon A$ and this verifies (8).

In particular, if we take $h(x)$ linear in Proposition 1 we obtain

COROLLARY 1. *Let g_1, g_2 be irreducible polynomials in $\boldsymbol{Q}[x]$. Then $P = \bigcup_1^2 P'\big(\boldsymbol{Q}(\theta_{g_i})\big)$ implies that either $\boldsymbol{Q}(\theta_{g_1}) \cap \Omega_{g_2} \neq \boldsymbol{Q}$ or $\boldsymbol{Q}(\theta_{g_2}) \cap \Omega_{g_1} \neq \boldsymbol{Q}$.*

If in the situation of Corollary 1 we let $g_1 = x^3 - 2$, $g_2 = x^2 + x + 1$, then it is easy to show that one of g_1 or g_2 has a zero mod p for each rational prime p. Thus we see that the hypotheses of Corollary 1 do not imply that one of g_1 or g_2 is linear, or even reducible (compare with the polynomial conjecture). For other examples see Schinzel [11].

II. We assume that we are given polynomials $h, g_1, \dots, g_l$ satisfying

$$V_p(h) \subset \bigcup_1^l V_p(g_i)$$

(i.e. the hypothesis of the polynomial conjecture). Let A be the set of integers λ_0 such that $h(x) - \lambda_0, g_1(x) - \lambda_0, \dots, g_l(x) - \lambda_0$ are all irreducible

over $\boldsymbol{Q}$. By Hilbert's irreducibility theorem Λ has asymptotic density one.

Consider the two conditions:

GH: $P'\big(\boldsymbol{Q}(\theta_{h-\lambda_0})\big) \subset \bigcup_{j=1}^{l} P'\big(\boldsymbol{Q}(\theta_{g_j-\lambda_0})\big)$ for all $\lambda_0 \in \Lambda$.

PCH: $V_p(h) \subset \bigcup_{j=1}^{l} V_p(g_j)$ for a.a.p.

Let λ_0 be any fixed value of Λ. If $p \in P'\big(\boldsymbol{Q}(\theta_{h-\lambda_0})\big)$ then $h-\lambda_0$ has a linear factor mod p and consequently $\lambda_0 \in V_p(h)$. Now, if PCH holds, then $\lambda_0 \in V_p(g_j)$ for some j, and so $p \in P'\big(\boldsymbol{Q}(\theta_{g_j-\lambda_0})\big)$. Thus PCH implies GH.

Let λ be an indeterminate, $\theta_{h-\lambda}$ a zero of $h(x)-\lambda$, and Ω_λ the composite of the splitting fields of $h-\lambda, g_1-\lambda, \ldots, g_l-\lambda$ over $\boldsymbol{Q}(\lambda)$. From Theorem 1 an idea due to Hilbert [7] enables us easily to prove

THEOREM 2. *Assume* $h, g_1, \ldots, g_l \in \boldsymbol{Z}[x]$. *Condition* GH *implies*

PH: $\bigcup_{\theta_{h-\lambda}} G\big(\Omega_\lambda/\boldsymbol{Q}(\theta_{h-\lambda})\big) \subset \bigcup_{1}^{l} \bigcup_{\theta_{g_i-\lambda}} G\big(\Omega_\lambda/\boldsymbol{Q}(\theta_{g_i-\lambda})\big)$.

Proof. From Theorem 1 we know that

$$\bigcup_{\theta_{h-\lambda_0}} G\big(\Omega_{\lambda_0}/\boldsymbol{Q}(\theta_{h-\lambda_0})\big) \subset \bigcup_{1}^{l} \bigcup_{\theta_{g_i-\lambda_0}} G\big(\Omega_{\lambda_0}/\boldsymbol{Q}(\theta_{g_i-\lambda_0})\big) \quad \text{for} \quad \lambda_0 \in \Lambda. \tag{9}$$

Let $m(x,\lambda) \in \boldsymbol{Q}[x,\lambda]$ be an irreducible normal polynomial, integral over $\boldsymbol{Q}[\lambda]$, whose splitting field over $\boldsymbol{Q}(\lambda)$ is Ω_λ. From Kummer's theorem we know that, with the exception of finitely many additional values of λ_0, the primes in Ω_λ over the prime $\lambda-\lambda_0$ in $\boldsymbol{Q}[\lambda]$ are in one-one correspondence with the irreducible factors of $m(x,\lambda_0)$. By the Hilbert irreducibility theorem, $m(x,\lambda_0)$ is irreducible for λ_0 with asymptotic density one.

From standard number theory, letting $\mathfrak{p}_{\lambda_0}$ be the single unramified prime above $\lambda-\lambda_0$, then (excluding an additional finite set of λ_0) $\Omega_\lambda/\mathfrak{p}_{\lambda_0} = \Omega_{\lambda_0}$. Therefore we obtain

$$[\Omega_{\lambda_0}:\boldsymbol{Q}] = [\Omega_\lambda:\boldsymbol{Q}(\lambda)] \quad \text{for} \quad \lambda_0 \in \Lambda', \tag{10}$$

where Λ' is a set of integers of asymptotic density one.

The group of automorphisms σ of $G\big(\Omega_\lambda/\boldsymbol{Q}(\lambda)\big)$ fixing $\mathfrak{p}_{\lambda_0}$ can be identified with the automorphisms $\bar{\sigma}$ of $G(\Omega_{\lambda_0}/\boldsymbol{Q})$ by the formula

$$\sigma(\eta)+\mathfrak{p}_{\lambda_0} = \bar{\sigma}(\eta+\mathfrak{p}_{\lambda_0}) = \bar{\sigma}(\bar{\eta}) \quad \text{for} \quad \eta \in O_{\Omega_\lambda}. \tag{11}$$

From (10) we see that for $\lambda_0 \in \Lambda'$, $G\big(\Omega_\lambda/\boldsymbol{Q}(\lambda)\big) = G(\Omega_{\lambda_0}/\boldsymbol{Q})$. From (11) it follows that $\sigma \in G\big(\Omega_\lambda/\boldsymbol{Q}(\eta)\big)$ if and only if $\bar{\sigma} \in G\big(\Omega_{\lambda_0}/\boldsymbol{Q}(\bar{\eta})\big)$ for $\eta \in O_{\Omega_\lambda}$. Thus for $\lambda_0 \in \Lambda \cap \Lambda'$ (of asymptotic density one) (9) implies PH.

For future reference we quote the following propositions which can be found in more generality in [3], while Proposition 3 can also be found in [12].

PROPOSITION 2. *If* $h(x) \in K[x]$ *and* x_1 *is any zero of* $h(x)-\lambda$, *then there is a one-one association between subfields of* $K(x_1)$ *containing* $K(\lambda)$ *and composition factors of* $h(x)$. *Namely, for* $K(\lambda) \subset M \subset K(x_1)$, $M = K\big(u(x_1)\big)$, *where* $u \in K[x]$ *and* $h = r\big(u(x)\big)$.

PROPOSITION 3. *Suppose* $f(x), g(x) \in \bar{K}[x]$ ($\bar{K}$ *a fixed algebraic closure of* K), $f\big(g(x)\big) \in K[x]$, *and the leading and constant coefficients of* $g(x)$ *are also in* K. *Then if* $\operatorname{char} K$ *does not divide degree of* f, $g(x)$ *and* $f(x)$ *are in* $K[x]$.

