This dissertation has been
microfilmed exactly as received 67-17,760

FRIED, Michael David, 1941-
VALUE SETS OF POLYNOMIALS.

The University of Michigan, Ph.D., 1967
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan

VALUE SETS OF POLYNOMIALS

by

Michael David Fried

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in the
University of Michigan
1967

Doctoral Committee:

Professor Donald J. Lewis, Chairman
Associate Professor Douglas E. Dickson
Professor William J. LeVeque
Professor Robert R. Lewis
Assistant Professor Robert R. MacRae

Abstract

Let $h(x) \in \mathbb{Z}[x]$ (the polynomial ring with coefficients in $\mathbb{Z}$) . For each rational prime p , we denote by $V_p(h)$ those cosets mod p taken on by h .

In this work, we will attempt to answer questions related to the determination of $h(x)$ by knowledge alone of $V_p(h)$ for a.a.p. (i.e. for all but a finite number of primes p). Primarily, we devote our attention to:

The Polynomial Conjecture - Let $h(x)$, $g_1(x),\cdots,g_\ell(x) \in \mathbb{Z}[x]$, and assume that $V_p(h) \subset \bigcup_{i=1}^{\ell} V_p(g_i)$ for a.a.p. Then there exists an index i , and a polynomial $r(x) \in \overline{\mathbb{Q}}[x]$ (where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$) such that $h(x) = g_i(r(x))$.

The polynomial conjecture has not been completely resolved, but as we shall show, in certain instances , it is true.

If in the polynomial conjecture we assume h is linear, the hypothesis is reduced to the condition $\bigcup_{1}^{\ell} V_p(g_i) = \{0,1,\cdots,p-1\}$ for a.a.p. The conclusion that there exists an index i such that $g_i(x)$ is linear is a consequence of the more general result:

Case A - The hypothesis of the polynomial conjecture implies the existence of an index i such that deg g_i divides deg h .

For the purposes of this work, a polynomial $h(x) \in \mathbb{Q}[x]$ will be called cyclic if $h(x) = a(x - b)^n + c$ for some $a,b,c \in \mathbb{Q}$.

Case B - Under the assumption that the polynomials $g_i(x)$, $i = 1,\dots,\ell$ are all cyclic, the polynomial conjecture is true.

Let $h(x)$, $g(x) \in L[x]$, 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 . We develop a necessary and sufficient condition that $h, g \in L[x]$ are a composite pair over L , and with this, we are able to answer certain questions about the factorization of the two variable polynomial $h(x) - g(y)$. One by-product of these techniques is:

Case C - In the polynomial conjecture, if we specialize the hypotheses to assume $V_p(h) = V_p(g)$ for a.a.p., for $h, g \in \mathbb{Z}[x]$, we are able to conclude that each decomposition of $h(x)$ into prime components has a corresponding 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 $g(x)$.

ACKNOWLEDGEMENTS

The writer wishes to thank his advisor, Professor Donald Lewis, for his help, encouragement and patience during the preparation of this thesis.

In addition, the writer thanks: Professor Armand Brumer for encouraging him to pursue the study of algebraic number theory, Professor Robert MacRae for showing the writer several alternate solutions to some of the contents herein, and Professor William LeVeque for his interest in the writer's work.

TABLE OF CONTENTS

		Page
ACKNOWLEDGEMENTS		ii
INTRODUCTION		1
SECTION		
I	PRELIMINARIES	8
II	DECOMPOSITION OF A POLYNOMIAL	20
III	THE POLYNOMIAL CONJECTURE	31
IV	QUADRATIC POLYNOMIALS	51
BIBLIOGRAPHY		59

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. Certainly one could not expect to find out much about a polynomial in $\mathbb{Z}[x]$ by knowing only its value set mod p for only one prime p. The object of this thesis is to show that if we let p run over all but a finite number of primes, the value sets mod p of a polynomial yield significant information about the nature of the polynomial.

Assume $h(x)$, $g(x)$ are elements of $\mathbb{Z}[x]$. For each rational prime p we denote those cosets mod p taken on by $h(x)$, by $V_p(h)$. If for almost all rational primes p (henceforth abbreviated a.a.p.) $V_p(h) \subset V_p(g)$, then we may conclude that either $h(x)-g(y)$ is a reducible polynomial in $\mathbb{Z}[x,y]$, or else g is linear. For, if $h(x)-g(y)$ were irreducible, the Hilbert Irreducibility Theorem ([1]) would imply that there exist infinitely many integers x_o such that $h(x_o)-g(y)$ is irreducible in $\mathbb{Z}[y]$. Since a non-linear polynomial which is irreducible in $\mathbb{Z}[y]$ has no zero

---

[1] Cf. Lang - Chap. 5. In this context, the Hilbert Irreducibility Theorem states that $\phi(x,y)$ irreducible in $\mathbb{Z}[x,y]$ remains irreducible in $\mathbb{Z}[y]$ when x is specialized to $x_o \in \mathbb{Z}$, for all but a set of integers x_o of asymptotic density zero.

mod p, for infinitely many primes p, there exist infinitely many primes p such that $h(x_0)-g(y) \equiv 0 \bmod p$ has no solution. Thus, unless g is linear, we have a contradiction to $V_p(h) \subset V_p(g)$ for a.a.p.

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 is an algebraically closed field we say merely that h, g are a composite pair.

For a time it was conjectured that h(x)-g(y) reducible in $\mathbb{C}[x,y]$ implies that h, g are a composite pair. This was shown false by a counter-example (Cf. Davenport, Lewis, Schinzel [1]). However, it is still not known whether h(x)-g(y) reducible in $\mathbb{Z}[x,y]$ implies that h, g are a composite pair over $\mathbb{Q}$.

In this work we wil attempt to answer questions related to the determination of a polynomial with coefficients in $\mathbb{Z}$ by knowledge alone of the value sets of that polynomial mod p, for a.a.p. Primarily we devote our attention to:

> The Polynomial Conjecture - Let $h(x), g_1(x), \ldots, g_k(x) \in \mathbb{Z}[x]$, and assume $V_p(h) \subset \bigcup_{i=1}^{k} V_p(g_i)$ for a.a.p. Then there exists an index i, and a polynomial $r(x) \in \bar{\mathbb{Q}}[x]$ (where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$) such that $h(x) = g_i(r(x))$.

If the polynomial conjecture were true, then

$V_p(h) \subset V_p(g)$ for a.a.p. would imply that h and g are a composite pair (indeed, even more than that). The polynomial conjecture has not been resolved, but, in certain instances it is true.

Before describing results related to the polynomial conjecture, we make note of an analog over $\mathbb{Z}$.

Theorem - Let $h(x), g_1(x), \ldots, g_\ell(x) \in \mathbb{Z}[x]$. Let $X = \{x_0 \in \mathbb{Z} \mid h(x_0) \in \bigcup_i^\ell V_{\mathbb{Z}}(g_i)\}$, where $V_{\mathbb{Z}}(g_i)$ denotes the set of values of g_i at the integers. If X has positive lower density, then there exists a polynomial $r(x) \in \mathbb{Q}[x]$ and an index i such that $g_i(r(x)) = h(x)$.([2])

Proof-

From the hypotheses we may with no loss assume $\ell = 1$ and $g_1(x) = g(x)$. Let $f(x,y) \in \mathbb{Z}[x,y]$. Let X' be that set of integers x_0 such that there exists a $y_0 \in \mathbb{Z}$ with $f(x_0,y_0) = 0$. If the lower density of X' is positive, we show that there exists $r(x) \in \mathbb{Q}[x]$ such that $f(x, r(x)) \equiv 0$.

Our theorem results when $X' = X$, $f(x,y) = h(x)-g(y)$. Our proof is modeled after that of Theorem 1 of Davenport, Schinzel, Lewis [2].

Factor $f(x,y)$ into irreducible factors over $\mathbb{Q}[x,y]$. From Gauss' Lemma, we may assume that these factors have

---

[2]This is in contrast to the polynomial conjecture which necessarily allows for $r(x) \in \bar{\mathbb{Q}}[x]$.

integer coefficients. In addition, one of these factors, say $\phi(x,y)$ satisfies the same conditions as does $f(x,y)$, with respect to a set of integers $X'' \subset X'$ with positive lower density. By the Hilbert Irreducibility Theorem, $\phi(x,y)$ remains irreducible when x is specialized to x_o for all but a set of integers x_o with zero density. The existence of a set of integers x_o with positive lower density such that $\phi(x_o,y) = 0$ is solvable in $\mathbb{Z}$ implies that $\phi(x,y)$ is linear in y. Thus, $\phi(x,y) = f_1(x) + f_2(x)y$ with $f_1, f_2 \in \mathbb{Z}[x]$. It follows from the irreducibility of $\phi(x,y)$ that there exist $a(x), b(x) \in \mathbb{Z}[x]$ such that $a(x)f_1(x) + b(x)f_2(x) = c$, $c \in \mathbb{Z}$. However, the existence of infinitely many x_o such that $\frac{f_1(x_o)}{f_2(x_o)}$ is an integer, implies that $\frac{c}{f_2(x_o)}$ is an integer for infinitely many x_o. Thus, $f_2(x)$ is a constant, and the result follows with $\frac{-f_1(x)}{c_1} = r(x)$.

Q. E. D.

Section I of this thesis is the technical key to the results relating to the polynomial conjecture, which are found in Section III. In Section I we assume that $h(x), g_1(x), \ldots, g_k(x) \in \mathbb{Z}[x]$ 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, <u>local polynomial hypothesis</u> 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, the hypothesis is reduced to the condition

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

The conclusion that there exists an index i such that $g_i(x)$ is linear is an immediate consequence of Corollary 3, which more generally implies, under the hypothesis of the polynomial conjecture, the existence of an index i such that $\deg g_i$ divides $\deg h$.

Case B -

For the purpose of this work a polynomial $h(x) \in \mathbb{Q}[x]$ will be said to be cyclic if $h(x) = a(x-b)^n + c$ for some $a, b, c \in \mathbb{Q}$. The terminology is suggested by the fact that the group of monodromy (the galois group of the splitting field of $h(x)-\lambda$ over $\bar{\mathbb{Q}}(\lambda)$, where λ is an indeterminate) of h is cyclic. We show in Theorem 5 that the polynomial conjecture is true if the polynomials $g_i(x)$, $i = 1, \cdots, \ell$, are all cyclic.

Case C -

Even in the conclusion of Theorem 5 it is not possible to replace the conclusion $r(x) \in \bar{\mathbb{Q}}[x]$ of the polynomial

conjecture by $r(x) \in Q[x]$. For example, suppose $h(x) = (2\cdot3\cdot5)x^2$, $g_1(x) = 2x^2$, $g_2(x) = 3x^2$, $g_3(x) = 5x^2$. Then $2\cdot3\cdot5$ is a quadratic residue mod p, only if at least one of 2, 3, or 5 is a quadratic residue mod p. Thus, we have $V_p(h) \subset \bigcup_1^3 V_p(g_i)$ for all p. However, no $g_i(x)$ and $h(x)$ form a composite pair over Q.

In Section IV we assume $h(x), g_1(x), \cdots, g_\ell(x)$ are all quadratic, and we find a necessary and sufficient condition in terms of the arithmetic properties of the coefficients of these polynomials in order that $V_p(h) \subset \bigcup_1^\ell V_p(g_i)$ for a.a.p. Thus, in this case we have a finite process for determining whether or not the hypothesis of the polynomial conjecture is satisfied. The technique of proof shows clearly that the same procedure can be carried out for cyclic polynomials all of the same prime degree.

Case D -

In Proposition 6 we show that the polynomial conjecture is true in the case where $\ell = 1$, and $g_1(x) = g(x)$ is of degree 2, 3, 4, or 5, or if the group of monodromy of $g(x)$ over $Q(\lambda)$ is the symmetric group or alternating group (as a permutation group acting on the zeros of $g(x)-\lambda$).

In Section II we develop a necessary and sufficient condition that $h, g \in L[x]$ are a composite pair over L, where L is any field. This condition enables us to answer some related questions concerning the factorization of the two variable polynomial $h(x)-g(y)$ (see Proposition 3 and

Theorem 3). One by-product of these techniques is another proof (see Theorem 2) of a theorem due to Ritt on the invariance of the degrees of the prime components in the decomposition of a polynomial with coefficients in a field of characteristic zero. For the definition of prime decomposition see Section II.

In the polynomial conjecture, even if we specialize the hypothesis 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 that each decomposition of $h(x)$ into prime component polynomials has a corresponding 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 $g(x)$.

