Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 6, No. 3, June 1974
Printed in Belgium

On Hilbert's Irreducibility Theorem

MICHAEL FRIED*

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48104

Communicated by H. Zassenhaus

Received December 28, 1971; revised November 10, 1973

A method for obtaining very precise results along the lines of the Hilbert Irreducibility Theorem is described and then applied to a special case. In addition, the relationship of the irreducibility theorem to other tools of diophantine analysis is investigated. In particular, we give a proof of the irreducibility theorem that uses only Noether's lemma and the fact that an absolutely irreducible curve has a rational point over a finite field of large order.

In this paper we treat problems related to several aspects of Hilbert's irreducibility theorem. Let L be a number field with ring of integers $\mathfrak{o}_L$. Let $f(x, y) \in L[x, y]$ be an irreducible polynomial in two variables. Then Hilbert's theorem states that there exists an infinite number of specializations of the variable x to $x_0 \in \mathfrak{o}_L$ such that $f(x_0, y)$ is an irreducible polynomial in one variable over L. In fact, using the techniques of Section 1 (or of [12, Section 5]) it can be shown that the set of $x_0 \in \mathfrak{o}_L$ for which $f(x_0, y)$ is reducible over L and for which the maximum of the absolute values of the conjugates of x_0 is less than N has cardinality bounded by $c \cdot N^{1/2}$ where c is a constant independent of N (dependent only on f and L). In the notation of Section 1, we write

$$| R(f, \mathfrak{o}_L, N)| < c \cdot N^{1/2}.$$

In addition, there exist constants $c_1, c_2 > 0$, and an integer l for which either

(0.1) $c_2 \cdot N^{1/l} < | R(f, \mathfrak{o}_L, N)| < c_1 \cdot N^{1/l}$, or

(0.2) $c_2 \cdot (\log N)^l < | R(f, \mathfrak{o}_L, N)| < c_1 \cdot (\log N)^l$, or

(0.3) $| R(f, \mathfrak{o}_L, N)|$ is bounded as a function of N.

* Author's address for 1973–74: Department of Mathematics, State University of New York at Stony Brook, Stony Brook, New York 11790.

We say that: $R(f, \mathfrak{o}_L)$ (as in Section 1) has *exponential density* in Case (0.1); and $R(f, \mathfrak{o}_L)$ has *logarithmic density* in Case (0.2).

The results of Section 1 are primarily concerned with the case when

(0.4) $L = \mathbf{Q}$, and

(0.5) $f(x, y) = h(y) - x$ for $h(y) \in \mathbf{Q}[y]$.

For $g \in \mathbf{Q}(y)$ we define $V(g, \mathbf{Z})$ to be the intersection of $\mathbf{Z}$ and the image of g on $\mathbf{Q}$. Clearly, $V(h, \mathbf{Z}) \subseteq R(h(y) - x, \mathbf{Z})$. Let $S(h, \mathbf{Z})$ be $R(h(y) - x, \mathbf{Z}) - V(h, \mathbf{Z})$. In Theorem 1 we show that $S(h, \mathbf{Z})$ is $\bigcup_{i=1}^{l} V(g_i, \mathbf{Z}) \cup \overline{V}$ where $\overline{V}$ is a finite set, and $g_1, \ldots, g_l$ are rational functions satisfying certain conditions (see Corollary 2). From this we deduce (Corollary 1) that $S(h, \mathbf{Z})$ is finite or has logarithmic density if either

(0.6) $\deg h$ is an odd prime-power, or

(0.7) h is an indecomposable polynomial (h is not a functional composition of two polynomials of lower degree).

Of course, we are most interested in finding out when $S(h, \mathbf{Z})$ is finite. From Corollary 2 we obtain Corollary 3; $S(h, \mathbf{Z})$ is finite if $\deg h = p$ is a prime for which $2p - 1$ is not a square. Corollary 3 uses a result of Wielandt, which is probably far from definitive. In particular, results of Feit and Scott [16] may be applied to show that $S(h, \mathbf{Z})$ is finite if $\deg h = p$ is a prime with $5 < p < 333$. The case $p = 5$ is exceptional, as we explain in example 2. In fact, $p = 5$ is the only known case of a prime for which $S(h, Z)$ is infinite with $\deg h = p$.