As a start to an investigation of the polynomial conjecture, expand each of $\theta_{h-\lambda}, \theta_{g_1-\lambda}, \ldots, \theta_{g_l-\lambda}$ at infinity. From the method of indeterminate coefficients all these expansions are of the form

$$\theta_{h-\lambda} = a_{-1}\lambda^{1/n} + a_0 + a_1\lambda^{-1/n} + \ldots,$$
$$\theta_{g_i-\lambda} = a_{-1}^{(i)}\lambda^{1/n_i} + a_0^{(i)} + a_1^{(i)}\lambda^{-1/n_i} + \ldots, \quad i = 1, \ldots, l.$$

Let N be the least common multiple of the integers $n, n_1, \ldots, n_l$, and let ζ_N be a primitive Nth root of 1. The power series expansions for $\theta_{h-\lambda}, \theta_{g_1-\lambda}, \ldots, \theta_{g_l-\lambda}$ give an embedding of Ω_λ into L_N, the field of all formal Laurent series in $\lambda^{-1/N}$ with coefficients in $\overline{\boldsymbol{Q}}$. Let σ be an operator on L_N defined by

$$a \in L_N, \quad \text{then} \quad \sigma\big(a(\lambda^{-1/N})\big) = a(\zeta_N\lambda^{-1/N}).$$

Since σ is a change of variable, it is a field automorphism of L_N, and we denote again by σ the restriction of this automorphism to Ω_λ.

COROLLARY 2. *If* $h, g_1, \ldots, g_l \in \boldsymbol{Z}[x]$ *and if* $V_p(h) \subset \bigcup_{1}^{l} V_p(g_i)$ *for a.a.p., then there exists an index* i *such that degree of* g_i *divides degree of* h.

Proof. From Theorem 2 our hypothesis implies PH. If $a \in L_N$, then $\sigma^n\big(a(\lambda^{-1/N})\big)$ equals $a(\zeta_N^n\lambda^{-1/N})$. Let m be the least integer such that a is expressible as $a = a(\lambda^{-1/m}) = a\big((\lambda^{-1/N})^{N/m}\big)$. Then $(\zeta_N^n)^{N/m} = 1$ if and only if $m \mid n$. So $\sigma^n(a) = a$ if and only if $m \mid n$. Each $\theta_{h-\lambda}$ is of the form $\theta_{h-\lambda} = \beta(\lambda^{-1/n}) = \beta\big((\lambda^{-1/N})^{N/m}\big)$. Thus $\sigma^n(\theta_{h-\lambda}) = \theta_{h-\lambda}$, and therefore σ^n must fix $\theta_{g_i-\lambda}$ for some index i. For this integer i, $n_i \mid n$.

The polynomial conjecture is trivially true if one of the $g_i(x)$ is linear, and from now on we will assume that this is not the case.

Let $\Omega_{g,\lambda} = \Omega_{g_1-\lambda} \ldots \Omega_{g_l-\lambda}$. From Proposition 2 there exist polynomials $h^*(x), v(x) \in \boldsymbol{Q}[x]$ such that

$$h = h^*(v) \quad \text{and} \quad \boldsymbol{Q}(\theta_{h-\lambda}) \cap \Omega_{g,\lambda} = \boldsymbol{Q}\big(v(\theta_{h-\lambda})\big).$$

From Lemma 1, $G\big(\Omega_{g,\lambda}/\boldsymbol{Q}(\theta_{h^*-\lambda})\big)$ is the restriction of $G\big(\Omega_\lambda/\boldsymbol{Q}(\theta_{h-\lambda})\big)$ to $\Omega_{g,\lambda}$. Therefore the relation PH yields

$$\bigcup_{\theta_{h^*-\lambda}} G\big(\Omega_{g,\lambda}/\boldsymbol{Q}(\theta_{h^*-\lambda})\big) \subset \bigcup_{1}^{l} \bigcup_{\theta_{g_i-\lambda}} G\big(\Omega_{g,\lambda}/\boldsymbol{Q}(\theta_{g_i-\lambda})\big). \tag{12}$$

If we knew that (12) implied the existence of an index i and a polynomial $r(x)\epsilon\overline{Q}[x]$ such that $g_i(r(x)) = h^*(x)$, then

$$h^*(v(x)) = g_i(r(v(x))) = h(x).$$

Therefore we would know that the polynomial conjecture is true. Since all further attempts to solve the polynomial conjecture will be based on (12) alone, we are free to assume $h^*(x) = h(x)$.

Denote the field $\Omega_{g,\lambda}\cdot\overline{Q}$ by $\Sigma_{g,\lambda}$, and the field $\Omega_{h-\lambda}\cdot\overline{Q}$ by $\Sigma_{h-\lambda}$. From (12) we deduce

$$\bigcup_{\theta_{h-\lambda}} G(\Sigma_{g,\lambda}/\overline{Q}(\theta_{h-\lambda})) \subset \bigcup_{1}^{l}\bigcup_{\theta_{g_i-\lambda}} G(\Sigma_{g,\lambda}/\overline{Q}(\theta_{g_i-\lambda})), \tag{13}$$

by considering only those elements in relation (12) which are fixed on the algebraic closure of Q in $\Omega_{g,\lambda}$.

LEMMA 3. *If $h(x)\epsilon\overline{Q}[x]$ and $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is abelian, then $h(x)$ is a cyclic polynomial.*

Proof. Since $\Sigma_{h-\lambda}$ is the splitting field of $h(x)-\lambda$ over $\overline{Q}(\lambda)$, our assumption that $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is abelian implies that $\Sigma_{h-\lambda} = \overline{Q}(\theta_{h-\lambda})$. Thus, $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is of order $n = \deg h$ and consists of powers of σ, the automorphism at infinity.

A cyclic group has exactly one subgroup of each order k dividing the order of the group. Using Proposition 2 we decompose $h(x)$ into $h_1(h_2(\ldots(h_r(x))$ where $h_1(h_2(\ldots(h_i(x))$ corresponds to the subfield of $\overline{Q}(\theta_{h-\lambda})$ of degree l_i over $\overline{Q}(\lambda)$, where l_{i+1}/l_i is a prime for $i = 1, \ldots, n-1$. Thus, $G(\Sigma_{h_i-\lambda}/\overline{Q}(\lambda))$ is cyclic of prime order the degree of h_i. But, $\Sigma_{h_i-\lambda}$ has at least one finite ramified prime over $\overline{Q}(\lambda)$. Since the inertial group of this prime is a subgroup of $G(\Sigma_{h_i-\lambda}/\overline{Q}(\lambda))$, this prime must be totally ramified. Therefore, $h_i(x)$ is a cyclic polynomial, and $h(x)$ is a composite of cyclic polynomials.

From the fact that $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is cyclic of order $n = \deg h$ we shall deduce that $h(x)$ is actually cyclic.