Section I - Preliminaries

We reproduce below some notation and theorems which will be used in Theorem 1 of this section. These can all be found in Hasse and we do not bother to produce separate references here.

By a number field we always mean a field which is finite dimensional as a vector space over the rationals.

Frobenius Symbol -

Assume $L \subset M$ are two number fields; $\mathfrak{o}_M$ and $\mathfrak{o}_L$ denote the subrings of M and L that consist of elements which are zeros of polynomials with rational integer coefficients, having leading coefficient 1. $\mathfrak{o}_M$ is called the ring of integers of M, and $L \subset M$ implies $\mathfrak{o}_L \subset \mathfrak{o}_M$. A prime ideal $\mathfrak{p}$ of $\mathfrak{o}_L$ generates an ideal $\mathfrak{o}_M \cdot \mathfrak{p}$ in $\mathfrak{o}_M$. Since prime ideals are maximal (as ideals) each ideal in $\mathfrak{o}_M$ can be written uniquely as a product of prime ideals of $\mathfrak{o}_M$, and we write $\mathfrak{o}_M \cdot \mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, where the $\mathfrak{P}_i$ denote primes of $\mathfrak{o}_M$. In this case we say: a prime $\mathfrak{p}$ of L, has g primes over it in M with ramification indices $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ and degrees $f_i(\mathfrak{P}_i/\mathfrak{p}) = [\mathfrak{o}_M/\mathfrak{P}_i : \mathfrak{o}_L/\mathfrak{p}]$. Since $\mathfrak{P}_i \cap \mathfrak{o}_L = \mathfrak{p}$, the field $\mathfrak{o}_M/\mathfrak{P}_i$ always contains the field $\mathfrak{o}_L/\mathfrak{p}$.

We say that $\mathfrak{p}$ is unramified in M if $e(\mathfrak{P}_i/\mathfrak{p}) = 1$

for $i = 1, \ldots, g$. Of the infinite number of primes of L, only finitely many are ramified in M. A prime $\mathfrak{P}$ of M is unramified in L if $e(\mathfrak{P}/\mathfrak{p} \cap \mathcal{O}_L) = 1$.

For the remainder of this discussion assume M/L is galois, and denote by $G(M/L)$ the galois group of automorphisms of M fixed elementwise on L. In this case $e_i = e$, $f_i = f$ where e, f are constants dependent only on $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime of M. Each element $\sigma \in G(M/L)$ acts on the elements of $\mathcal{O}_M$ sending them into $\mathcal{O}_M$, and hence the image $\sigma(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_M$. Both $\mathfrak{P}$ and $\sigma(\mathfrak{P})$ lie over the same prime $\mathfrak{p}$ of L, i.e. $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L = \sigma(\mathfrak{P}) \cap \mathcal{O}_L$ since σ is fixed on elements of $\mathcal{O}_L$. The group $G(M/L)$ is transitive on the primes above $\mathfrak{p}$ in the sense that if $\mathfrak{P}' \cap \mathcal{O}_L = \mathfrak{p}$ there exists $\sigma' \in G(M/L)$ such that $\sigma'(\mathfrak{P}) = \mathfrak{P}'$.

For a prime $\mathfrak{P}$ of M, unramified over L, we distinguish a certain subgroup of $G(M/L)$ called the decomposition group of $\mathfrak{P}$:

$$Z_{\mathfrak{P}} = \{\sigma \in G(M/L) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

the group $Z_{\mathfrak{P}}$ is cyclic of order $f(\mathfrak{P}/\mathfrak{p})$. From the elements of $Z_{\mathfrak{P}}$, we pick a particular generator which we denote by $\left[\frac{M/L}{\mathfrak{P}}\right]$, and which is called the Frobenius symbol of $\mathfrak{P}$ over L. This element of $G(M/L)$ is uniquely described by the congruence condition:

$$\left[\frac{M/L}{\mathfrak{p}}\right] x \equiv x^{|\mathfrak{y}|} \bmod \mathfrak{p} \qquad \text{for each} \qquad x \in \mathcal{O}_M .$$

The symbol $|\mathfrak{y}|$ designates the norm of $\mathfrak{y}$, which is the cardinality of the residue class field $\mathcal{O}_L/\mathfrak{y}$.

If $\mathfrak{y}$ is a prime of L, unramified in M, then the symbol $\left(\frac{M}{\mathfrak{y}}\right)$ denotes the whole class of elements of G(M/L) conjugate (by elements of that group) to the Frobenius symbol of some prime $\mathfrak{p}$ lying over $\mathfrak{y}$. If $\mathfrak{y}\cdot\mathcal{O}_M = \prod_1^g \mathfrak{p}_i$, then $\left(\frac{M}{\mathfrak{y}}\right) = \bigcup_1^g \left[\frac{M/L}{\mathfrak{p}_i}\right]$.

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 $\mathfrak{y}$ of L such that $\left(\frac{M}{\mathfrak{y}}\right) \in U$ has a Dirichlet density and that density is $\frac{\text{card } U}{\text{card } G}$. This is the content of the Frobenius Density Theorem. A set of primes A of a number field L is said to have Dirichlet density α if

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{y} \in A} \frac{1}{|\mathfrak{y}|^s}}{-\log(s-1)} = \alpha .$$

A Theorem of Artin

Let M be any number field containing L, $\hat{M}$ the galois closure of M (i.e. $\hat{M}$ is the intersection of all fields galois over L containing M), and $G = G(M/L)$. From galois theory, there exists $\alpha \in M$ such that $M = L(\alpha)$. The group G can be considered as a transitive permutation group acting on the conjugates of α over L. If $\sigma \in \left(\frac{\hat{M}}{\mathfrak{y}}\right)$, $\sigma = \pi_1 \cdots \pi_r$, where $\mathfrak{y}$ is a prime of L

unramified in $\hat{M}$ and where π_i are the disjoint cycles formed by representing σ as a permutation on the conjugates of α, then $\mathfrak{p}$ factors into primes in M in the following way:

$$\mathfrak{p} \cdot \mathcal{O}_M = \prod_1^r \mathfrak{q}_i$$

where the $\mathfrak{q}_i$, $(i = 1, \cdots, r)$ are distinct prime ideals of degree $f_i = f(\mathfrak{q}_i/\mathfrak{p}) =$ length of π_i. In particular, $\mathfrak{p}$ is of degree one in $\hat{M}$ if and only if $\mathfrak{p}$ factors completely in M (i.e. $f(\mathfrak{q}_i/\mathfrak{p}) = 1$ for $i = 1, \cdots, r$).

Composite of Two Galois Groups

Let L_1/L and L_2/L be two galois extensions. The galois group $G(L_1 \cdot L_2/L)$ can be looked upon as

$$G = \{ (\sigma_1, \sigma_2) \in G_1 \times G_2 \mid \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2} \} \quad .$$

The action of $(\sigma_1, \sigma_2) \in G(L_1 \cdot L_2/L)$ is described by $(\sigma_1, \sigma_2)(\alpha\beta) = \sigma_1(\alpha)\sigma_2(\beta)$ for $\alpha \in L_1$, $\beta \in L_2$. Extend the action linearly to $L_1 \cdot L_2$.

This identification of the galois group is particularly convenient when one manipulates Frobenius symbols. For example, if $\mathfrak{p}$ is a prime of L and $\mathfrak{P}$ is a prime of $L_1 \cdot L_2/L$ lying over $\mathfrak{p}$, which is unramified in $L_1 \cdot L_2$, then:

$$\left[\frac{L_1 \cdot L_2/L}{\mathfrak{P}}\right] = \left(\left[\frac{L_1/L}{\mathfrak{P} \cap \mathcal{O}_{L_1}}\right], \left[\frac{L_2/L}{\mathfrak{P} \cap \mathcal{O}_{L_2}}\right]\right) \quad .$$

and in particular the restriction of $\left[\frac{L_1 \cdot L_2/L}{\mathfrak{p}}\right]$ to $\mathcal{O}_{L_1}$ is $\left[\frac{L_1/L}{\mathfrak{p} \cap \mathcal{O}_{L_1}}\right]$.

Preparation for Theorem 1

Let L be a number field. We will use the following notation:

P = primes (finite) of $\mathbb{Q}$.

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

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

Kummer's theorem implies that a polynomial $h(x) \in \mathbb{Z}[x]$ 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 $\mathbb{Q}(\theta_h)$, where θ_h is a zero of $h(x)$. This allows us to translate the local polynomial hypothesis (see the Introduction) to the relation

$$P'(\mathbb{Q}(\theta_h)) \dot{\subset} \dot{\bigcup_1^\ell} P'(\mathbb{Q}(\theta_{g_i}))$$

Theorem 1 - Let $h, g_1, \cdots, g_\ell$ be irreducible polynomials of $\mathbb{Z}[x]$. Then $P'(\mathbb{Q}(\theta_h)) \dot{\subset} \dot{\bigcup_1^\ell} P'(\mathbb{Q}(\theta_{g_i}))$ holds if and only if

$$\bigcup_{\theta_h} G(\Omega/\mathbb{Q}(\theta_h)) \subset \dot{\bigcup_1^\ell} \bigcup_{\theta_{g_i}} G(\Omega/\mathbb{Q}(\theta_{g_i}))$$

where Ω is the composite of the fields $\Omega_h, \Omega_{g_1}, \cdots, \Omega_{g_\ell}$ which are respectively the splitting fields of the polynomials $h, g_1, \ldots, g_\ell$ over $\mathbb{Q}$.

Remark: This theorem is a generalization of a theorem of Schinzel.

Proof -

If $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$, then from Artin's Theorem, a prime $p \in P$ which is unramified in Ω_f has a prime ideal factor of degree one in $\mathbb{Q}(\Theta_f)$ if and only if $\lambda = \left[\frac{\Omega}{\mathfrak{p}}, f\right]$, where $\mathfrak{p}$ is a prime of Ω_f over p, has a cycle of length one when λ is represented as acting on the zeros Θ_f of $f(x)$. This is equivalent to

$$\lambda \in \bigcup_{\Theta_f} G(\Omega_f/\mathbb{Q}(\Theta_f)) .$$

Suppose $\mathfrak{P}$ is a prime of Ω over $\mathfrak{p}$, $\mathfrak{p}$ a prime of Ω_h over p. If $\left[\frac{\Omega}{\mathfrak{P}}\right] \in \bigcup_{\Theta_h} G(\Omega/\mathbb{Q}(\Theta_h))$ then

$$\left[\frac{\Omega}{\mathfrak{P}}\right]\Big|_{\Omega_h} = \left[\frac{\Omega_h}{\mathfrak{p}}\right] \in \bigcup_{\Theta_h} G(\Omega_h/\mathbb{Q}(\Theta_h)) .$$

Conversely, if $\left[\frac{\Omega_h}{\mathfrak{p}}\right] \in \bigcup_{\Theta_h} G(\Omega_h/\mathbb{Q}(\Theta_h))$, then any extension of $\left[\frac{\Omega_h}{\mathfrak{p}}\right]$ to Ω is contained in $\bigcup_{\Theta_h} G(\Omega/\mathbb{Q}(\Theta_h))$ since $\mathbb{Q}(\Theta_h) \subset \Omega_h$. Thus, p has a prime ideal factor of degree one in $\mathbb{Q}(\Theta_h)$ if and only if $\left[\frac{\Omega}{\mathfrak{P}}\right] \in \bigcup_{\Theta_h} G(\Omega/\mathbb{Q}(\Theta_h))$.

Similarly, p has a prime ideal factor of degree one in one of the fields $\mathbb{Q}(\Theta_{g_i})$, $i = 1, \cdots, \ell$, if and only if $\left[\frac{\Omega}{\mathfrak{P}}\right] \in \bigcup_{1}^{\ell} \bigcup_{\Theta_{g_i}} G(\Omega/\mathbb{Q}(\Theta_{g_i}))$.

From the hypothesis $P'(\mathbb{Q}(\Theta_h)) \subset \bigcup_{1}^{\ell} P'(\mathbb{Q}(\Theta_{g_i}))$, if $\sigma \in \bigcup_{\Theta_h} G(\Omega/\mathbb{Q}(\Theta_h))$ and σ is of the form $\left[\frac{\Omega}{\mathfrak{P}}\right]$ for

infinitely many primes $\mathfrak{P}$ of Ω, then $\sigma \in \bigcup_{\theta_{g_i}} G(\Omega/\mathbb{Q}(\theta_{g_i}))$.