For L a number field different from $\mathbf{Q}$, there may exist indecomposable polynomials h, defined over L, of degree n for which $S(h, \mathfrak{o}_L)$ has exponential density. In such cases, $L \cap \mathbf{Q}(\zeta_n) \neq \mathbf{Q}$ (where ζ_n is a primitive n-th root of 1). Such examples are discussed in [10, Section VI], and it is suspected that these examples of degree 7, 11, 13, 15, 21, and 31 are the only such examples. These examples are the source of much additional number theory anomaly. For $h \in L[y]$ let $V_{\mathfrak{p}}(h)$ be the values assumed by h modulo the prime ideal $\mathfrak{p}$ of $\mathfrak{o}_L$ (as in Section 2). Consider pairs of polynomials $h, g \in L[y]$ for which $V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$ for all but a finite number of primes $\mathfrak{p}$ (a.a. $\mathfrak{p}$). When $g(y) = h(ay + b)$ for constants $a, b \in L$ (h, g are *linearly related*) it is easy to see that $V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$ for a.a. $\mathfrak{p}$. As an application of the theory of Section 2 we show that the indecomposable polynomials h for which $S(h, \mathfrak{o}_L)$ has exponential density are *exactly* the indecomposable polynomials for which there exists $g \in L[y]$ where h, g are *not* linearly related, and $V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$ for a.a. $\mathfrak{p}$.

In particular, (Theorem 2) for $h \in \mathbf{Q}[y]$ satisfying (0.6) or (0.7) if $V_p(h) = V_p(g)$ for a.a. $\mathfrak{p}$, then h and g are linearly related (i.e., h is determined by its value sets modulo p).

Let P be an elementary statement (general diophantine problem) involving polynomials with coefficients in $\mathfrak{o}_L$. Section 2 develops some of the tools for a primitive recursive procedure for deciding

(*) whether the reduction modulo $\mathfrak{p}$ of P is true for a.a. $\mathfrak{p}$. These tools include a non-regular analogue of the Cebotarev density theorem for function fields over finite fields, (generalizing results of S. Cohen [4] and S. Lang [19]) and a precise form of Noether's lemma. Ax [1] showed there is a decision procedure for deciding (*), but, as his technique utilized ultra-products and logic, the procedure is not primitive recursive. Combining the method of Section 2 with a generalization of Bertini's theorem (generalizing further still the statement of [10, Section II.2] for algebraic pencils) we can give an inductive argument completing our procedure. This argument will appear in a later paper.

In [5] we gave a rough, but useful, procedure for investigating (*). One of the essential tools used there was Hilbert's irreducibility theorem. Hilbert's theorem also played a role in the related matters discussed in Jarden's paper [11]. Therefore, we show in Theorem 3 that the purely algebraic methods of Section 2 yield a proof of the irreducibility theorem. In fact, Hilbert's theorem is roughly a consequence of Noether's lemma and the fact that an absolutely irreducible curve over a finite field has rational points if the order of the finite field is "large." This latter fact is a consequence of the celebrated Riemann hypothesis for curves over finite fields, which has finally been demonstrated to be of a reasonably elementary nature (see [2]).

Andrej Schinzel has greatly influenced the author through his contributions to the problems considered here. In addition, we would like to thank Jack MacLaughlin for discussions concerning the group theoretical literature related to Corollary 2.

The author's correspondence indicates confusion as to which of the announced items in [7] this paper corresponds. Families of Riemann surfaces (I) has been broken up into three (expanded) papers: this one; [9] (upon which the proofs of Corollary 1 and 2 depend); and the partly expository paper [10].

The reader might view the juxtaposition of the results of this paper as gravy on one's frosting (both appealing, but not during the same course). We hope, nevertheless, that we have exposed some apposite aspects of Hilbert's famous theorem, thereby placing it in a more general Diophantine context.

1. Hilbert's Irreducibility Theorem

Let L be an algebraic number field, finite dimensional over $\mathbf{Q}$. Let L^* be a fixed algebraic closure of L. We denote by $\mathfrak{o}_L$ the ring of integers of L. For $h(y) \in L(y)$, let

$R(h(y) - x, \mathfrak{o}_L) = \{x_0 \in \mathfrak{o}_L \mid h(y) - x_0$ is reducible over $L\}$ (alternatively, $R(h, \mathfrak{o}_L)$),

$W(h, \mathfrak{o}_L) = \{x_0 \in \mathfrak{o}_L \mid h(y) - x_0$ has, at least, 3 irreducible factors over $L\}$, and

$V(h, \mathfrak{o}_L) = \{x_0 \in \mathfrak{o}_L \mid h(y) - x_0$ has a zero in $L\}$.