Let $f(x) = (g(x))^k + d$ where $g(x) = (x-b)^l + e$. We claim that $G(\Sigma_{f-\lambda}/\overline{Q}(\lambda))$ is cyclic only if $e = 0$. Changing λ to $\lambda - d$, and x to $x+b$ we assume $f(x)-\lambda = (x^l+e)^k-\lambda$. The zeros of this polynomial are

$$x_{t,s} = \zeta_l^t(\zeta_k^s\lambda^{1/k} - e)^{1/l}$$

where ζ_l, ζ_k are primitive l and kth roots of 1. If $G(\Sigma_{r-\lambda}/\overline{Q}(\lambda))$ is cyclic, then $\overline{Q}(x_{0,0})$ would contain all other zeros of $x_{t,s}$. However, letting

$\lambda^{1/k} = z$, if $(\zeta_k z - e)^{1/l}\epsilon\overline{Q}((z-e)^{1/l})$, there exist polynomials u and v such that

$$\frac{u((z-e)^{1/l})}{v((z-e)^{1/l})} = (\zeta_k z - e)^{1/l}.$$

We easily deduce in order that v is constant, u is linear, and then that $e = 0$. Applying this argument several times to the decomposition of $h(x)$ in terms of the $h_i(x)$, $i = 1, \ldots, r$, we see that $h(x)$ must be a cyclic polynomial.

We note that Lemma 3 is not true if we do not have characteristic 0. In fact, for $h(x) = X^p - X\epsilon\mathbf{Z}/(p)[x]$ we have $G(\Sigma_{h-\lambda}/\overline{\mathbf{Z}/(p)}(\lambda))$ cyclic. See [4] for a simple generalization of this.

THEOREM 3. *If $h, g_1, \ldots, g_l\epsilon\mathbf{Z}[x]$ and $V_p(h) \subset \bigcup_1^l V_p(g_i)$ for a.a.p., and if in addition, $g_1, \ldots, g_l$ are cyclic polynomials, then there exists $r(x)\epsilon\overline{Q}[x]$ and an index i such that $h(x) = g_i(r(x))$.*

Proof. From the remarks following Corollary 2, we may presume that $\theta_{h-\lambda}\epsilon\Sigma_{g,\lambda}$, and thus that $\Sigma_{h-\lambda} \subset \Sigma_{g,\lambda}$. Therefore $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is a factor group of $G(\Sigma_{g,\lambda}/\overline{Q}(\lambda))$. Since the latter is a subgroup of the direct product of the cyclic groups $G(\Sigma_{g_i-\lambda}/\overline{Q}(\lambda))$ for $i = 1, \ldots, l$, we conclude that $G(\Sigma_{h-\lambda}/\overline{Q}(\lambda))$ is abelian.

From Lemma 3 we deduce that h is a cyclic polynomial. If $h(x) = a(x-b)^n + c$, by relabeling, we may assume that N is the composite of the fields $\Sigma_{g_i-\lambda}$, $i = 1, \ldots, s$ which are ramified over $\lambda - c$. Using the remaining polynomials, let N_i $(i = 1, \ldots, r)$ be the composite of the fields $\Sigma_{g_i-\lambda}$ which have a common finite ramified prime among them. Since there are no proper fields unramified at all finite places over $\overline{Q}(\lambda)$, $N \cap (N_1 \ldots N_r) = \overline{Q}(\lambda)$. We then see inductively that

$$G(\Sigma_{g,\lambda}/\overline{Q}(\lambda)) = G(N/\overline{Q}(\lambda)) \times G(N_1/\overline{Q}(\lambda)) \times \ldots \times G(N_r/\overline{Q}(\lambda)).$$

Let k be the l.c.m. of $\deg g_1, \ldots, \deg g_s$. Then $G(N/\overline{Q}(\lambda))$ is cyclic of order k and we let τ be a generator. Similarly, let η_i $(i = 1, \ldots, \nu)$ be respectively, generators of the cyclic groups $G(N_i/\overline{Q}(\lambda))$ $(i = 1, \ldots, \nu)$. Let $\eta = (\eta_1, \ldots, \eta_\nu)$. The automorphism

$$(\tau^n, \eta)\epsilon G(\Omega_{g,\lambda}/\overline{Q}(\lambda))$$

is fixed on $\overline{Q}(\theta_{h-\lambda})$. Since η fixes none of $\theta_{g_j-\lambda}$ for $j = s+1, \ldots, l$, the hypothesis implies

$$(\tau^n, \eta)\epsilon G(\Sigma_{g,\lambda}/\overline{Q}(\theta_{g_i-\lambda}))$$

for some $i = 1, \ldots, s$. For this index i, $\tau^n \in G\left(N/\bar{\boldsymbol{Q}}(\theta_{g_i-\lambda})\right)$, and we conclude that $\deg g_i \mid \deg h$.

The remainder of this section is restricted to the case of the polynomial conjecture where $l = 1$, and we bring to bear primarily group theory to deduce consequences from relation (12) in the case $l = 1$.

THEOREM 4. *Let $h, g \in \boldsymbol{Z}[x]$, and assume that $V_p(h) \subset V_p(g)$ for a.a.p. If g is a composite of polynomials of one of the following types:*

(a) $G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(y)\right)$ *(when represented as a permutation group on the zeros of $g(x)-\lambda$) is the symmetric group or alternating group;*

(b) *g is a polynomial of prime degree;*

then there exists $r(x) \in \boldsymbol{Q}[x]$ such that $g\left(r(x)\right) = h(x)$.

Remark. See also the comments following the proof of Theorem 4.

Proof. From the condition

$$\bigcup_{\theta_{h-\lambda}} G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\right) \subset \bigcup_{\theta_{g-\lambda}} G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{g-\lambda})\right) \tag{14}$$

if $h = g_1(h_2)$ and $g = g_1(g_2)$, we may replace λ by one fixed determination of $g_1^{-1}(\lambda)$ and look only at elements fixed on $\Omega_{g_1-\lambda}$ to deduce

$$\bigcup_{\theta_{h_2-\lambda}} G\left(\Omega_{g_2-\lambda}/\boldsymbol{Q}(\theta_{h_2-\lambda})\right) \subset \bigcup_{\theta_{g_2-\lambda}} G\left(\Omega_{g_2-\lambda}/\boldsymbol{Q}(\theta_{g_2-\lambda})\right).$$

Also, if $h = h_1(h_2)$, $g = g_1(g_2)$ where h_1 and g_1 are indecomposable, an argument similar to that leading to formula (12) implies that (14) is true with h and g replaced respectively by h_1 and g_1. To obtain this formula just restrict elements of $G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\lambda)\right)$ to $\Omega_{g_1-\lambda}$. Thus, if (14) implies our theorem is true under conditions (a) and (b), then the theorem is true in general by induction.

We note also that from Corollary 2, $\deg g \mid \deg h$. But, $\theta_{h-\lambda}$ is expressible as a rational function of the $\theta_{g-\lambda}$, which are in turn Laurent series in $\lambda^{-1/n'}$ where $\deg g = n'$. Therefore $\deg h \mid \deg g$, and so $\deg h = \deg g$.