However, the Frobenius density theorem states that each $\sigma \in G(\Omega/\mathbb{Q})$ is of the form $\left[\frac{\Omega}{\mathfrak{P}}\right]$ for infinitely many primes $\mathfrak{P}$ of Ω.

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

Q. E. D.

Two Lemmas of Galois Theory

Lemma 1 - Let $f(x) \in L[x]$ be an irreducible polynomial, where L is any perfect field. Let $\Omega = L(x_1, \cdots, x_n)$ be the splitting field of f over L, where $x_1, \cdots, x_n$ are the zeros of f. If M is any galois subfield of Ω containing L, set $K = L(x_1) \cap M$. Then any automorphism of $G(M/L)$ which leaves K elementwise fixed can be extended to an element of $G(\Omega/L(x_1))$.

Proof -

We show that the irreducible polynomial for x_1 over K remains irreducible over M. Since $[L(x_1) : K]$ is the degree of the irreducible polynomial for x_1 over K, this is

equivalent to showing that $[M\cdot L(x_1) : M] = [L(x_1) : K]$. If this is true, and $\sigma \in G(M/K)$, then σ may be extended to an isomorphism of $M\cdot L(x_1)$ into $M\cdot L(x_i)$ where x_i is any other zero of the irreducible polynomial of x_1 over K. The automorphism we desire is an extension of this automorphism (where i = 1) to an automorphism of Ω.

From the formula

$$[M\cdot L(x_1) : M][M : K] = [M\cdot L(x_1) : L(x_1)][L(x_1) : K]$$

we need only show that $[M: K] = [M\cdot L(x_1): L(x_1)]$. From the theorem of natural irrationalities

$$G(M\cdot L(x_1)/L(x_1)) = G(M/L(x_1)\cap M) = G(M/K) .$$

Since card $G(M/K) = [M: K]$, we are done.

Q. E. D.

Lemma 2 - Let $f(x)$, Ω and M be as in Lemma 1, and in addition assume $L(x_1)\cap M = L$. Then there exists an automorphism $\sigma \in G(\Omega/M) - \bigcup_{i=1}^{n} G(\Omega/M\cdot L(x_i))$.

Proof -

As in Lemma 1 where K is $L = L(x_1)\cap M$, we see that $f(x)$ is irreducible over M. Thus $G(\Omega/M)$ is transitive as a permutation group on the zeros of f, and the groups $G(\Omega/M\cdot L(x_i))$, $i = 1,\cdots,n$ are the groups conjugate to $G(\Omega/M\cdot L(x_1))$. Since the union of the conjugates of a proper subgroup of a group does not contain each element of the group, σ exists.

Q. E. D.

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

Proposition 1 - Let h, g_1, g_2 be irreducible over $\mathbb{Q}$. If $P'(\mathbb{Q}(\theta_h)) \doteq \overset{2}{\underset{1}{U}} P'(\mathbb{Q}(\theta_{g_i}))$ then either

$$\mathbb{Q}(\theta_{g_1}) \cap (\Omega_{g_2} \cdot \Omega_h) \neq \mathbb{Q} \quad \text{or} \quad \mathbb{Q}(\theta_{g_2}) \cap (\Omega_{g_1} \cdot \Omega_h) \neq \mathbb{Q} \quad .$$

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

$$(1) \quad \sigma_1 \in G(\Omega_{g_1}/\mathbb{Q}) - \bigcup_{\theta_{g_1}} G(\Omega_{g_1}/\mathbb{Q}(\theta_{g_1})) \quad ,$$

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

Similarly, there exists

$$(2) \quad \sigma_2 \in G(\Omega_{g_2}/\mathbb{Q}) - \bigcup_{\theta_{g_2}} G(\Omega_{g_2}/\mathbb{Q}(\theta_{g_2}))$$

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

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

$$(3) \quad \bigcup_{\theta_h} G(\Omega/\mathbb{Q}(\theta_h)) \subset \overset{2}{\underset{1}{U}} \bigcup_{\theta_{g_i}} G(\Omega/\mathbb{Q}(\theta_{g_i})) \, .$$

If $(\sigma_1, \sigma_2, 1) \in G(\Omega_{g_1}/\mathbb{Q}) \times G(\Omega_{g_2}/\mathbb{Q}) \times G(\Omega_h/\mathbb{Q})$ is an element of $G(\Omega/\mathbb{Q})$ we obtain a contradiction as follows. Since $(\sigma_1, \sigma_2, 1)|_{\Omega_h}$ is the identity, $(\sigma_1, \sigma_2, 1) \in G(\Omega/\mathbb{Q}(\theta_h))$ for each θ_h. However $(\sigma_1, \sigma_2, 1)|_{\Omega_{g_i}} = \sigma_i$ for $i = 1, 2$ and this contradicts (3).

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

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

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 the field T contains $\Omega_h \cap (\Omega_{g_1} \cdot \Omega_{g_2})$, 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

(5) $G(\Omega'/T) \subset G(\Omega'/\Omega_h)$

Let $A = G(\Omega'/\Omega_h)$, $B = G(\Omega'/\Omega_{g_1})$, $C = G(\Omega'/\Omega_{g_2})$ so that $B \cap C = G(\Omega'/\Omega_{g_1} \cdot \Omega_{g_2}) = \{1\}$

Using the following easy to verify facts:

(a) If Ω/L is galois, then $M, N \subset \Omega$, $L \subset M$ and $L \subset N$ implies $G(\Omega/M \cdot N) = G(\Omega/M) \cap G(\Omega/N)$.

(b) If in addition M/L is galois, then $G(\Omega/M\cap N) = G(\Omega/N)\cdot G(\Omega/M)$. we may reduce (5) to

(6) $$\{B\cdot(A\cap C)\}\cap\{C\cdot(A\cap B)\}\subset A\,.$$

If $cb = c'b'$, where $b \in B$, $b' \in A\cap B$, $c \in A\cap C$, and $c' \in C$, then $c^{-1}c' = c(b')^{-1} \in C\cap B = \{1\}$. Thus, $cb \in A$, and this verifies (6).

Q. E. D.

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

<u>Corollary 1</u> - Let g_1, g_2 be irreducible polynomials in $\mathbb{Q}[x]$. Then $P \doteq \bigcup_1^2 P'(\mathbb{Q}(\Theta_{g_i}))$ implies that either $\mathbb{Q}(\Theta_{g_1})\cap\Omega_{g_2} \neq \mathbb{Q}$ or $\mathbb{Q}(\Theta_{g_2})\cap\Omega_{g_1} \neq \mathbb{Q}$.

We give an example of the situation expressed in Corollary 1. Let $g_1 = x^3-2$, $g_2 = x^2+x+1 \in \mathbb{Z}[x]$. To show that one of g_1 or g_2 has a zero mod p for each rational prime p, we consider two cases:

<u>Case 1</u> - $p \equiv 5 \bmod 6$

$a^3 \equiv 1 \bmod p$ implies either $a = 1$ or $3 \mid \phi(p) = p-1$. Thus, if $p \equiv 5 \bmod 6$, the kernel of the map $x \to x^3$ is just 1, and so there exists x_o such that $x_o^3 \equiv 2 \bmod p$.

Case 2 - $p \equiv 1 \bmod 6$

$a^3 \equiv 1 \bmod p$ has exactly 3 solutions, so that $x^2+x+1 \equiv 0 \bmod p$ has two solutions.

Note: This example shows that the hypotheses of Corollary 1 do not imply that one of g_1 or g_2 is linear, or even reducible.

Section II - Decomposition of a Polynomial

If $h(x) \in K[x]$, K a field of characteristic zero, then for λ an indeterminate we define $\Omega_{h-\lambda}$ to be the splitting field of $h(x) - \lambda$ over $K(\lambda)$. The zeros of $h(x) - \lambda$ will be designated by $x_1, \cdots, x_n$. where $n = \deg h$.

The representation $h(x) = h_1(h_2(\cdots(h_r(x))$ is said to be a prime decomposition of the polynomial $h(x)$ in $K[x]$ if $h_i(x) \in K[x]$ and none of $h_i(x)$ can be decomposed further into two non-linear polynomials. We can use the word 'decomposition' to distinguish between this and the situation where a polynomial is factored in $K[x]$. We say (following Ritt) that the decomposition of $h(x)$ is equivalent to another decomposition $h(x) = h_1'(h_2'(\cdots(h_s'(x))$ if $s = r$, and there exist linear functions $\psi_1, \cdots, \psi_{r-1}$ such that $h_1'(x) = h_1(\psi_1(x))$, $\psi_1^{-1}(h_2(\psi_2(x))) = h_2'(x), \cdots,$ $\psi_{r-1}^{-1}(h_r(x)) = h_r'(x)$. Two <u>equivalent decompositions will be considered the same</u>. We note that it is a consequence of Theorem 2 that the number of components in a prime decomposition of a polynomial is invariant. However, not all decompositions of a polynomial need be equivalent as the example $h(x) = x^{m \cdot n} = (x^m)^n = (x^n)^m$, with $(m,n) = 1$, shows.

Let h,g be a composite pair over K (see page 2).

Then $h(x)-g(y)$ is divisible by a proper factor $h_1(x)-g_1(y) \in K[x,y]$. In Proposition 3 we show that the converse is true. In Theorem 3 we give an explicit description of the different ways in which h,g can be represented as a composite pair.

Lemma 3 - 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 $K(\lambda) \subset M \subset K(x_1)$, $M = K(u(x_1))$, where $u \in K[x]$ and $h = r(u(x))$.

Proof -

(a) If M is a field such that $K(\lambda) \subseteq M \subseteq K(x_1)$, then by Lüroth's Theorem $M = K(\mu)$. Since $\lambda \in K(\mu)$, $\lambda = \frac{r(\mu)}{s(\mu)}$ where r,s are relatively prime polynomials of $K[x]$. Also $\mu = \frac{u(x_1)}{v(x_1)}$ where u,v are relatively prime polynomials of $K[x]$. Therefore,

$$(7) \qquad \frac{r\left(\frac{u}{v}(x_1)\right)}{s\left(\frac{u}{v}(x_1)\right)} = \lambda = h(x_1)$$

yields an identity since x_1 is an indeterminate.

If x is constant, and v is not constant, then a zero of v in $\bar{K}$ would be a finite pole of the left side of (7). However the right side of(7) has no finite pole. Thus, if s is a constant, so is v, and $r'(u'(x_1)) = \lambda = h(x_1)$ for polynomials $r',u' \in K[x]$, with $u'(x_1) = \mu$.

If s is not constant, and γ is some zero of s, $\frac{u(x)}{v(x)} = \gamma$ has a zero $x = \beta$ unless $u(x) - \gamma v(x) = c \in K$. If β exists, then β is a pole of the left side of (7), which again is a contradiction. Suppose γ_1, γ_2 are two distinct zeros of s. It is impossible for both of the polynomials $u(x) - \gamma_1 v(x)$ and $u(x) - \gamma_2 v(x)$ to be constant. So the existence of β is guaranteed. This leaves only the possibility $s(x) = a(x - \gamma)^t$ for some $\gamma, a \in K$, $t \in \mathbb{Z}$, and $u(x) = \gamma v(x) + c$.

From (7) we obtain

$$r\left(\gamma + \frac{c}{v(x)}\right)\left(\frac{v(x)}{c}\right)^t \left(\frac{1}{a}\right) = h(x). \tag{8}$$

The left side of (8) is not a polynomial unless $t \geq \deg r$. Thus $v(x)$ is a composite factor of $h(x)$, and $K(\mu) = K(v(x_1))$.

Suppose $M = K(u'(x_1)) = K(u''(x_1))$ where $u', u'' \in K[x]$. Then from the above, we know there exist polynomials $r', r'' \in K[x]$ such that $r'(u'(x)) = h(x) = r''(u''(x))$. From a standard argument in genus zero function fields (see Walker - pg. 196) there exist constants $a, b \in K$ such that $au' + b = u''$. Thus u', u'' correspond to equivalent decompositions of $h(x)$.

(b) Conversely, if $h(x) = r'(u'(x))$ we may associate with this decomposition $M = K(u'(x_1))$.

Q. E. D.

For a decomposition $h(x) = r(u(x))$ and a fixed zero x_1 of $h(x) - \lambda$ we will find it convenient to denote $u(x_1)$ by $r^{-1}(\lambda)$.