Certainly, we have $V(h, \mathfrak{o}_L) \subset R(h(y) - x, \mathfrak{o}_L)$. However, a more complete description of $R(h, \mathfrak{o}_L)$ can be given. For simplicity we restrict ourselves to the case where h is a polynomial. Consider $g \in L(y)$ where $g = g_1(y)/g_2(y)$ with g_1, g_2 relatively prime polynomials. We have need for the following conditions:

(1.1) $\Omega_{h-x} = \Omega_{g-x}$, where Ω_{h-x} is the splitting field of $h(y) - x$ over $L(x)$;

(1.2) $g_2(z) \cdot (h(y) - g(z))$ is a reducible polynomial in two variables over L (we say $h(y) - g(z)$ is reducible); and

(1.3) either $g_2(y)$ is constant; or $g_2(y)$ is a power of a linear polynomial and $\deg g_1 \geqslant \deg g_2$; or $g_2(y)$ is a power of an irreducible quadratic polynomial and $\deg g_1 = \deg g_2$.

Definition 1. Let $f(y) \in L(y)$. We say $f(y)$ is decomposable over L if $f(y) = f^{(1)}(f^{(2)}(y))$ where $\deg f^{(i)}(y) > 1$ for $i = 1, 2$. Otherwise, we say $f(y)$ is indecomposable over L. If $f(y)$ is written as a ratio $f_1(y)/f_2(y)$ of relatively prime polynomials, then $\deg f$ is the integer $\max(\deg f_1, \deg f_2)$.

Definition 2. Let $f(y), g(y) \in L(y)$. We say that f and g are linearly related if $f((ay + b)/(cy + d)) = g(y)$ for some $a, b, c, d \in L$. We say that f is composite with g if there exists $r(y) \in L(y)$ such that $g(r(y)) = f(y)$.

We remind the reader of the definitions of the: *cyclic* polynomial of degree n, $h(y) = ay^n + b$, $a, b \in L$; and the *Chebychev* polynomial of degree n, $h(y) = 2^{-n-1}\{(y + (y^2 + 4)^{1/2})^n + (y - (y^2 + 4)^{1/2})^n\}$.

The next proposition is proved in ([9], Theorem 1) and it is the technical basis on which the results of this paper depend.

PROPOSITION 1. *Let* $h(y) \in L(y)$. *Suppose* $\bar{g}(y) = (\bar{g}_1/\bar{g}_2) \in L(y)$ *with* $\bar{g}_1, \bar{g}_2$ *relatively prime polynomials. Assume that* $\bar{g}_2(z) \cdot (h(y) - \bar{g}(z))$ *is reducible as a polynomial in two variables. Assume also that if* $h = h_1(h_2(y))$ *with* $h_1, h_2 \in L[y]$ *and* $\deg h_1, \deg h_2 > 1$, *then* $\bar{g}_2(z) \cdot (h_1(y) - \bar{g}(z))$ *is not reducible. Then there exists* $g(y) \in L(y)$ *such that* $g(g_2(y)) = \bar{g}(y)$ *for some* $g_2(y)$ *in* $L(y)$ *and* (1.1) *and* (1.2) *hold.*

Suppose in addition that h, g *are polynomials and* h *is indecomposable. Assume that* $h(y) - g(z) = \prod_1^t \varphi_i(y, z)$ *with* $t > 1$ *where* $\varphi_i(x, y)$ *are absolutely irreducible polynomials (irreducible over* L^**). Then*:

(1.4) $\deg g = \deg h = n$, *and* $g(y)$ *is indecomposable*; *and*

(1.5) $t = 2$ (*so that* $h(y) - g(z)$ *has exactly two irreducible factors*) *unless* h *and* g *are both linearly related to a cyclic or Chebychev polynomial* ([6], p. 41).