For the remainder of this argument we will let

$$H = G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\right), \quad G^* = G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{g-\lambda})\right).$$

We disregard the fact that we have not distinguished between the various conjugates of H and G^*. If $H = G^*$, then the fundamental theorem of galois theory implies $\boldsymbol{Q}(\theta_{h-\lambda}) = \boldsymbol{Q}(\theta_{g-\lambda})$, and therefore that $g(ax+b) = h(x)$ for some $a, b \in \boldsymbol{Q}$. If H were a transitive group when represented on the letters $\theta_{g-\lambda}$ then we could conclude from Lemma 2 that there exists $\tau \in H$ which moves each of the $\theta_{g-\lambda}$. For if τ did not exist, the union of the stabilizers of the $\theta_{g-\lambda}$ in H would be all of H. However, this would contradict the fact that the union of the conjugates of a proper subgroup cannot cover the group. The existence of such a $\tau \in H$ would in turn contradict (14). Therefore H must be *intransitive* on the zeros of $g(x)-\lambda$.

CASE (a). *$G = G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\lambda)\right)$ is the alternating or symmetric group of degree n.*

An intransitive permutation group of degree n on the letters $x_1, \ldots, x_n$ has order dividing $(s_1!)(s_2!)\ldots(s_r!)$ where the letters $x_1, \ldots, x_n$ are divided into r transitivity classes of which the ith contains s_i elements. If the order of H were as large as $(n-1)!$, then G would be of order $n!$ and therefore the symmetric group. Thus H (being an intransitive group) would have exactly one of the letters fixed, and so $H = G^*$. Thus, we may assume the order of H is $\leqslant 2!(n-2)!$. But, since G is the alternating or symmetric group of degree n, the order of H is $\geqslant (n-1)!/2$. Thus, we are done if $n \geqslant 6$. Case (b) handles $n = 5$, and $n = 2, 3, 4$ are trivial.

CASE (b). *$\deg g$ is a prime.*

From Proposition 4 (Section III) the transitivity classes of H on the letters $\theta_{g-\lambda}$ are in one-one correspondence with the irreducible factors of $h(x)-g(y)$ over $\boldsymbol{Q}$. Since H is intransitive on the $\theta_{g-\lambda}$, $h(x)-g(y)$ must be reducible. From [12], since $\deg h = \deg g = \text{prime}$, $g(ax+b) = h(x)$ for some $a, b \in \boldsymbol{Q}$ unless both g and h are cyclic. However, it is easy to see that $\Omega_{h-\lambda} \subset \Omega_{g-\lambda}$ implies that in this case also there exist $a, b \in \boldsymbol{Q}$ such that $g(ax+b) = h(x)$.

Comments. Using some group theory and a little geometry, Theorem 4 can be strengthened to include a category:

(c) polynomials of 'low' degree. The author has actually carried this out where the degree of g is 4, 6, 8, or 9 (not covered by category (b)). The apropos geometry is well-known (see [13], especially Chapters 4 and 10). However, in this case we can give a very simple specialized treatment which is meant to be a review that may be referred to in subsequent work. Before we start we note one technical fact needed to incorporate these arguments into the induction of Theorem 4. The use of Riemann surfaces requires us to use formula (13) in the case $l = 1$, instead of formula (14). However, since Case (b) of Theorem 4 requires that our polynomials be considered over $\boldsymbol{Q}$, it is necessary to know that all decompositions of a polynomial over $\bar{\boldsymbol{Q}}$ correspond in a one-one way to decompositions of the same polynomial over $\bar{\boldsymbol{Q}}$, and in fact; if $h(x)$ and $g(x)$ are a *composite pair* over $\bar{\boldsymbol{Q}}$, then they are a *composite pair* over $\boldsymbol{Q}$, unless $h(x)$ has a decomposition containing some cyclic polynomials. This latter possibility is already handled by Case (b) of Theorem 4, and the other statements are easy consequences of Proposition 3.

Let $g(x) \in \bar{\boldsymbol{Q}}[x]$. We describe a set of generators for $G\left(\Sigma_{g-\lambda}/\bar{\boldsymbol{Q}}(\lambda)\right)$. A *finite branch point* is a complex number λ_0 for which $g'(x)$ (the deri-

vative of $g(x)$) and $g(x)-\lambda_0$ have a zero in common, or equivalently $g(x)-\lambda_0$ has a double zero at least. Suppose

$$g(x)-\lambda_0 = a\prod_1^t (x-x_j)^{s_j}.$$

Then the expansion of the zeros of $g(x)-\lambda$ about λ_0 yields a set of expansions of the form:

$$x_1+a_{1,1}\zeta_{s_1}^r(\lambda-\lambda_0)^{1/s_1}+a_{1,2}\zeta_{s_1}^{2r}(\lambda-\lambda_0)^{2/s_1}+\ldots, \quad r=0,1,\ldots,s_1-1,$$
$$x_2+a_{2,1}\zeta_{s_2}^r(\lambda-\lambda_0)^{1/s_2}+a_{2,2}\zeta_{s_2}^{2r}(\lambda-\lambda_0)^{2/s_2}+\ldots, \quad r=0,1,\ldots,s_2-1,$$

... etc. where ζ_{s_i} is a primitive s_ith root of 1. As with the expansion at infinity (see remarks preceding Corollary 2) we may embed $\Sigma_{h-\lambda}$ in L_N the field of formal Laurent series in $(\lambda-\lambda_0)^{1/N}$ where N is the least common multiple of $s_1,\ldots,s_t$. Let τ_{λ_0} be the operator on L_N defined by

$$a\in L_N, \quad \text{then} \quad \tau_{\lambda_0}\big(a(\lambda-\lambda_0)^{1/N}\big) = a\big(\zeta_N(\lambda-\lambda_0)^{1/N}\big).$$

The restriction of τ_{λ_0} to $\Sigma_{g-\lambda}$ is an element of $G\big(\Sigma_{g-\lambda}/\bar{\boldsymbol{Q}}(\lambda)\big)$, and is in fact a generator for the inertial group of some valuation of $\Sigma_{g-\lambda}$ lying over λ_0. We say that τ_{λ_0} has index $\sum_{i=1}^t (s_i-1)$. The two fundamental facts are:

(a)' $\sum_{\lambda_0 \text{ finite}} \operatorname{ind}\tau_{\lambda_0} = n-1$ (easy to see);

(b)' the elements τ_{λ_0} generate $G\big(\Sigma_{g-\lambda}/\bar{\boldsymbol{Q}}(\lambda)\big)$ (not so easy).

If we do this also for $\Sigma_{h-\lambda}$, then the same elements τ_{λ_0} describe actions on the zeros of $h(x)-\lambda$, using $\Sigma_{h-\lambda}\subset\Sigma_{g-\lambda}$. If the degree of g is low we can see by inspection of the expansions that τ_{λ_0} induces similar actions on the $\theta_{h-\lambda}$ and $\theta_{g-\lambda}$. For low degrees we can therefore use formula (13) to combinatorially draw the conclusion of Theorem 4. Some techniques extending these will be used in a subsequent paper.

THEOREM 5. *Assume* $h, g\in\boldsymbol{Z}[x]$. *Then* $V_p(h)=V_p(g)$ *for a.a.p. implies: each decomposition of* $h(x)$ *into primely composite polynomials has a corresponding decomposition of* $g(x)$ *where the degrees of the prime components* $h(x)$ *are the same in the given order as the degrees of the prime components in the respective decomposition of* $g(x)$.