Proposition 2 - Assume $h,g \in K[x]$. Then h,g are a composite pair over K if and only if for each x_j there exists y_i a zero of $g(y) - \lambda$ such that $K(x_j) \cap K(y_i)$ contains $K(\lambda)$ as a proper subfield.

Proof -

Lemma 3 assures us that $K(x_1) \cap K(y_1) = K(u(x_1)) = K(w(y_1))$ for some polynomials u,w. We may assume without loss that $u(x_1) = w(y_1)$ (by the same argument as the last line of part (a) of Lemma 3). Also there exists $r \in K[x]$, such that

$$r(u(x_1)) = r(w(y_1)) = \lambda = h(x_1) = g(y_1).$$

The degree of r is greater than one if and only if $K(\lambda)$ is a proper subfield of $K(x_1) \cap K(y_1)$. The converse is obvious.

Q. E. D.

Proposition 3 - The polynomial $h(x)-g(y)$ is factorizable over K in the form $(h_1(x)-g_1(y))\phi(x,y)$, with $\deg \phi > 0$, if and only if h,g are a composite pair over K.

Proof -

Let ω be an indeterminate, and assume that x^*,y^* satisfy $h_1(x^*) = \omega = g_1(y^*)$. Let λ be the indeterminate

$h(x^*) = \lambda = g(y^*)$. If $\omega \in K(\lambda)$ then $\omega = \frac{u(\lambda)}{v(\lambda)}$ for some polynomials $u, v \in K[\lambda]$. However, this results in the relation $h_1(x) \equiv \frac{u(h(x))}{v(h(x))}$. This identity implies that h_1 is a non-constant polynomial in $h(x)$. However, we are assuming deg $h_1 <$ deg h. Therefore $K(\lambda)$ is a proper subfield of $K(x^*) \cap K(y^*)$ and we may apply Proposition 2 to conclude that h,g are a composite pair over K. The converse has already been noted at the beginning of this section.

Q. E. D.

Lemma 4 - If $h(x) \in K[x]$ and $h(x) = r(u(x))$, $r, u \in \bar{K}[x]$, then there exist $a,b \in \bar{K}$ such that: $au(x) + b = u'(x)$, and $r\left(\frac{x}{a} - \frac{b}{a}\right) = r'(x)$ are in $K[x]$ and $r'(u'(x)) = h(x)$.

Proof -

Pick $a \neq 0$, b so that the leading coefficient and constant coefficient of $u'(x)$, are in K. Clearly $r'(u'(x)) = h(x)$. We must show that this implies r' and $u' \in K[x]$.

Write $\sum_{i=0}^{k} b_i x^i = u'(x)$, $\sum_{j=0}^{s} a_j x^j = r'(x)$ so that our assumption $b_k \in K$ implies $a_s \in K$. In the equation $r'(u'(x))$, b_i appears linearly in the coefficient of $x^{k(s-1)+i}$ which is a rational function of $a_s, b_k, b_{k-1}, \cdots, b_i$. Thus we conclude by induction that $b_i \in K$. Since $u'(x) \in K[x]$, it is now obvious that $r'(x) \in K[x]$.

Q. E. D.

As an immediate consequence of Lemma 4 we obtain

Proposition 4 - Assume $h(x) \in K[x]$. The decompositions of $h(x)$ over $\bar{K}$ are equivalent uniquely to the decompositions of $h(x)$ over K.

Proposition 4 does not imply that the relation "h,g a composite pair over K" is equivalent to "h,g a composite pair." For example $h(x) = x^2$ and $g(x) = 2x^2$ are a composite pair over $\bar{\mathbb{Q}}$, but not over $\mathbb{Q}$.

We make several observations:

A great deal of information concerning the zeros of $h(x) - \lambda$ can be obtained by expanding the zeros about infinity. By the method of undetermined coefficients we see that if deg h = n, then there exists a zero $x_1 = a_{-1}\lambda^{\frac{1}{n}} + a_0 + a_1\lambda^{-\frac{1}{n}} + a_2\lambda^{-\frac{2}{n}} + \cdots$ with $a_i \in K(a_{-1})$. In addition, the other zeros are obtained from x_1 by replacing $\lambda^{\frac{1}{n}}$ by $\zeta\lambda^{\frac{1}{n}}$ where ζ is any n-th root of 1.

Conversely, if $\alpha \in \bar{K}(x_1,\cdots,x_n)$ is integral of degree n over $\bar{K}[\lambda]$, and $\alpha = b_{-1}\lambda^{\frac{1}{n}} + b_0 + b_1\lambda^{-\frac{1}{n}} + \cdots$, then α is a zero of $\alpha^n + r_1(\lambda)\alpha^{n-1} + \cdots + r_n(\lambda) = 0$ where $r_i(\lambda) \in \bar{K}[\lambda]$. The values $|r_i(\lambda)\alpha^{n-i}|_\infty$, $i = 1,\cdots,n$ are all distinct, and if $\deg r_n(\lambda) > 1$ or $\deg r_i(\lambda) > 0$ for $i = 1,\cdots,n-1$ we get a contradiction to the polynomial relation since $|\alpha^n|_\infty = 1$.[3]

---

[3] Let $L = \bigcup_{k=1}^{\infty} L_k$, where L_k is the field of all formal Laurent series in $\lambda^{-\frac{1}{k}}$ with coefficients in $\bar{K}$. $|\ |_\infty$ is a function from L into Q such that $|\sum_{n=N}^{\infty} a_n(\lambda^{-\frac{1}{k}})^n|_\infty = -\frac{N}{k} = |(\lambda^{-\frac{1}{k}})^N|_\infty$ if $a_N \neq 0$. If $\alpha, \beta \in L$, then $|\alpha\beta|_\infty = |\alpha|_\infty + |\beta|_\infty$ and $|\alpha + \beta|_\infty \geq \min(|\alpha|_\infty, |\beta|_\infty)$.

Lemma 5 - Let M,N be two subfields of $K(x)$ of degrees m,n respectively over $K(\lambda)$ where λ is a polynomial in x. Then: (1) $M \cap N$ is a subfield of $K(x)$ of degree (m,n) over $K(\lambda)$, (2) $M \cdot N$ is a subfield of $K(x)$ of degree $[m,n]$ over $K(\lambda)$.

Proof -

From Lemma 3 and Proposition 4, we may replace K by $\bar{K}$. Also from Lemma 3 and the remarks preceding this Lemma, we may choose α and $\beta \in K(x_1)$ such that $M = K(\alpha)$ and $N = K(\beta)$, where $\alpha = \lambda^{\frac{1}{m'r}} + a_0 + a_1 \lambda^{-\frac{1}{m'r}} + \cdots$,

$\beta = \lambda^{\frac{1}{n'r}} + b_0 + b_1 \lambda^{-\frac{1}{n'r}} + \cdots$, and where $m'r = m$, $n'r = n$, $r = (m,n)$.

(a) The following procedure suffices to construct the unique polynomial $f(x) \in \bar{K}[x]$ of degree m' such that $f(\alpha) = \lambda^{\frac{1}{r}} + c_1 \lambda^{-\frac{1}{m'r}} + \cdots$.

$$\alpha^{m'} = \lambda^{\frac{1}{r}} + m' a_0 \lambda^{\frac{m'-1}{m'r}} + \cdots ,$$

$$\alpha^{m'} - m' a_0 \alpha^{m'-1} = \lambda^{\frac{1}{r}} + a_1' \lambda^{\frac{m'-2}{m'r}} + \cdots ,$$

$$\alpha^{m'} - m' a_0 \alpha^{m'-1} - a_1' \alpha^{m'-2} = \lambda^{\frac{1}{r}} + a_1'' \lambda^{\frac{m'-3}{m'r}} + \cdots ,$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

Similarly there is a polynomial $g(x) \in \bar{K}[x]$ of degree n' such that $g(\beta) = \lambda^{\frac{1}{r}} + d_1 \lambda^{-\frac{1}{n'r}} + \cdots$. But, from Lemma 3, there exist polynomials $r(x)$, $s(x) \in \bar{K}[x]$ such that $\alpha = r(x_1)$, $\beta = s(x_1)$. Thus, $f(r(x_1)) - g(s(x_1))$ is a polynomial in x_1 whose expansion is of form

$(c_1 \lambda^{-\frac{1}{m \cdot r}} + \cdots) + (d_1 \lambda^{-\frac{1}{n \cdot r}} + \cdots)$ (i.e. no terms of order ≥ 0). Since x_1 is a transcendental, this implies that $f(r(x)) \equiv g(s(x))$. Thus, $f(\alpha) = g(\beta)$. It follows that M and N have an element in common which is a Laurent expansion in $\lambda^{-\frac{1}{k}}$ where $k \geq r$. Since $f(\alpha) \in M \cap N$, k must be a divisor of both m and n, and so $k | r$. Thus $k = r$ and $M \cap N$ is of degree r over $\bar{K}(\lambda)$.

(b) From Lemma 3, $M \cdot N = K(Y)$ where $Y = c_{-1} \lambda^{\frac{1}{k}} + c_0 + c_1 \lambda^{-\frac{1}{k}} + \cdots$, where k is the degree of $M \cdot N$ over $K(\lambda)$. Since $\alpha \in K(Y)$, $\beta \in K(Y)$ we know that $m | k, n | k$. Thus $[m,n] | k$. However, α and β can be regarded as Laurent series in $\lambda^{-\frac{1}{[m,n]}}$, and so every element of $M \cdot N$ is a Laurent series in $\lambda^{-\frac{1}{[m,n]}}$. Thus $k | [m,n]$, and we conclude $k = [m,n]$.

Q. E. D.

Corollary 2 - If $\lambda \in K[x]$ there is at most one subfield of $K(x)$ of degree d over $K(\lambda)$.

Proof -

Let $[M: K(\lambda)] = [N: K(\lambda)]$. Then Lemma 5 implies $[M \cdot N: K(\lambda)] = [M: K(\lambda)] = [N: K(\lambda)]$ so $M \cdot N = M = N$.

Q. E. D.

Theorem 2 - (J. F. Ritt) If we write $h(x) = h_1(h_2(\cdots(h_r(x)) = g_1(g_2(\cdots(g_s(x))$ where h_i, g_i are primely composite polynomials, then $r = s$ and the degrees of the h_i's are the same as the degree of the g_i's (although we need not have deg g_i = deg h_i for each i).

Proof -

From Lemma 3, if $K(\lambda) \subset M \subset N \subset K(x_1)$ (where x_1 is a zero of $h(x) - \lambda$), then there exist $\alpha, \beta \in K(x_1)$, and $g(x) \in K[x]$ such that $N = K(\alpha)$, $M = K(\beta)$ and $g(\alpha) = \beta$. Applying the statement of Lemma 3 where we let x_1 be α, λ be β, we see that g is compositely prime if and only if there are no proper fields between M and N. Thus we conclude that each maximal chain of subfields starting with $K(\lambda)$ and ending with $K(x_1)$ corresponds to a unique decomposition of $h(x)$ into primes. Conversely, the Laurent series $h_1^{-1}(\lambda)$, $h_2^{-1}(h_1^{-1}(\lambda)), \cdots$ are generators of fields forming a maximal chain between $K(\lambda)$ and $K(x_1)$.

Let $\widetilde{M} : M_1 \subset M_2 \subset \cdots \subset M_r$, $\widetilde{L} : L_1 \subset \cdots \subset L_s$ be two maximal chains of subfields between $K(\lambda)$ and $K(x_1)$. Let $X_{ij} = M_{i+1} \cap (M_i \cdot L_j)$, and $Y_{ji} = L_{j+1} \cap (L_j \cdot M_i)$.

$$M_i \subset X_{i1} \subset X_{i2} \cdots \subset X_{is} \subset M_{i+1}$$

$$L_j \subset Y_{j1} \subset Y_{j2} \cdots \subset Y_{jr} \subset L_{j+1}$$

The deg h_i's are the quantities $[M_{i+1} : M_i]$. Since

M_i, M_{i+1} are a pair in a maximal chain, there exists an integer t_i such that:

$$X_{i1} = X_{i2} = \cdots = X_{it_i} = M_i, \quad \text{and}$$

$$X_{it_i+1} = \cdots = X_{is} = M_{i+1}.$$

We wish to show there exists an integer j such that $[M_{i+1} : M_i] = [L_{j+1} : L_j]$. The integer $j = t_i$ works if we show:

$$(9) \qquad [X_{ij+1} : X_{ij}] = [Y_{ji+1} : Y_{ij}].$$

Denote $[M_i : K(\lambda)]$ by m_i, $[L_j : K(\lambda)]$ by n_j. From Lemma 3, the left side of (9) is:

$$\frac{(m_{i+1}, [m_i, n_{j+1}])}{(m_{i+1}, [m_i, n_j])} = \frac{\dfrac{m_{i+1} \cdot [m_i, n_{j+1}]}{[m_{i+1}, [m_i, n_{j+1}]]}}{\dfrac{m_{i+1} \cdot [m_i, n_j]}{[m_{i+1}, [m_i, n_j]]}} = \frac{[m_{i+1}, n_j]\,[m_i, n_{j+1}]}{[m_{i+1}, n_{j+1}]\,[m_i, n_i]}$$

By symmetry this is also the right side of (9).