Let ζ_n *be a primitive n-th root of* 1. *Assume that* $L \cap \mathbf{Q}(\zeta_n) \subset M$, *where* M *is the totally real subfield of* $\mathbf{Q}(\zeta_n)$. *Then* h *and* g *must be linearly related.*

THEOREM 1. *Let* $h(y) \in L[y]$. *Then we have*

$$R(h, \mathfrak{o}_L) = \left(\bigcup_{i=1}^{l} V(g(i), \mathfrak{o}_L) \right) \cup V(h, \mathfrak{o}_L) \cup \overline{V}, \tag{1.6}$$

where $\overline{V}$ *is a finite set, and* $h, g(1, y), \ldots, g(l, y)$ *are a maximal set of rational functions for which no function is composite with another*; *and*

$$\Omega_{h-x} \supset \Omega_{g(i,y)-x}, \quad h(y) - g(i, z)$$

is reducible (as in (1.2)), *and* $g(i, y)$ *satisfies* (1.3) *for* $i = 1, \ldots, r$.

If we assume in addition that h *is an indecomposable polynomial that is neither cyclic nor Chebychev, then we have*

$$W(h, \mathfrak{o}_L) \subseteq \left(\bigcup_{j=1}^{t} V(g(\beta(j)), \mathfrak{o}_L) \right) \cup \overline{\overline{V}} \tag{1.7}$$

where $\overline{\overline{V}}$ *is a finite set, and* $g(\beta(1), y), \ldots, g(\beta(t), y)$ *is the subset of* $g(1, y), \ldots, g(l, y)$ *consisting of the non-polynomials.*

Proof. Factor $h(y) - x$ over an algebraically closed extension of $L(x)$ to obtain

$$h(y) - x = c \prod_{i=1}^{n} (y - y_i), \qquad \text{for some constant } c.$$

If we fix determinations of the algebraic functions $y_1,\ldots, y_n$, then for $x_0 \in \mathfrak{o}_L$ we may associate values $y_i(x_0)$ to these functions. Let $M \cup N = \{1, 2,\ldots, n\}$ denote a partition of the integers from 1 to n into disjoint non-empty sets.

Suppose $c \cdot \prod_{i\in M}(y - y_i(x_0)) \in \mathfrak{o}_L[y]$ for infinitely many $x_0 \in \mathfrak{o}_L$. Consider the curve $\mathscr{C}_M$ which has a generic point given by

$$\xi^{(M)} = \left(x, \sum_{i\in M} y_i, \sum_{\substack{i<j \\ i,j\in M}} y_i y_j,\ldots, \prod_{i\in M} y_i\right), \text{ or}$$

$$\xi^{(M)} = (x, \xi_1^{(M)},\ldots, \xi_m^{(M)}), \text{ where } m \text{ is the order of } M.$$

This curve has infinitely many points whose coordinates are in $\mathfrak{o}_L$. By a theorem of Siegel's ([14], p. 51) this implies that $\mathscr{C}_M$ is of genus zero. Therefore, the function field for $\mathscr{C}_M$ is $L(x, \xi_1^{(M)},\ldots, \xi_m^{(M)}) = L(z)$ for some transcendental function z.

Thus, x is a rational function of z (say $x = g^{(M)}(z)$). If $f_u^{(M)}(z) = \xi_u^{(M)}$, then

$$c \cdot \prod_{i\in M}(y - y_i) = \sum f_u^{(M)}(z)\, y^{m-u}.$$

Therefore $h(y) - g^{(M)}(z)$ is reducible and $\Omega_{g^{(M)}-x} \subset \Omega_{h-x}$ (because $L(z) \subset \Omega_{h-x}$).

It is a consequence of the Thue–Siegel–Roth Theorem ([13], p. 159) that if $g^{(M)}(z)$ takes on infinitely many quasi-integral values for arguments in L, then the curve $g^{(M)}(z) - x = 0$ has at most two places over the place $x = 0$. By a linear fractional change of the variable z we may assume that (1.3) holds. See the discussion of [10, Section II.3, Remark 1]. From the collection $g^{(M)}(y)$ as M runs over partitions (as above), we select a maximal subset $g(1, y),\ldots, g(l, y)$ such that

$$\bigcup_M V(g^{(M)}(y), \mathfrak{o}_L) = \left(\bigcup V(h, \mathfrak{o}_L)\right) \cup \left(\bigcup_{i=1}^{l} V(g(i, y), \mathfrak{o}_L)\right)$$

and no rational function in the set is composite with another. This concludes the proof of the first part of the theorem.