Proof. From PH (see Theorem 2) we conclude that

$$\bigcup_{\theta_{h-\lambda}} G\big(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\big) = \bigcup_{\theta_{g-\lambda}} G\big(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{g-\lambda})\big)$$

and $\Omega_{g-\lambda}=\Omega_{h-\lambda}$. From Proposition 2 we need only show that to each subfield of $\boldsymbol{Q}(\theta_{h-\lambda})$ containing $\boldsymbol{Q}(\lambda)$ there corresponds a subfield of $\boldsymbol{Q}(\theta_{g-\lambda})$ of the same degree over $\boldsymbol{Q}(\lambda)$.

Let M be a subfield of $\boldsymbol{Q}(\theta_{h-\lambda})$ containing $\boldsymbol{Q}(\lambda)$. From Proposition 2, $M=\boldsymbol{Q}(\theta_{h^*-\lambda})$ where $h=h^*\big(r(x)\big)$. The restriction of the elements of $G\big(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\big)$ to $\Omega_{h^*-\lambda}$ yields $G\big(\Omega_{h^*-\lambda}/\boldsymbol{Q}(\theta_{h^*-\lambda})\big)$.

Lemma 1 implies that the restriction of elements of $G\big(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{g-\lambda})\big)$ to $\Omega_{h^*-\lambda}$ yields $G\big(\Omega_{h^*-\lambda}/\boldsymbol{Q}(\theta_{g^*-\lambda})\big)$ where $\boldsymbol{Q}(\theta_{g-\lambda})\cap\Omega_{h^*-\lambda}=\boldsymbol{Q}(\theta_{g^*-\lambda})$.

We obtain

$$\bigcup_{\theta_{h^*-\lambda}} G\big(\Omega_{h^*-\lambda}/\boldsymbol{Q}(\theta_{h^*-\lambda})\big) = \bigcup_{\theta_{g^*-\lambda}} G\big(\Omega_{h^*-\lambda}/\boldsymbol{Q}(\theta_{g^*-\lambda})\big).$$

Repeating the argument of the second paragraph of the proof of Theorem 4, we conclude that $\Omega_{h^*-\lambda}=\Omega_{g^*-\lambda}$ and $\deg h^*=\deg g^*$.

III. Schinzel [10] has shown that if $f(x,y)$ in $\boldsymbol{Z}[x,y]$ is irreducible, then there exists an arithmetic progression P of integers such that $f(x_0,y)$ is an irreducible polynomial in one variable for $x_0\in P$. We will show that for suitable conditions on $f(x,y)$ we may find such an arithmetic progression that has the additional property that its modulus is a prime number. More precisely:

THEOREM 6. *Let* $f(x,y)\in\boldsymbol{Z}[x,y]$ *have a totally ramified Puiseux expansion over some place on the x-sphere. Then there exists an arithmetic progression* P *with prime modulus such that* $x_0\in P$ *implies* $f(x_0,y)$ *irreducible.*

By a totally ramified Puiseux expansion about a we mean that $y=\sum_N^\infty a_i(x-a)^{i/n}$ is an expansion for $f(x,y)$, where $\deg_y f=n$ and the denominator n is essential in the expansion. In particular we note that $f(x)-g(y)$ has a totally ramified Puiseux expansion at ∞ if and only if $(\deg f,\deg g)=1$. The existence of such a Puiseux expansion automatically implies the irreducibility of $f(x,y)$ because a Puiseux expansion for an irreducible polynomial $\varphi(x,y)$ has ramification less than or equal to $\deg_y\varphi$.

Proof of Theorem 6. Dörge [3] (see also Lang [8]) showed how to reduce the question of a polynomial remaining irreducible under rational integer specialization of one of its variables to a question about integer solutions to a polynomial in two variables. It will be necessary to investigate his method in detail to obtain our result.

If $f(x,y)$ is irreducible, then we write

$$f(x,y)=\Big[\prod_1^n (y-y_i)\Big]h(x)$$

where $h(x)$ is a rational function. For each partition of the integers $1,2,\ldots,n$ into two non-empty disjoint sets A and B, we decompose

$$f(x,y)=G_A\cdot G_B \quad \text{where} \quad G_A=h(x)\prod_{i\in A}(y-y_i).$$

Then one of the coefficients of G_A (as a polynomial in y) is not a rational function of x over $\boldsymbol{Q}$. In fact, in the case where $f(x, y)$ has a totally ramified expansion over the place a, $\prod_{i\in A} y_i$ is not a power series in $(x-a)$ (but rather in $(x-a)^{1/r}$ for some integer $r>1$). Let $\prod_{i\in A} y_i = z_A$. It is important to notice that the conjugates of z_A can also not be expressed as a power series in $(x-a)$. If x_0 is an integer for which $f(x_0, y)$ is reducible (assume $h(x_0) \neq 0$), there exists a set A such that $z_A(x_0) \in \boldsymbol{Q}$. For simplicity, we notice that we may multiply each function $z_A(x)$ by an element of $\boldsymbol{Z}[x]$, so that for each A, $z_A(x)$ is integral over $\boldsymbol{Z}[x]$. Therefore if $z_A(x_0) \in \boldsymbol{Q}$, then $z_A(x_0) \in Z$.

Let $f_A(x, Z)$ be the irreducible polynomial in $\boldsymbol{Z}[x, Z]$ having z_A as a zero. We must now show that there exists an arithmetic progression P with prime modulus, such that $f_A(x_0, Z) = 0$ has no solution in $\boldsymbol{Z}$ for any A, if $x_0 \in P$.

Let Ω_{f_A} be the splitting field (over $\boldsymbol{Q}(x)$) of $f_A(x, Z)$, and let Ω_x be the composite of the fields Ω_{f_A}. By exactly the same methods used to prove Theorem 2, we see that if such an arithmetic progression did not exist, then we would have

$$\bigcup_A \bigcup_{\substack{z_A^{(i)} \text{ runs over} \\ \text{conjugates of } z_A}} G\left(\Omega_x/\boldsymbol{Q}(z_A^{(i)}, x)\right) = G\left(\Omega_x/\boldsymbol{Q}(x)\right). \tag{15}$$

The automorphism of Ω_x described by sending $(x-a)^{1/n} \xrightarrow{a} \zeta_n(x-a)^{1/n}$ (ζ_n a primitive nth root of 1) is easily seen to be an element of the right side of (15), but not the left. With this contradiction the theorem is proved.

Note. With somewhat the same analysis as above it is possible to show that the conclusion of Theorem 6 remains true for irreducible polynomials $f(x)-g(y) \in \boldsymbol{Z}[x, y]$ if $\deg g \nmid \deg f$. However, even in the case where $\deg f = \deg g$ our method does not obtain the corresponding result (unless, of course, the degrees are very small).

The simplest case of the polynomial conjecture which has not been resolved is that described by the hypothesis; $h(x), g(x) \in \boldsymbol{Z}[x]$ have the same value sets mod p for a.a.p. Although Theorems 4 and 5 give reasonable information, they are far short of the desired conclusion that there exists $a, b \in \boldsymbol{Q}$ such that $g(ax+b) = h(x)$. We will now give two examples that show that neither group theory alone, nor formal power series manipulations alone can obtain this result.