Q. E. D.

We conclude this section with an example whose significance will become most clear in Section III. We give two polynomials $h_1(x)$, $h_2(x)$ such that $h_1(x) - \lambda$, $h_2(x) - \lambda$

have the same splitting field over $Q(\lambda)$, but h_1, h_2 are not a composite pair.

Example - Let $h_1(x) = (x^2-1)^2$. The zeros of $h_1(x) - \lambda$ are $x_1 = \sqrt{1 + \sqrt{\lambda}}$, $x_2 = -\sqrt{1 + \sqrt{\lambda}}$, $x_3 = \sqrt{1 - \sqrt{\lambda}}$, $x_4 = -\sqrt{1 - \sqrt{\lambda}}$. We list the elements of $G(Q(x_1, x_2, x_3, x_4)/Q(\lambda))$ as permutations:

$$\sigma_1 = 1, \quad \sigma_2 = (x_1 x_2), \quad \sigma_3 = (x_3 x_4), \quad \sigma_4 = (x_1 x_2)(x_3 x_4)$$

$$\sigma_5 = (x_1 x_3 x_2 x_4), \quad \sigma_6 = (x_1 x_4 x_2 x_3), \quad \sigma_7 = (x_1 x_4)(x_2 x_3),$$

$$\sigma_8 = (x_1 x_3)(x_2 x_4).$$

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 $x_1 + x_3$ has degree 4. From the comments preceding the statement of Lemma 5, $x_1 + x_3$ is a zero of a polynomial of form $h_2(x) - \lambda$ (since $x_1 + x_3$ is integral over $Q[\lambda]$ and it has an expansion at infinity of the form $a_{-1} \lambda^{1/4} + a_0 + a_1 \lambda^{-1/4} + \cdots$). It is easy to compute $h_2(x)$, and it turns out to be $1/4\, x^4 - x^2$. Clearly $h_1(x)$, $h_2(x)$ are not a composite pair. Since $(x_1 + x_4) - (x_2 + x_4) = 2x_1$, and $(x_2 + x_3) + (x_1 + x_3) = 2x_3$, we see that $\Omega_{h_1 - \lambda} = \Omega_{h_2 - \lambda}$.

Section III - The Polynomial Conjecture

We assume that we are given polynomials $h, g_1, \cdots, g_s$ satisfying the hypothesis $V_p(h) \subset \bigcup_1^s V_p(g_i)$ (i.e. the hypothesis of the polynomial conjecture). Our first task will be to translate Theorem 1 into a theorem which is capable of telling us something about the structure of the polynomials $h(x), g_1(x), \cdots, g_s(x)$ under this hypothesis.

Let Λ be the set of integers λ_0 such that $h(x)-\lambda_0, g_1(x)-\lambda_0, \cdots, g_s(x)-\lambda_0$ are all irreducible over $\mathbb{Q}$. By Hilbert's irreducibility theorem Λ has asymptotic density one.

Consider the two conditions:

GH : $P'(\mathbb{Q}(\Theta_{h-\lambda_0})) \doteq \bigcup_{j=1}^{s} P'(\mathbb{Q}(\Theta_{g_j-\lambda_0}))$ for all $\lambda_0 \in \Lambda$

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

Let λ_0 be any fixed value of Λ. If $p \in P'(\mathbb{Q}(\Theta_{h-\lambda_0}))$ then $h-\lambda_0$ has a linear factor mod p and consequently $\lambda_0 \in V_p(h)$. Now, if PCH holds, then $\lambda_0 \in V_p(g_i)$ for some j. It follows that $g_j-\lambda_0$ has a linear factor mod p and thus $p \in P'(\mathbb{Q}(\Theta_{g_j-\lambda_0}))$. Thus PCH implies GH. We are not able to decide whether GH implies PCH. However, it is easy to deduce that GH is equivalent to

PCH* : $V_p^s(h) \subset \bigcup_1^\ell V_p^s(g_i)$ for a.a.p.

(where $V_p^s(h)$ is the collection of values assumed by h with multiplicity one mod p).

Theorem 1 shows that condition GH for a fixed $\lambda_0 \in \Lambda$, is equivalent to a condition on galois groups. We next obtain a similar result for the condition PCH. The idea for the proof goes back to Hilbert, who proved his irreducibility theorem for just such problems.

Theorem 3 - Assume $h, g_1, \cdots, g_\ell \in \mathbb{Z}[x]$. Condition GH implies

PH : $\bigcup_{\Theta_{h-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\Theta_{h-\lambda})) \subset \bigcup_1^\ell \bigcup_{\Theta_{g_i-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\Theta_{g_i-\lambda}))$

where λ is an indeterminate, $\Theta_{h-\lambda}$ a zero of $h(x)-\lambda$, and Ω_λ is the composite of the splitting fields of $h-\lambda, g_1-\lambda, \cdots, g_\ell-\lambda$ over $\mathbb{Q}(\lambda)$.

Proof -

From Theorem 1 we see immediately that we must prove that

$$\bigcup_{\Theta_{h-\lambda_0}} G(\Omega_{\lambda_0}/\mathbb{Q}(\Theta_{h-\lambda_0})) \subset \bigcup_1^\ell \bigcup_{\Theta_{g_i-\lambda_0}} G(\Omega_{\lambda_0}/\mathbb{Q}(\Theta_{g_i-\lambda_0}))$$

for each allowable $\lambda_0 \in \Lambda$ (where the subscript λ_0 on Ω_{λ_0} denotes the composition of the splitting fields of $h-\lambda_0, g_1-\lambda_0, \cdots, g_\ell-\lambda_0$) implies

$$\bigcup_{\Theta_{h-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\Theta_{h-\lambda})) \subset \bigcup_{i} \bigcup_{\Theta_{g_i-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\Theta_{g_i-\lambda})) .$$

Let $m(x,\lambda) \in \mathbb{Q}[x,\lambda]$ be an irreducible normal polynomial, integral over $\mathbb{Q}[\lambda]$, whose splitting field over $\mathbb{Q}(\lambda)$ is Ω_λ.(4)

From Kummer's Theorem we know that, with the exception of finitely many additional values of λ_o, the primes in Ω_λ over the prime $\lambda - \lambda_o$ in $\mathbb{Q}[\lambda]$ are in one-one correspondence with the irreducible factors of $m(x,\lambda)$ mod $(\lambda - \lambda_o)$, hence with the irreducible factors of $m(x,\lambda_o)$. By the Hilbert irreducibility theorem, $m(x,\lambda_o)$ is irreducible, except for a set of λ_o of asymptotic density zero.

Denote by $\mathcal{O}_{\Omega_\lambda}$ the integral closure of $\mathbb{Q}[\lambda]$ in Ω_λ. Thus, for a set of λ_o of density one, there is a single unramified prime $\mathfrak{p}_{\lambda_o}$ over $\lambda - \lambda_o$, and $L_{\lambda_o} = \mathcal{O}_{\Omega_\lambda}/\mathfrak{p}_{\lambda_o}$ is the splitting field of $m(x,\lambda_o)$ over $\mathbb{Q}$. Let $\{\Theta_\lambda\}$ generically represent the union of the zeros of $h(x)-\lambda$, $g_1(x)-\lambda$, $\cdots$, $g_\ell(x)-\lambda$, and $\{\Theta_{\lambda_o}\}$ the union of the zeros of $h(x)-\lambda_o$, $\cdots$, $g_\ell(x)-\lambda_o$. The elements of the set $\{\Theta_\lambda\}$ are all integral over $\mathbb{Q}[\lambda]$, and together they generate Ω_λ over $\mathbb{Q}(\lambda)$. Thus, if we complete $\mathcal{O}_{\Omega_\lambda}$ with

---

(4) As a polynomial in x, $m(x,\lambda)$ is integral over $\mathbb{Q}[\lambda]$ if its leading coefficient is in $\mathbb{Q}$. By normal we mean that a zero of $m(x,\lambda)$ generates the splitting field of $m(x,\lambda)$ over $\mathbb{Q}(\lambda)$. From galois theory, if L/K is a finite algebraic and separable field extension, there exists $\Theta \in L$ such that $K(\Theta) = L$. The polynomial for Θ over K is normal, if L/K is galois.

respect to $\mathfrak{p}_{\lambda_0}$, then (with finitely many exceptional values of λ_0), $\{\vartheta_\lambda\}$ also generates the completion, which we call $\mathfrak{O}_{\Omega_\lambda}$. Thus, $\mathfrak{O}_{\Omega_\lambda}/\mathfrak{p}_{\lambda_0} = \mathcal{O}_{\Omega_\lambda}/\mathfrak{p}_{\lambda_0}$, and for a set of λ_0 of density one, the set $\{\vartheta_{\lambda_0}\}$ generates $\mathcal{O}_{\Omega_\lambda}/\mathfrak{p}_{\lambda_0} = L_{\lambda_0}$. But, by definition, the field generated by the set $\{\vartheta_{\lambda_0}\}$ is Ω_{λ_0}. Thus, for a set Λ' of λ_0 (of asymptotic density one) there is a single unramified prime $\mathfrak{p}_{\lambda_0}$ of Ω_λ over $\lambda - \lambda_0$. We therefore conclude that

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

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

The group of automorphisms σ of $G(\Omega_\lambda/\mathbb{Q}(\lambda))$ fixing $\mathfrak{p}_{\lambda_0}$ (i.e. the decomposition group of $\mathfrak{p}_{\lambda_0}$) can be identified with the automorphisms $\bar{\sigma}$ of $G(\Omega_{\lambda_0}/\mathbb{Q})$ by the formula:

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

From (10) we see that for $\lambda_0 \in \Lambda'$, $G(\Omega_\lambda/\mathbb{Q}(\lambda)) = G(\Omega_{\lambda_0}/\mathbb{Q})$ and from (11) we see that $\sigma \in G(\Omega_\lambda/\mathbb{Q}(\eta))$ if and only if $\bar{\sigma} \in G(\Omega_{\lambda_0}/\mathbb{Q}(\bar{\eta}))$ for any $\eta \in \mathcal{O}_{\Omega_\lambda}$. The sets Λ, Λ' being of asymptotic density one, have an intersection $\Lambda \cap \Lambda'$ of asymptotic density one. Thus, for $\lambda_0 \in \Lambda \cap \Lambda'$

$$\bigcup_{\vartheta_{h-\lambda_0}} G(\Omega_{\lambda_0}/\mathbb{Q}(\vartheta_{h-\lambda_0})) \subset \bigcup_i \bigcup_{\vartheta_{g_i-\lambda_0}} G(\Omega_{\lambda_0}/\mathbb{Q}(\vartheta_{g_i-\lambda_0}))$$

if and only if

$$\bigcup_{\theta_{h-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\theta_{h-\lambda})) \subset \bigcup_{i} \bigcup_{\theta_{g_i-\lambda}} G(\Omega_\lambda/\mathbb{Q}(\theta_{g_i-\lambda})) \quad .$$

Q. E. D.

As a start to an investigation of the polynomial conjecture, expand each of $\theta_{h-\lambda}, \theta_{g_1-\lambda}, \cdots, \theta_{g_\ell-\lambda}$ at infinity. From the discussion preceding Lemma 5, all these expansions are of the form:

$$\theta_{h-\lambda} = a_{-1}\lambda^{\frac{1}{N}} + a_0 + a_1\lambda^{-\frac{1}{N}} + \cdots$$

$$\theta_{g_i-\lambda} = a_{-1}^{(i)}\lambda^{\frac{n_i}{N}} + a_0^{(i)} + a_1^{(i)}\lambda^{-\frac{n_i}{N}} + \cdots, \quad i = 1, \cdots, \ell .$$

Let N be the least common multiple of the integers $n, n_1, \cdots, n_\ell$, and let ζ_N be a primitive N-th root of 1. The power series expansions for $\theta_{h-\lambda}, \theta_{g_1-\lambda}, \cdots, \theta_{g_\ell-\lambda}$ give an embedding of Ω_λ into L_N, the field of all formal Laurent series in $\lambda^{-\frac{1}{N}}$ with coefficients in $\bar{\mathbb{Q}}$. Let σ be an operator on L_N defined in the following way:

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

Since σ is a change of variable, it is obviously a field automorphism of L_N, and the fixed field of σ is the set of formal Laurent series in λ^{-1}. We denote again by σ

the restriction of this automorphism to Ω_λ, and we note that σ leaves $Q(\lambda)$ elementwise fixed.

Corollary 3 - If $h, g_1, \cdots, g_k \in Z[x]$ and if $V_p(h) \subset \overset{k}{\underset{1}{\cup}} V_p(g_i)$ for a.a.p., then there exists an index i such that the degree of g_i divides the degree of h. In particular, if h is linear, so is g_i for some i.

Proof -

From Theorem 3, our hypothesis implies

$$\bigcup_{\theta_{h-\lambda}} G(\Omega_\lambda / Q(\theta_{h-\lambda})) \subset \overset{k}{\underset{i}{\cup}} \bigcup_{\theta_{g_i-\lambda}} G(\Omega_\lambda / Q(\theta_{g_i-\lambda})).$$

If $\alpha \in L_N$, then $\sigma^n(\alpha(\lambda^{\frac{1}{N}})) = \alpha(\zeta_N^n \lambda^{\frac{1}{N}})$. Let m be the least integer such that α is expressible as $\alpha = \alpha(\lambda^{\frac{1}{m}}) = \alpha((\lambda^{\frac{1}{N}})^{\frac{N}{m}})$. Then $(\zeta_N^n)^{\frac{N}{m}} = 1$ if and only if $m|n$. So $\sigma^n(\alpha) = \alpha$ if and only if $m|n$.

Each $\theta_{h-\lambda}$ is of the form

$$\theta_{h-\lambda} = \beta(\lambda^{\frac{1}{n}}) = \beta((\lambda^{\frac{1}{N}})^{\frac{N}{n}}).$$

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, $n_1|n$.

Q. E. D.

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 $\Omega_{g_1,\lambda} = \Omega_{g_1-\lambda} \cdots \Omega_{g_k-\lambda}$. From Lemma 3 there exist polynomials $h^*(x), v(x) \in Q[x]$

such that $h = h^*(v)$ and

$$\mathbb{Q}(\theta_{h-\lambda}) \cap \Omega_{g,\lambda} = \mathbb{Q}(v(\theta_{h-\lambda})) \quad .$$

From Lemma 1, the collection of elements obtained by restricting the elements of $G(\Omega_\lambda/\mathbb{Q}(\theta_{h-\lambda}))$ to $\Omega_{g,\lambda}$ is just $G(\Omega_{g,\lambda}/\mathbb{Q}(\theta_{h-\lambda}))$. Therefore our relation PH (see Theorem 4) yields

$$(12) \qquad \bigcup_{\theta_{h-\lambda}} G(\Omega_{g,\lambda}/\mathbb{Q}(\theta_{h-\lambda})) \subset \bigcup_{i}^{g} \bigcup_{\theta_{g_i-\lambda}} G(\Omega_{g,\lambda}/\mathbb{Q}(\theta_{g_i-\lambda})) .$$

If we know that (12) implies the existence of an index i and a polynomial $r(x) \in \bar{\mathbb{Q}}[x]$ 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 that $h^*(x) = h(x)$.

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

$$(13) \qquad \bigcup_{\theta_{h-\lambda}} G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\theta_{h-\lambda})) \subset \bigcup_{i}^{g} \bigcup_{\theta_{g_i-\lambda}} G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\theta_{g_i-\lambda}))$$

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

Lemma 6 - If $h(x) \in \bar{\mathbb{Q}}[x]$ and $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is abelian, then $h(x)$ is a cyclic polynomial.

Proof -

Since $\Sigma_{h-\lambda}$ is the splitting field of $h(x)-\lambda$ over $\bar{\mathbb{Q}}(\lambda)$, our assumption that $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is abelian implies that $\Sigma_{h-\lambda} = \bar{\mathbb{Q}}(\theta_{h-\lambda})$. Thus $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ 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 Lemma 3 we decompose $h(x)$ into $h_1(h_2(\cdots(h_r(x))$ where $h_1(h_2(\cdots(h_i(x))$ corresponds to the subfield of $\bar{\mathbb{Q}}(\theta_{h-\lambda})$ of degree ℓ_i over $\bar{\mathbb{Q}}(\lambda)$, where ℓ_{i+1}/ℓ_i $(i = 1,\cdots,n-1)$ is a prime. Thus we conclude that each $h_i(x)$, $i = 1,\cdots,r$ is of prime degree, and $G(\Sigma_{h_i-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is cyclic of order $\deg h_i$.

In the discussion preceding Corollary 3, we showed how to attach an automorphism σ of $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ to the ramification that occured at infinity. Similarly, we are able to attach such an automorphism to any finite ramified place.([4]) Suppose λ_0 is a value of λ such that $h(x)-\lambda_0$ has a multiple zero α. Then $h(x)-\lambda_0 = (x-\alpha)^{m(\alpha)}g(x)$, where $(g(x),x-\alpha) = 1$. Thus, $x-\alpha$ is expandable in powers of $(\lambda-\lambda_0)^{1/m(\alpha)}$ and no integer smaller than $m(\alpha)$ will

---

[4] The action of this automorphism on a Taylor series in $(\lambda-\lambda_0)^{1/t}$ (where t is the ramification index) is obtained by sending $(\lambda-\lambda_0)^{1/t}$ into $\zeta_t(\lambda-\lambda_0)^{1/t}$ where ζ_t is a primitive t-th root of one.

suffice. The sum $\Sigma(m(\alpha)-1) = n-1$, the number of values λ_o (counting with multiplicity) that satisfy $h(x)-\lambda_o$ and $h'(x)$ have common zero α (cf. Walker - page 25).

We apply these remarks to the polynomials $h_i(x)$, $i = 1,\cdots,r$. Since the curve $h_i(x)-\lambda = 0$ has a ramified place λ_o and this place must be ramified of index equal to the degree of $h_i(x)$ (from the fact that this ramification corresponds to an automorphism of $G(\Sigma_{h_i-\lambda}/\bar{\mathbb{Q}}(\lambda))$) we conclude that $h_i(x)-\lambda_o = a(x-b)^{\ell_i/\ell_{i-1}}$ for some $a,b \in \bar{\mathbb{Q}}$. Thus, $h_i(x)$ is a cyclic polynomial, and therefore $h(x)$ is a composite of cyclic polynomials. From the fact that $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is cyclic of order $n = \deg h$, we shall deduce that $h(x)$ is actually cyclic.

Let $f(x) = (g(x))^k+d$ where $g(x) = (x-b)^\ell+e$. We claim that $G(\Sigma_{f-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is cyclic only if $e = 0$. Changing λ to $\lambda-d$, x to $x+b$, we may with no loss assume: $f(x)-\lambda = (x^\ell+e)^k-\lambda$. The zeros of this polynomial are:

$$x_{t,s} = \zeta_\ell^t(\zeta_k^s\lambda^{\frac{1}{k}} - e)^{\frac{1}{\ell}}$$

where ζ_ℓ, ζ_k are primitive ℓ and k-th roots of one. If $G(\Sigma_{f-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is cyclic, then $\bar{\mathbb{Q}}(x_{o,o})$ would contain all the other zeros $x_{t,s}$. However, letting $\lambda^{1/k} = z$, if $(\zeta_k z-e)^{1/\ell} \in \bar{\mathbb{Q}}((z-e)^{1/\ell})$, there exist polynomials r and s such that

$$\frac{r((z-e)^{1/\ell})}{s((z-e)^{1/\ell})} = (\zeta_k z-e)^{1/\ell} .$$

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

Q. E. D.

Lemma 7 - Let $h(x), g_1(x),\cdots, g_\ell(x) \in \bar{\mathbb{Q}}[x]$ be cyclic polynomials such that $\Sigma_{h-\lambda} \subset \Sigma_{g,\lambda}$ and

$$G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\theta_{h-\lambda})) \subset \bigcup_i \bigcup_{\theta_{g_i-\lambda}} G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\theta_{g_i-\lambda})) .$$

Then for some index i, there exists $r(x) \in \bar{\mathbb{Q}}[x]$ such that $g_i(r(x)) = h(x)$.

Proof -

A cyclic polynomial is ramified over exactly one finite prime. If $h(x) = a(x-b)^n+c$, by relabeling, we may assume that N is the composite of the fields $\Sigma_{g_i-\lambda}$, $i = 1,\cdots,s$, which are ramified over $\lambda-c$. Using the remaining polynomials, let $N_i (i = 1,\cdots,v)$ be the composite of the fields $\Sigma_{g_i-\lambda}$ which have one common ramified prime among them.

If there exists an index i between 1 and s such that $\deg g_i \mid \deg h$, then $g_i = a'(x-b')^{n_i}+c$, $n_i \mid n$, and it is

easy to find the appropriate polynomial $r(x)$. Since there are no proper subfields unramified over $\bar{\mathbb{Q}}(\lambda)$, $N \cap N_1 \cdots N_v = \bar{\mathbb{Q}}(\lambda)$ and we see inductively that

$$G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\lambda)) = G(N/\bar{\mathbb{Q}}(\lambda)) \times G(N_1/\bar{\mathbb{Q}}(\lambda)) \times \cdots \times G(N_v/\bar{\mathbb{Q}}(\lambda)).$$

Let k be the l.c.m. of $\deg g_1, \cdots, \deg g_s$. Let τ be the automorphism on N described by $\tau\left(\alpha((\lambda-c)^{\frac{1}{k}})\right) = \alpha\left(\zeta_k(\lambda-c)^{\frac{1}{k}}\right)$. The group $G(N/\bar{\mathbb{Q}}(\lambda))$ is cyclic of order k and generated by τ. Similarly, there exist automorphisms η_i $(i = 1,\cdots,v)$ which are respectively, generators of the cyclic groups $G(N_i/\bar{\mathbb{Q}}(\lambda))$ $(i = 1,\cdots,v)$. Let $\eta = (\eta_1, \cdots, \eta_v)$. The automorphism $(\tau^n, \eta) \in G(\Omega_{g,\lambda}/\bar{\mathbb{Q}}(\lambda))$ is fixed on $\bar{\mathbb{Q}}(\theta_{h-\lambda})$. Since η fixes none of $\theta_{g_j-\lambda}$ for $j = s+1,\cdots,\ell$ the hypothesis implies

$$(\tau^n, \eta) \in G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\theta_{g_i-\lambda})) \qquad \text{for some } i = 1,\cdots,s.$$

For this index i, $\tau^n \in G(N/\bar{\mathbb{Q}}(\theta_{g_i-\lambda}))$ and we conclude that $\deg g_i \mid \deg h$.

Q. E. D.

Theorem 4 - If $h, g_1, \cdots, g_\ell \in \mathbb{Z}[x]$ and $V_p(h) \subset \bigcup_i V_p(g_i)$ for a.a.p., and if in addition, $g_1, \cdots, g_\ell$ are cyclic polynomials, then there exists $r(x) \in \bar{\mathbb{Q}}[x]$ and an index i such that $h(x) = g_i(r(x))$.

Proof -

Although no assumption was made about h, from the remarks preceding Lemma 6, we may immediately presume that $\Theta_{h-\lambda} \in \Omega_{g,\lambda}$, and thus that $\Sigma_{h-\lambda} \subset \Omega_{g,\lambda}$. Therefore, $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is a factor group of $G(\Sigma_{g,\lambda}/\bar{\mathbb{Q}}(\lambda))$. Since the latter is a subgroup of the direct product of the cyclic groups $G(\Sigma_{g_i-\lambda}/\bar{\mathbb{Q}}(\lambda))$ for $i = 1,\cdots,\ell$, we conclude that $G(\Sigma_{h-\lambda}/\bar{\mathbb{Q}}(\lambda))$ is abelian.

From Lemma 6, we see that h is a cyclic polynomial, and from Lemma 7, the conclusion of the theorem follows.

Q. E. D.

Corollary 4 - Let $\ell_1, \ell_2, \cdots, \ell_k$ by an increasing sequence of integers such that: $h(x) \in \mathbb{Z}[x]$ takes on values mod p for a.a.p. which are all among $\ell_1,\cdots,\ell_k$-th powers. Then there exists $a' \in \mathbb{Q}$, $r'(x) \in \mathbb{Q}[x]$ and an index i such that $h(x) = a'(r'(x))^{\ell_i}$.