The hypothesis $V_p(h) = V_p(g)$ for a.a.p. does imply

$$\Omega_{h-\lambda} = \Omega_{g-\lambda}, \tag{16}$$

$$\bigcup_{\theta_{h-\lambda}} G\left(\Omega_{h-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\right) = \bigcup_{\theta_{g-\lambda}} G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{g-\lambda})\right), \tag{17}$$

(18) there exists $\sigma \in G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\lambda)\right)$ such that σ represented as acting on either the $\theta_{h-\lambda}$ or $\theta_{g-\lambda}$ is an n-cycle.

Example 1. Professor J. McLaughlin gave us the following example of a group G which may be represented in inequivalent ways on two different sets of letters $\{x_1, \ldots, x_n\}$, $\{y_1, \ldots, y_n\}$ such that G is primitive on both sets of letters, $\bigcup_1^n G_{x_i} = \bigcup_1^n G_{y_i}$ (where G_{x_i} denotes the stabilizing group of x_i), and there is an element of G which is an n-cycle on both sets of letters. The group $\boldsymbol{P}(2, p^k)$ is doubly transitive (and thus primitive) on both points $(\{x_1, \ldots, x_n\})$ and lines $(\{y_1, \ldots, y_n\})$. It is very easy to see that if an element of $\boldsymbol{P}(2, p^k)$ fixes some point, then it must also fix some line, and conversely.

If we let $\alpha \in \boldsymbol{F}_{p^{3k}}$ (finite field with p^{3k} elements) be a primitive generator of the cyclic group of non-zero elements, then $1, \alpha, \alpha^2$ is also a basis over $\boldsymbol{F}_{p^k}$ for $\boldsymbol{F}_{p^{3k}}$. Multiplication by α on $\boldsymbol{F}_{p^{3k}}$ induces a projective transformation T such that $T(\alpha^r) = \alpha^{r+1}$. Thus T is a cyclic transformation of the points of the vector space $\boldsymbol{F}_{p^{3k}}$ over $\boldsymbol{F}_{p^k}$. To show that T is also a cyclic transformation on the lines of projective space, we use a trick related to us by Richard Misare. If we look at the affine space underlying the projective space, and we denote by L any non-trivial linear functional such that $L(1) \neq 0$, then the functional $L_\beta(x) = L(\beta x)$ has kernel $\beta^{-1}(\ker L)$. A linear functional is described by its kernel and the value at one point of the kernel. Since the linear functionals of a finite field are all of the form L_β, we see that the planes of this vector space (through the origin) are cyclically permuted among each other by T. Therefore the lines of the induced projective space are also cyclically permuted by T.

We note a couple of facts related to Example 1. If $g(x) \in \boldsymbol{Q}[x]$, then the subgroups of $G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\lambda)\right)$ containing $G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\theta_{h-\lambda})\right)$ are (by the fundamental theorem of galois theory) in one-one correspondence with fields between $\boldsymbol{Q}(\theta_{h-\lambda})$ and $\boldsymbol{Q}(\lambda)$. By Proposition 2 the latter are in one-one correspondence with the composition factors of $g(x)$. Thus, by well-known group theory, $G\left(\Omega_{g-\lambda}/\boldsymbol{Q}(\lambda)\right)$ is a primitive group (on the letters $\theta_{g-\lambda}$) if and only if $g(x)$ is indecomposable. The argument of the proof of Theorem 4 shows that we may presume this with no loss.

We make now one last conjecture (our third) which, combined with Proposition 4, implies that the situation of Example 1 cannot be a counterexample to the polynomial conjecture.

Conjecture 3. *Suppose $h(x), g(x) \in \boldsymbol{Q}[x]$ are of the same degree n. Let*

$$h(x)-g(y) = \prod_{i=1}^{r} \varphi_i(x, y)$$

be the factorization of $h(x)-g(y)$ into irreducible factors over $\boldsymbol{Q}$. Then, if none of the φ_i are linear, one of the numbers $(n, \deg\varphi_i)$, $i = 1, \ldots, r$, is different from 1.

Conjecture 3 has been made as weak as possible because of our previous experience with conjectures about the factorization of polynomials in two variables.

PROPOSITION 4. *Let $h(x), g(x) \in \boldsymbol{Q}[x]$. In the notation of Section II let $\Omega_\lambda = \Omega_{h-\lambda} \cdot \Omega_{g-\lambda}$. Then the transitivity classes of the quantities $\theta_{g-\lambda}$ when acted on by the group $G\big(\Omega_\lambda/\boldsymbol{Q}(\theta_{h-\lambda})\big)$ are in one-one correspondence with the irreducible factors (over $\boldsymbol{Q}$) of $h(x)-g(y)$.*

Proof. The irreducible factors of $h(\theta_{h-\lambda})-g(y)$ are the minimal polynomials for the quantities $\theta_{g-\lambda}$ over $\boldsymbol{Q}(\theta_{h-\lambda})$. The rest follows by galois theory.

If in Example 1 we let $p^k = q$, then the q^2+q+1 lines fall into two transitivity classes under the action of G_{x_1} (i.e. the $q+1$ lines through x_1, are in one transitivity class, the remainder in another). However, since $(q+1, q^2+q+1) = (q^2, q^2+q+1) = 1$, we would obtain a contradiction to Conjecture 3.

EXAMPLE 2. We now show that (16) is not strong enough to imply the conclusion of the polynomial conjecture. Let $h(x) = (x^2-1)^2$. The zeros of $h(x)-\lambda$ are

$$x_1 = \sqrt{1+\sqrt{\lambda}}, \quad x_2 = -\sqrt{1+\sqrt{\lambda}}, \quad x_3 = \sqrt{1-\sqrt{\lambda}}, \quad x_4 = -\sqrt{1-\sqrt{\lambda}}.$$

We list the elements of $G\big(\boldsymbol{Q}(x_1, x_2, x_3, x_4)/\boldsymbol{Q}(\lambda)\big)$ as permutations:

$$\sigma_1 = 1, \quad \sigma_2 = (x_1x_2), \quad \sigma_3 = (x_3x_4), \quad \sigma_4 = (x_1x_2)(x_3x_4),$$
$$\sigma_5 = (x_1x_3)(x_2x_4), \quad \sigma_6 = (x_1x_4)(x_2x_3), \quad \sigma_7 = (x_1x_4)(x_2x_3),$$
$$\sigma_8 = (x_1x_3)(x_2x_4).$$

By applying the σ_i's to the element x_1+x_3, we find its conjugates to be x_1+x_4, x_2+x_4, x_2+x_3, and so x_1+x_3 is of degree 4. Since x_1+x_3 is integral over $\boldsymbol{Q}[\lambda]$ and it has an expansion at infinity of the form $a_{-1}\lambda^{1/4}+a_0+a_1\lambda^{-1/4}+\ldots$, it is easy to see that x_1+x_3 is a zero of a polynomial of form $g(x)-\lambda$. In fact, $g(x)$ turns out to be $\frac{1}{4}x^4-x^2$. Clearly $g(x)$ and $h(x)$ are not a composite pair. Since $(x_1+x_4)-(x_2+x_3) = 2x_1$, and $(x_2+x_3)+(x_1+x_3) = 2x_3$, we see that $\Omega_{h-\lambda} = \Omega_{g-\lambda}$.