Proof -

From Theorem 4 above, we may conclude immediately from these hypotheses that there exists an index i such that: $h(x) = (r(x))$ for some $r(x) \in \bar{\mathbb{Q}}[x]$. From Lemma 4, there exist constants $a,b \in \bar{\mathbb{Q}}$ such that $\left(\frac{x-b}{a}\right)^{\ell_i} \in \mathbb{Q}[x]$ and $ar(x)+b \in \mathbb{Q}[x]$. Thus we conclude that $a^{\ell_i} \in \mathbb{Q}$ and $b \in \mathbb{Q}$. Let $r'(x) = ar(x)$, and $a^{-\ell_i} = a'$ to conclude the lemma.

Q. E. D.

The remainder of this section is restricted to the case of the polynomial conjecture where $\ell = 1$, and we bring to bear only group theory to deduce consequences from relation (12) in the case $\ell = 1$. The fact that such reasoning cannot completely resolve even the case where $\ell = 1$ will be illustrated at the end of this section by an example which Professor J. McLaughlin showed to me.

We start with a group theory lemma.

Lemma 8 - An intransitive permutation group G of degree n has order dividing $(s_1!)(s_2!)\cdots(s_r!)$ where the n letters $a_1,\cdots,a_n$ are divided into r transitivity classes of which the i-th contains s_i elements.

Proof -

Writing each element of G as a product of disjoint cycles, G has a representation as a direct product of groups G_i, where G_i is a transitive permutation group on s_i letters. Thus the order of G_i is a multiple of s_i and a divisor of $s_i!$.

Q. E. D.

Proposition 6 - Let $h,g \in \mathbb{Z}[x]$, and assume that $V_p(h) \subset V_p(g)$ for a.a.p. If $G(\Omega_{g-\lambda}/\mathbb{Q}(\lambda))$ (when represented as a permutation group on the zeros of $g(x)-\lambda$) is the symmetric group, the alternating group, or any group of degree 2,3,4,5, then there exists $r(x) \in \mathbb{Q}[x]$ such that $g(r(x)) = h(x)$.

Proof -

From relation (12) we may assume $\Omega_{h-\lambda} \subset \Omega_{g-\lambda}$ and

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

From corollary 3, deg g|deg h. But, $\theta_{h-\lambda}$ is expressible as a rational function of the $\theta_{g-\lambda}$, which are in turn Laurent series in $\lambda^{-\frac{1}{n'}}$ where deg g = n'. Therefore deg h|deg g, and so deg h = deg g.

For the rest of this argument, we will let

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

If $H = G^*$, then the fundamental theorem of galois theory implies that $\mathbb{Q}(\theta_{h-\lambda}) = \mathbb{Q}(\theta_{g-\lambda})$, and from Corollary 3, this in turn implies the existence of $a,b \in \mathbb{Q}$ such that $g(ax+b) = h(x)$. In each of the cases below, we tacitly assume $H \neq G^*$. If H were a transitive group when represented on the letters $\theta_{g-\lambda}$ then we could conclude 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 <u>intransitive</u> on the zeros of $g(x)-\lambda$.

Case 1 - G is alternating or symmetric group of degree $n \geq 6$.

If the order of H were $(n-1)!$, then G would be of order $n!$ and therefore the symmetric group. Thus H (being an intransitive group) would leave exactly one of the letters fixed (being an intransitive group) and so $H = G^*$ (where we have properly selected G^* from among its possible conjugates). Thus, from Lemma 8 of this section, we may assume the order of H is less than or equal to $2!(n-2)!$. But, since G is assumed to be the alternating or symmetric group of degree n, the order of $H \geq \frac{(n-1)!}{2}$. Thus, we are done, unless $n \leq 5$.

For $n = 2$ or 3, we easily deduce that we must have $H = G^*$.

Case 2 - $n = 4$

Repeating the argument of Case 1 for $n = 4$, unless H fixes one of the $\Theta_{g-\lambda}$, we find that the order of $H \leq 4$ and a divisor of 4. If the order of H were 4, then the order of G would be 16 and G would not be of degree 4. So the order of H is 2. Since each element of H must fix one of the $\Theta_{g-\lambda}$'s (from the union of the conjugates of H contained in the union of the conjugates of G^*) H is a stabilizer of some $\Theta_{g-\lambda}$.

Case 3 - $n = 5$

Again, as in Case 1 for $n = 5$, we deduce that unless H fixes one of the $\Theta_{g-\lambda}$, the order of H is a divisor of

$3!(2!)$. Thus, we automatically can exclude the case where G is the symmetric group of degree 5.

If order of H is divisible by 4, we can argue in the following way: The 2-sylow subgroups of G are exactly the conjugates of the group generated by $\{(12)(34), (13)(24)\}$ (where we have replaced the letters $\theta_{3-\lambda}$ by the numbers $1,2,3,4,5$ in some order). G acts (by conjugation) on the 2-sylow subgroups in exactly the same way it acts on the $\theta_{3-\lambda}$, and since the order of H is divisible by 4, it too must contain one of the 2-sylow subgroups of G. Thus H must be a stabilizer of one of the $\theta_{3-\lambda}$.

This leaves us to deal with the subcases where order of H is $2,3$, or 6 and order of G is $10,15$, or 30. Since each element of H fixes one of the $\theta_{3-\lambda}$, if H were cyclic it would be a stabilizer of one of $\theta_{3-\lambda}$. If the order of G is 30, by the Sylow Theorem, G must contain 10 3-sylows (since 10 is the only number dividing 30 which is congruent to 1 mod 3). But, if there were more than 5 2-cycles in G, we would contradict order of G being 30. Thus G can be considered as acting on the 2-sylow subgroups by conjugation and since H contains a 2-sylow, $H = G^*$.

Q. E. D.

For our last proposition, we further specialize the hypotheses of the polynomial conjecture to assume $V_p(h) = V_p(g)$ for a.a.p.

Proposition 7 - Assume $h, g \in \mathbb{Z}[x]$. 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 of $h(x)$ 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 3), we conclude that

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

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

Let M be a subfield of $\mathbb{Q}(\theta_{h-\lambda})$ containing $\mathbb{Q}(\lambda)$. Thus, from Lemma 3, $M = \mathbb{Q}(\theta_{h^*-\lambda})$ where $h = h^*(r(x))$. The restriction of the elements of $G(\Omega_{g-\lambda}/\mathbb{Q}(\theta_{h-\lambda}))$ to $\Omega_{h^*-\lambda}$ yields $G(\Omega_{h^*-\lambda}/\mathbb{Q}(\theta_{h^*-\lambda}))$, and from Lemma 2 the restriction of elements of $G(\Omega_{g-\lambda}/\mathbb{Q}(\theta_{g-\lambda}))$ to $\Omega_{h^*-\lambda}$ yields $G(\Omega_{h^*-\lambda}/\mathbb{Q}(\theta_{g^*-\lambda}))$ where $\mathbb{Q}(\theta_{g-\lambda}) \cap \Omega_{h^*-\lambda} = \mathbb{Q}(\theta_{g^*-\lambda})$. We obtain:

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

Repeating the argument of the first paragraph of Proposition 6, we conclude that $\Omega_{h^*-\lambda} = \Omega_{g^*-\lambda}$, and $\deg h^* = \deg g^*$.

Q. E. D.

Of the unresolved cases of the polynomial conjecture, the simplest would seem to be that described by the hypotheses of Proposition 7 (i.e. $V_p(h) = V_p(g)$ for a.a.p.). From the example at the end of Section II we know that the condition $\Omega_{h-\lambda} = \Omega_{g-\lambda}$ does <u>not</u> imply that $h(x) = g(ax+b)$ for some $a,b \in \mathbb{Q}$.

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

(15) $\Omega_{h-\lambda} = \Omega_{g-\lambda}$

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

(17) There exists $\sigma \in G(\Omega_{g-\lambda}/\mathbb{Q}(\lambda))$ such that σ represented as acting on either the $\theta_{h-\lambda}$, or $\theta_{g-\lambda}$ is an n-cycle.

We now show that there does exist a group G which may be represented in inequivalent ways on two different sets of letters $\{x_1,\cdots,x_n\}, \{y_1,\cdots,y_n\}$ 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 $\sigma \in G$ such that $\sigma(x_i) = x_{i+1}$, $\sigma(y_i) = y_{i+1}$. The projective group $P(2,p^k)$ acting on projective space with coefficients in $\mathbb{F}_{p^k}$ is the group we desire. The group $P(2,p^k)$ is doubly transitive (and thus primitive) on both points and lines (our two sets of letters being the points $\{x_1,\cdots,x_n\}$ and lines $\{y_1,\cdots y_n\}$ of this projective space).

Assume that a transformation T fixes a line L. With no loss, we assume L is the line $x_o = 0$, so $T\begin{pmatrix}0\\a\\b\end{pmatrix} = \begin{pmatrix}0\\a_1\\b_1\end{pmatrix}$. Thus, T is of the form:

$$T = \begin{pmatrix} a & o & o \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} .$$

Therefore, T fixes the point (1,b,c) where b and c are given as solutions of the equations $ab = b_1 + b_2b + b_3c$, $ac = c_1 + c_2b + c_3c$. Using the projective space duality between lines and points, we see that each transformation that fixes some line fixes also some point, and conversely. Thus, $\cup G_{x_i} = \cup G_{y_i}$. These representations for G are not the same though because $G_{y_i} \neq G_{x_i}$ for $i = 1,\cdots,n$. This can be seen by using our computation above, where we assume with no loss that y_1 is a letter representing the line $x_o = 0$.

If we let $\alpha \in \mathbb{F}_{p^k}$ be a primitive generator of the cyclic group of nonzero elements, then $1, \alpha, \alpha^2$ is also a

basis over $\mathbb{F}_{p^k}$ for $\mathbb{F}_{p^{3k}}$. This gives us a very useful representation of $\mathbb{F}_{p^k}^3$. Multiplication by α on $\mathbb{F}_{p^{3k}}$ induces a projective transformation over $\mathbb{F}_{p^k}$, and if we call this transformation T, $T(\alpha^r) = \alpha^{r+1}$, and so T is a cyclic transformation of the points of this vector space. To show that T is also a cyclic transformation on the lines of projective space, I use a trick related to me 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 $\beta^{-1}(\ker L)$. Since a linear functional is described by its kernel, and the value at one point off the kernel, and since the linear functionals of a finite field are all of form L_β, we see that the planes of this vector space (through the origin) are cyclically permuted among each other by T, and therefore so are the lines of the induced projective space.

This example shows that the complete resolution of the polynomial conjecture will require additional study on the nature of the fields $\Omega_{k-\lambda}$.

Section IV - Analysis of the Polynomial Conjecture When All Polynomials Are Quadratic

Let I be the multiplicative group of non-zero integers modulo the non-zero square integers. Let $\langle -1,1 \rangle$ denote the multiplicative group of two elements, and $\mathbb{F}_2$ the field of two elements.

Lemma A - Let $b_1, \cdots, b_n$ be distinct elements of I. Let $q_1, \cdots, q_s$ be the set of primes that appear in at least one of the b_i, $i = 1, \cdots, n$. There exists a homomorphism $\phi : I \to \langle -1,1 \rangle$ such that $\phi(p) = 1$ if p is a prime not among $q_1, \cdots, q_s$ and $\phi(b_i) = -1$ for $i = 1, \cdots, n$ if and only if; there exists no product consisting of an odd number of distinct b_i's, such that $\prod_{j=1}^{2\ell+1} b_{i_j} \equiv 1$.

Proof -

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

$$(a) \qquad \sum_{j=1}^{s} a_i(j) x_j = 1 \qquad i = 1, \cdots, n$$

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 the equations (a) have $(x_1, \cdots, x_s)$, then $\phi(b_i) = (-1)^{\sum a_i(j) x_j} = -1$. Conversely, if the desired ϕ of the lemma exists, there is a solution vector $(x_1, \cdots, x_s) \in \mathbb{F}_2^s$. A solution vector for (a) exists if and only if:

$$\text{rank} \left| a_i(j) \right| = \text{rank} \left| a_i(j) \;\vdots\; \right| .$$

If there exists a relation over $\mathbb{F}_2$ among the rows of $a_1(j)$ this relation may be expressed as

$$(a_{k_1}(1), \cdots, a_{k_1}(s)) + \cdots + (a_{k_t}(1), \cdots, a_{k_t}(s)) = (0, \cdots, 0).$$

The rank of the two matrices is therefore the same if and only if every relation of this form has t even. The relation is equivalent to $b_{k_1} \cdots b_{k_t} \equiv 1$.