More generally, we state without proof the very simple

LEMMA 4. *If $h(x) \in \boldsymbol{Q}[x]$, and $\alpha \in \Omega_{h-\lambda}$ has the properties*

(T_1) *α is integral over $\boldsymbol{Q}[\lambda]$,*

(T_2) *α is of degree $n = \deg h$ over $\boldsymbol{Q}[\lambda]$,*

(T_3) *α has an expansion at infinity of form $a_{-1}\lambda^{1/n}+a_0+a_1\lambda^{1/n}+\ldots$ where $a_{-1} \neq 0$,*

then there exists $g(x) \in \boldsymbol{Q}[x]$ such that $g(\alpha) = \lambda$.

Note. We do not yet know if properties (T_1), (T_2), and (T_3) imply that α is a linear combination over $\bar{\boldsymbol{Q}}$ of the quantities $\theta_{n-\lambda}$, but if this were so it would be very helpful in solving the polynomial conjecture.

Quadratic polynomials. We finish with the statements of some combinatorial results that we believe give the full story on the polynomial conjecture when all the polynomials involved are of degree 2. We add that a similar result is true when all the polynomials are cyclic of the same prime degree. However, when the degrees are not prime, the analysis might run into insurmountable difficulties because of the occurrence of linear equations over non-integral domains.

We remark that Hecke [6] (Satz 147) has a very clever proof of Corollary A using the zeta function. However, a generalization of that fact is needed here, so we have included a straightforward proof of Lemma A whose extension to Lemma B is obvious.

Let I be the multiplicative group of non-zero integers modulo the non-zero square integers. Let $\{-1, 1\}$ denote the multiplicative group of two elements.

LEMMA A. *Let $b(1), \ldots, b(n)$ be distinct elements of I. Let $q_1, \ldots, q_s$ be the set of primes that appear in at least one of the $b(i)$, $i = 1, \ldots, n$. There exists a homomorphism $\Phi\colon I \to \{-1, 1\}$ such that $\Phi(p) = 1$ if p is a prime not among $q_1, \ldots, q_s$, and $\Phi\big(b(i)\big) = -1$ for $i = 1, \ldots, n$, if and only if there exists no product consisting of an odd number of distinct $b(i)$'s such that*

$$\prod_{j=1}^{2l+1} b(i_j) \equiv 1.$$

Proof. Consider the following set of linear equations with coefficients in $\boldsymbol{F}_2$.

$$\text{(a)} \qquad \sum_{j=1}^{s} a_i(j)x(j) = 1 \quad \text{for} \quad i = 1, \ldots, n,$$

where

$$a_i(j) = \begin{cases} 0 & \text{if } q_j \text{ does not appear in } b(i), \\ 1 & \text{if } q_j \text{ does appear in } b(i). \end{cases}$$

Let $\Phi(q_j) = (-1)^{x(j)}$. If there exists a solution vector $\big(x(1), \ldots, x(s)\big)$ to the equations (a), then

$$\Phi\big(b(i)\big) = (-1)^{s(i)} = -1 \quad \text{where} \quad s(i) = \sum a_i(j)x(j).$$

Conversely, if the desired Φ of the lemma exists, there is a solution vector $\big(x(1), \ldots, x(s)\big) \in \boldsymbol{F}_2^s$. A solution vector for (a) exists if and only if

$$\operatorname{rank}\Big[a_i(j)\Big] = \operatorname{rank}\Big[a_i(j)\,\Big|\,\Big].$$

If there exists a relation over $\boldsymbol{F}_2$ among t rows of $|a_i(j)|$ (say the rows $k_1, \ldots, k_t$), then we have equality of the two ranks only if t is even. The relation is equivalent to $b(k_1) \ldots b(k_t) \equiv 1$.

COROLLARY A. *Let $b(1), \ldots, b(n)$ be a set of distinct square-free integers. There exists an arithmetic progression A of primes p such that $b(i)$, $i = 1, \ldots, n$, is a quadratic non-residue* mod p *if and only if there exists no product of an odd number of distinct $b(i)$'s which is a square.*

Proof. If $\prod_{j=1}^{2l+1} b(i_j)$ is a square, then for all primes different from $q_1, \ldots, q_s$ (set of primes appearing in the $b(i)$'s, $i = 1, \ldots, n$)

$$\left(\frac{b(i_j)}{p}\right) = -1 \quad \text{implies} \quad \left(\frac{\prod_{j=1}^{2l+1} b(i_j)}{p}\right) = -1.$$

This is a contradiction.

In the other direction, if there exists no product of an odd number of distinct $b(i)$'s which is a square, Lemma A implies the existence of $\Phi\colon I \to \{-1, 1\}$ such that $\Phi\big(b(i)\big) = -1$ for $i = 1, \ldots, n$. If we can find an arithmetic progression A of primes p such that $\left(\frac{q_i}{p}\right) = \Phi(q_i)$ for $j = 1, \ldots, s$, then we would have $\left(\frac{b(i)}{p}\right) = -1$ for $i = 1, \ldots, n$. Finding A is an elementary exercise.

LEMMA B. (Extension of Lemma A.) *Let $B(1) = \{b(1), \ldots, b(n_1)\}$, $B(2) = \{b(n_1+1), \ldots, b(n_2)\}, \ldots, B(k) = \{b(n_{k-1}+1), \ldots, b(n_k)\}$ be disjoint sets of elements of I. There exists a homomorphism $\Phi\colon I \to \{-1, 1\}$ such that*

(c) $$\Phi\big(b(1)\big) = \Phi\big(b(2)\big) = \ldots = \Phi\big(b(n_1)\big) = -1,$$

(d) $$\Phi\big(b(n_i+1)\big) = \Phi\big(b(n_i+2)\big) = \ldots = \Phi\big(b(n_{i+1})\big) \quad \text{for} \quad i = 1, \ldots, k-1$$

if and only if there exists a subcollection $B(1), B(r_1), \ldots, B(r_t)$ with $2 \leqslant r_1 < \ldots < r_t \leqslant k$ such that when a product satisfies

(e) $$\prod_{j=1}^{m} b(i_j) \equiv 1 \ (\text{where } b(i_j) \text{ are distinct})$$

then the total number of $b(i_j)$'s, $j = 1, \ldots, m$, in the union of $B(1), B(r_1), \ldots, B(r_t)$ is even.

Proof. Analogous to the proof of Lemma A.

If $h, g_1, \ldots, g_l$ are quadratic polynomials in $\boldsymbol{Z}[x]$, then we may assume $h = ax^2 + c$, $g_i(x) = a(i)x^2 + c(i)$, $i = 1, \ldots, l$, with $a, a(1), \ldots, a(l)$ all square free. In this normalized form some of the resulting

polynomials may not have integer coefficients. In this case, multiply all polynomials by some one constant to put them back in $\boldsymbol{Z}[x]$. This will change any relation between their value sets for at most finitely many primes.