Q. E. D.

Corollary A - Let $b_1, \cdots, b_n$ be a set of distinct square-free integers. There exists an arithmetic progression A of primes p such that b_i, $i = 1, \cdots, n$, 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 $\prod_{j=1}^{2\ell+1} b_{i_j}$ is a square, then for all primes

different from $q_1, \cdots, q_s$ (set of primes appearing in the b_i's, $i = 1, \cdots, n$)

$\left(\frac{b_{ij}}{p}\right) = -1$ implies $\left(\prod_{j=1}^{2k+1} \frac{b_{ij}}{p}\right) = -1$, which 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 $\phi : I \to \{-1, 1\}$ such that $\phi(b_i) = -1$ for $i = 1, \cdots, n$. If we can find an arithmetic progression A of primes p such that $\left(\frac{q_j}{p}\right) = \phi(q_j)$ for $j = 1, \cdots, s$, then we have $\left(\frac{b_i}{p}\right) = -1$ for $i = 1, \cdots, n$. Since ϕ was defined on all primes, we may without loss assume $q_1 = -1$, and $q_2 = 2$. We try to find an integer x^* such that primes p satisfying $p \equiv x^* \bmod 8\, q_3 \cdots q_s$ form an arithmetic progression satisfying our requirements.

Let $x^* \equiv x_0 \bmod 8$ so that $\left(\frac{-1}{p}\right) = \phi(-1)$, $\left(\frac{2}{p}\right) = \phi(2)$. For $j = 3, \cdots, s$;

$$\left(\frac{q_j}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q_j - 1}{2}} \left(\frac{p}{q_j}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q_j - 1}{2}} \left(\frac{x^*}{q_j}\right) .$$

Choose $x^* \equiv$ residue or non-residue mod q_j so as to satisfy $(-1)^{\frac{p-1}{2} \cdot \frac{q_j - 1}{2}} \left(\frac{x^*}{q_j}\right) = \phi(q_j)$. By the Chinese remainder theorem there exists an x^* satisfying these congruences simultaneously.

Q. E. D.

Lemma B - (Extension of Lemma A)

Let $B_1 = \{b_1, \cdots, b_{n_1}\}$, $B_2 = \{b_{n_1+1}, \cdots, b_{n_2}\}$, $\cdots$, $B_k = \{b_{n_{k-1}+1}, \cdots, b_{n_k}\}$ be disjoint sets of elements of I. There exists a homomorphism $\phi : I \to \{-1,1\}$ such that $\phi(b_1) = \cdots = \phi(b_{n_1}) = -1$, and $\phi(b_{n_i+1}) = \cdots = \phi(b_{n_{i+1}})$ (5) for $i = 1, \cdots, k-1$ if and only if there exists a subcollection $B_1, B_{i_1}, \cdots, B_{i_t}$ with $2 \leq i_1 < \cdots < i_t \leq k$ such that when a product $\prod_{j=1}^{\mu} b_{i_j} \equiv 1$ (where b_{i_j} are distinct) then the total number of b_{i_j}'s , $j = 1, \cdots, \mu$ in the union of $B_1, B_{i_1}, \cdots, B_{i_t}$ is even.

Proof -

As in Lemma A consider the set $q_1, \cdots, q_s$ of primes that appear in at least one of $b_1, \cdots, b_{n_k}$. Let $L_i = \sum_{j=1}^{s} a_i(j)x_j$ where again

$$a_i(j) = \begin{cases} 0 \text{ if } q_j \text{ does not appear in } b_i \\ 1 \text{ if } q_j \text{ does appear in } b_i \end{cases}$$

---

[5] We have not specified the sign in the expression $\phi(b_{n_i+1}) = \cdots = \phi(b_{n_{i+1}})$ for $i = 1, \cdots, k-1$.

ϕ exists if and only if we can find $\epsilon_i = 0$ or 1 for $l = 2, \cdots, k$ such that the linear equations

$$L_1 = \cdots = L_{n_1} = 1, \; L_{n_1+1} = \cdots = L_{n_2} = \epsilon_2, \cdots, L_{n_k} = \epsilon_k$$

have the rank of their coefficient matrix equal to the rank of their augmented matrix.

If $(a_{\ell_1}(1), \cdots, a_{\ell_1}(s)) + (a_{\ell_2}(1), \cdots, a_{\ell_2}(s)) + \cdots + (a_{\ell_v}(1), \cdots, a_{\ell_v}(s)) = (0, \cdots, 0)$ is a relation among the rows of the coefficient matrix, then the augmented matrix will have higher rank unless the sum of the ϵ_{ℓ_i}'s, including repetitions, is even. Here $\epsilon_\ell = 1$ corresponds to $L_i = 1$ for $i = 1, \cdots, n_1$.

Q. E. D.

Theorem A - Let $h, g_1, \cdots, g_\ell$ be quadratic polynomials $\in \mathbb{Z}[x]$. Assume $V_p(h) \subset \bigcup_i V_p(g_i)$ for a.a.p. Without loss we may assume $h = ax^2 + c$, $g_i(x) = a_i x^2 + c_i$ $(i = 1, \cdots, \ell)$ with $a, a_1, \cdots, a_\ell$ all square free.(6) Assume for $i = 1, \cdots, n_1$ that $c_i = c$ and for $i > n_1$, $c_i \neq c$. For $i > n_1$, further divide up the c_i's into classes

---

6To get the normalized forms $ax^2 + c$ we complete the square on the polynomials $h, g_1, \cdots, g_\ell$. This may result in polynomials whose coefficients are not in $\mathbb{Z}$. In this case, multiply all polynomials by some one constant to put them back in $\mathbb{Z}[x]$. This will change their value sets for at most finitely many primes.

such that $c_{n_1+1} = \cdots = c_{n_2}, c_{n_2+1} = \cdots = c_{n_3}$,

$c_{n_{k-1}+1} = \cdots = c_{n_k}$. Let $b_i = aa_i$, $i = 1, \cdots, \ell$,

and $B_r = \{b_{n_{r-1}+1}, \cdots, b_{n_r}\}$, $r = 1, \cdots, k$.

Then we conclude that for each subset of indices $(i_1, \cdots, i_T)$ with $2 \leq i_1 < \cdots < i_T \leq k$ there exists some product of distinct b_i's, $\prod_{j=1}^{u} b_{i_j} \equiv 1$ mod squares such that the total number of b_i's in the product that are in the union of $B_1, B_{i_1}, \cdots, B_{i_T}$ is odd.

Proof -

With no loss we may assume that each B_i consists of distinct elements. Assume there exists a subset of indices $(i_1, \cdots, i_T)$ with $= 2 \leq i_1 < \cdots < i_T \leq k$ such that for every product of distinct b_i's, $\prod_{j=1}^{u} b_{i_j} \equiv 1$ mod squares, the total number of b_i's in the product, that are in one of $B_1, B_{i_1}, \cdots, B_{i_T}$ 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 $i = 1, \cdots, \ell$. Since this would contradict the hypothesis, our conclusion must hold.

Let $q_1, \cdots, q_s$ be the primes which appear in $b_1, \cdots, b_\ell$ (including without loss $q_1 = -1$, $q_2 = 2$). Let ϕ be the homomorphism given by Lemma B such that

$$\Phi(b_1) = \cdots = \Phi(b_{n_1}) = -1\ ,\ \Phi(b_{n_1+1}) = \cdots = \Phi(b_{n_2})\ ,$$
$$\cdots\ ,\ \Phi(b_{n_{k-1}+1}) = \cdots = \Phi(b_{n_k}).$$

In a manner similar to that of corollary A we can find an arithmetic progression of primes p (call this A.P. A^*) such that $p \equiv x^* \bmod 8\, q_3 \cdots q_s$ for some integer x^*, and $\left(\frac{b_1}{p}\right) = \cdots = \left(\frac{b_{n_1}}{p}\right) = -1\ ,\ \left(\frac{b_{n_1+1}}{p}\right) = \cdots = \left(\frac{b_{n_2}}{p}\right)\ ,$
$\left(\frac{b_{n_{k-1}+1}}{p}\right) = \cdots = \left(\frac{b_{n_k}}{p}\right)$.

Let $p_1, \cdots, p_k$ be distinct primes larger than both $|a \cdot 8 \cdot q_3 \cdots q_s|$ and $\max_{\nu,\gamma} (|C_{n_\nu} - C_{n_\gamma}|)$. By the Chinese remainder theorem there exists an integer such that $C_{n_i} - \lambda \equiv p_i \bmod p_i^2$. For $j \neq i$, $p_j \nmid (C_{n_i} - \lambda)$ because $p_j \nmid (C_{n_i} - C_{n_j})$.

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

$$p \equiv x^* \bmod \left[8(q_3 \cdots q_s)(C_{n_1} - \lambda/p_1) \cdots (C_{n_k} - \lambda/p_k)\right]$$

$$p \equiv m_1 \bmod p_1 \quad \text{for} \quad i = 1, \cdots, k,$$

where m_1 is chosen so that

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

For p satisfying $p \equiv x^* \bmod \left[8 \cdot q_3 \cdots q_s (C_{n_1} - \lambda/p_1) \cdots (C_{n_k} - \lambda/p_k)\right]$ the values of $\left(\frac{a_{n_i}}{p}\right)$ and $\left(\frac{C_{n_i} - \lambda/p_i}{p}\right)$ and $(-1)^{\frac{p_i-1}{2}}$ are determined by the congruence alone.

Since $\left(\frac{a}{p}\right)\left(\frac{a_i}{p}\right) = \left(\frac{b_i}{p}\right) = -1$ for $i = 1, \cdots, n$, and $p \in A^{**}$, we conclude that $\left(\frac{a}{p}\right)\left(\frac{c-\lambda}{p}\right) = 1$,

$$\left(\frac{a_{n_i}}{p}\right)\left(\frac{c_{n_i}-\lambda}{p}\right) = -1 = \left(\frac{a_{n_{i-1}+1}}{p}\right)\left(\frac{c_{n_i}-\lambda}{p}\right) .$$

for $i = 1, \cdots, k$.

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

Q. E. D.

Corollary B - If $h, g_1, \cdots, g_\ell$ are quadratic polynomials such that $V_p(h) \subset \bigcup_1^\ell V_p(g_i)$ for a.a.p. Then, with the notation of the Theorem above, $c_i = c$ for some i.

Proof -

If $c_i \neq c$ for $i = 1, \cdots, \ell$, then B_1 is the empty set, and we apply the Theorem with the empty set of indices, to conclude that in any relation $\prod_{j=1}^{M} b_{ij} \equiv 1 \bmod$ squares, the total number of b_{ij}'s in B_1 is even (since 0 is even).

Q. E. D.

Clearly the criteria of Theorem A to test for the hypothesis of the polynomial conjecture is one which may be verified in a finite number of steps.

BIBLIOGRAPHY

1. R. Carmichael. Groups of Finite Order, Dover Publications, New York (1937).

2. H. Davenport, D. Lewis and A. Schinzel [1]. "Equations of the Form $f(x) = g(y)$," Quarterly J. Math., Oxford (2), Vol. 12 (1961), 304-312.

3. H. Davenport, D. Lewis and A. Schinzel [2]. "Polynomials of Certain Special Types," Acta Arithmetica, Vol. IX (1964), 108-116.

4. H. Hasse. Bericht uber neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkorper, Teil I and II, Physica-Verlag (1965).

5. D. Hilbert. "Uber die Irreduzibilitat Ganzer Rationaler Functionen mit Ganzzahligen Koeffizienten," Journal f. reine und Angew. Math., Bd. 110, s. 104-129 (1892).

6. N. Jacobson. Lectures in Abstract Algebra, Vol. III, D. Van Nostrand Company, Toronto (1963).

7. S. Lang. Diophontine Geometry, Interscience tracts in Pure and Applied Mathematics, New York (1964).

8. J. Ritt. "Prime and Composite Polynomials," Transactions of the American Mathematical Society, Vol. 23 (1922), 51-66.

9. A. Schinzel. "On a Theorem of Bauer and Some of Its Applications," Acta Arithmetica, Vol. XI (1966), 333-344.

10. R. Walker. Algebraic Curves, Dover Publications, New York (1950).