THEOREM A. *Let $h, g_1, \ldots, g_l$ be quadratic polynomials such that $V_p(h) \subset \bigcup_1^l V_p(g_i)$ for a.a.p. Assume for $i = 1, \ldots, n_1$ that $c(i) = c$, and for $i > n_1$ further divide up the $c(i)$'s into classes such that $c(n_1+1) = \ldots = c(n_2)$, $c(n_2+1) = \ldots = c(n_3), \ldots, c(n_{k-1}+1) = \ldots = c(n_k)$. Let $b(i) = a \cdot a(i)$, $i = 1, \ldots, l$ and $B(j) = \{b(n_{j-1}+1), \ldots, b(n_j)\}$ for $j = 1, \ldots, k$.*

Then we conclude that for each subset of indices $\{r_1, \ldots, r_t\}$ with $2 \leqslant r_1 < \ldots < r_t \leqslant k$ there exists some product of distinct $b(i)$'s, $\prod_{j=1}^{m} b(i_j) \equiv 1$ mod *squares such that the total number of $b(i)$'s in the product that are in the union of $B(1), B(r_1), \ldots, B(r_t)$ is odd.*

Proof. With no loss we may assume that each $B(i)$ consists of distinct elements. Assume there exists a subset of indices $(r_1, \ldots, r_t)$ such that for every product, $\prod_{j=1}^{m} b(i_j) \equiv 1$ mod squares, the total number of $b(i)$'s in the product that are also in one of $B(1), B(r_1), \ldots, B(r_t)$ is even. We shall show that there exists an integer λ and an arithmetic progression A of primes p such that $h(x) - \lambda \equiv 0 \bmod p$, $p \in A$, has a solution, but $g_i(x) - \lambda \equiv 0 \bmod p$ has no solution for $i = 1, \ldots, l$. Since this would contradict the hypothesis, the conclusion of Theorem A must hold.

Let $q_1, \ldots, q_s$ be the primes which appear in $b_1, \ldots, b_l$ (including without loss $q_1 = -1$, $q_2 = 1$). Let Φ be the homomorphism given by Lemma B such that

$$\Phi\big(b(1)\big) = \ldots = \Phi\big(b(n_1)\big) = -1,$$
$$\Phi\big(b(n_i+1)\big) = \ldots = \Phi\big(b(n_{i+1})\big), \quad i = 1, \ldots, k-1.$$

In a manner similar to that of Corollary A we can find an arithmetic progression of primes p (call this A^*) such that $p \equiv x^* \bmod 8q_3 \ldots q_s$ for some integer x^*, and

$$\left(\frac{b(1)}{p}\right) = \ldots = \left(\frac{b(n_1)}{p}\right) = -1,$$
$$\left(\frac{b(n_i+1)}{p}\right) = \ldots = \left(\frac{b(n_{i+1})}{p}\right) \quad \text{for} \quad i = 1, \ldots, k-1.$$

Let $p_1, \ldots, p_k$ be distinct primes larger than either $|a \cdot 8 \cdot q_3 \ldots q_s|$ or $\max_{i,j} |c(n_i) - c(n_j)|$. By the Chinese remainder theorem there exists an integer λ such that $c(n_i) - \lambda \equiv p_i \bmod p_i^2$. Note that for $i \neq j$, $p_j \nmid \big(c(n_i) - \lambda\big)$ because $p_j \nmid \big(c(n_i) - c(n_j)\big)$.

Define an arithmetic progression of primes A^{**} by the following set of linear equations:

(f) $$p \equiv x^* \bmod \left[8(q_3 \dots q_s)(c(n_1)-\lambda/p_1)\dots(c(n_k)-\lambda/p_k)\right],$$

(g) $$p \equiv m_i \bmod p_i \quad \text{for} \quad i = 1, \dots, k,$$

where m_i is chosen so that

(h) $$-1 = \left(\frac{a(n_i)}{p}\right)\left(\frac{c(n_i)-\lambda}{p}\right) = \left(\frac{a(n_i)}{p}\right)\left(\frac{c(n_i)-\lambda/p_i}{p}\right)\left(\frac{p_i}{p}\right)$$
$$= \left(\frac{m_i}{p_i}\right)(-1)^{\frac{p-1}{2}\cdot\frac{p_i-1}{2}}\left(\frac{a(n_i)}{p}\right)\left(\frac{c(n_i)-\lambda/p_i}{p}\right).$$

For p satisfying (f) the values of $\left(\frac{a(n_i)}{p}\right)$ and $\left(\frac{c(n_i)-\lambda/p_i}{p}\right)$ and $(-1)^{(p-1)/2}$ are determined by that congruence alone. Since

$$\left(\frac{a}{p}\right)\left(\frac{a(i)}{p}\right) = \left(\frac{b(i)}{p}\right) = -1 \quad \text{for} \quad i = 1, \dots, l \text{ and } p \in A^{**},$$

we conclude that

$$\left(\frac{a}{p}\right)\left(\frac{c-\lambda}{p}\right) = 1, \quad \text{and} \quad \left(\frac{a(i)}{p}\right)\left(\frac{c(i)-\lambda}{p}\right) = -1 \quad \text{for} \quad i = 1, \dots, l.$$

Let $A = A^{**}$. Then for primes $p \in A$, $h(x)-\lambda \equiv 0 \bmod p$ has a solution although $g_i(x)-\lambda \equiv 0 \bmod p$ has no solution for $i = 1, \dots, l$. From the Dirichlet density theorem there exist infinitely many primes in the arithmetic progression A. This contradicts our assumption that $V_p(h) \subset \bigcup_1^l V_p(g_i)$ for a.a.p.

Clearly the criterion of Theorem A to test for the hypothesis of the polynomial conjecture is one which may be verified in a finite number of steps. Of course, Theorem A has as a particular corollary that the polynomial conjecture is true when all the polynomials involved are quadratic. This was also a consequence of Theorem 3.

References

[1] J. Ax, *Decision procedures for finite fields*, Ann. of Math., to appear.

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

[3] K. Dörge, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*, Math. Ann. 96 (1927), pp. 176-182.

[4] a. M. Fried and R. MacRae, *On the invariance of chains of fields*, Illinois J. Math., to appear.

b. *On curves with separated variables*, Math. Ann., to appear.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, teil I und II, Physica-Verlag, 1965.

[6] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923.

[7] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Functionen, mit ganzzahligen Koeffizienten*, Journal f. Reine und Angew. Math. 110 (1892), pp. 104-129.

[8] S. Lang, *Diophantine Geometry*, Interscience Tracts in Pure and Applied Mathematics, New York 1964.

[9] C. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials*, Acta Arith. 12(1967), pp. 289-299.

[10] A. Schinzel, *On Hilbert's Irreducibility Theorem*, Ann. Polon. Math. 16(1965), pp. 333-340.

[11] — *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), pp. 333-344.

[12] — *Reducibility of polynomials of the form $f(x)-g(y)$*, Colloq. Math. 18 (1967), pp. 213-218.

[13] G. Springer, *Introduction to Riemann Surfaces*, Addison-Wesley Publishing Co., 1957.

[14] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), pp. 497-508.

THE INSTITUTE FOR ADVANCED STUDY
Princeton, New Jersey

Reçu par la Rédaction le 11. 1. 1968