Now assume h is indecomposable. The process above shows that

$$W_h \subset \bigcup_{j=1}^{t} (V(g(\beta(j)), \mathfrak{o}_L)) \cup \overline{V}$$

where $h(y) - g(\beta(j), z)$ has at least three irreducible factors. Since h is indecomposable, Proposition 1 (expression (1.5)) shows that $g(\beta(j), z)$ cannot be a polynomial unless h is a cyclic or Chebychev polynomial.

As in the introduction, we define $S(h, \mathfrak{o}_L)$ to be $R(h, \mathfrak{o}_L) - V(h, \mathfrak{o}_L)$. For each positive real number N we let $S(h, \mathfrak{o}_L, N)$ be the set of $x_0 \in S(h, \mathfrak{o}_L)$ for which the maximum of the absolute values of the conjugates of x_0 is less than N. As in expressions (0.1) and (0.2) with $R(h, \mathfrak{o}_L, N)$ replaced by $S(h, \mathfrak{o}_L, N)$ we speak of: $S(h, \mathfrak{o}_L)$ as having *exponential density* if

$$c_2 \cdot N^{1/l} < |S(h, \mathfrak{o}_L, N)| < c_1 \cdot N^{1/l}$$

for some constants $c_1, c_2 > 0$, and integer l; or $S(h, \mathfrak{o}_L)$ as having *logarithmic density* if

$$c_2 \cdot (\log N)^l < |S(h, \mathfrak{o}_L, N)| < c_1 \cdot (\log N)^l.$$

Consider $V(g, \mathfrak{o}_L)$ for g satisfying one of the conditions in (1.3). It is easy to see that if $g(y)$ is a non-constant polynomial, then there exist constants $c_1, c_2 > 0$ such that

$$c_2 N^{1/\deg g} < |V(g, \mathfrak{o}_L, N)| < c_1 N^{1/\deg g}.$$

In the case that $g_2(y)$ is a power of an irreducible quadratic polynomial over L, let L' be the field obtained by adjoining the zeros of $g_2(y)$ to L. If $g_2(y)$ is not constant and $V(g, \mathfrak{o}_L)$ is not finite, then there exist constants $c_1, c_2 > 0$ such that

$$c_2(\log N)^l < |V(g, \mathfrak{o}_L, N)| < c_1 (\log N)^l$$

where l is the rank of the units in $\mathfrak{o}_L$ if $g_2(y)$ is a power of a linear polynomial, and l is the rank of the units in $\mathfrak{o}_{L'}$ if $g_2(y)$ is a power of an irreducible quadratic polynomial. In the former case, this follows from the fact that $g_1(y)/y^k$ with $k > 0$ takes on values in a fixed fractional ideal only for values of y in finitely many cosets of the units of $\mathfrak{o}_L$ in L (see [14] or [13, p. 159]). In the latter case we reduce to the former case by considering a linear fractional change of the variable y over L' sending the two distinct zeros of $g_2(y)$ to 0 and ∞, respectively. ∎

COROLLARY 1. *Let $h(y) \in \mathbf{Q}[y]$ be such that either h is an indecomposable polynomial (condition (0.7)) or* deg *h is an odd prime-power (condition (0.6)). Then, either $S(h, \mathbf{Z})$ is finite or $S(h, \mathbf{Z})$ has logarithmic density.*

Proof. From the remarks above this will follow if we show that among the rational functions $g(1, y), \ldots, g(l, y)$ satisfying (1.3) as in the conclusion of Theorem 1, there are no polynomials. For the case (0.6) this was demonstrated in [7]. However, we note that it was incorrectly concluded there that $S(h, \mathbf{Z})$ must be finite. For the case (0.7) this follows from

Proposition 1. In fact, if $g(1, y)$ (say) is a polynomial, since $h(y) - g(1, z)$ is reducible, Proposition 1 contradicts the fact that h and g are defined over $\mathbf{Q}$. ∎

We need some additional notation from group theory. Let G be a finite group with a faithful, transitive permutation representation T. This consists of an embedding $T : G \to S_n$ where S_n is the symmetric group on n letters and the image of G is a transitive group. We say that T has degree n. The groups $G(T, 1),..., G(T, n)$ are the subgroups of G that stabilize a letter. We obtain an equivalence class of permutation representations by considering the collection $T^\alpha : G \to S_n$, $\alpha \in S_n$ where $T^\alpha(\sigma) = \alpha \cdot T(\sigma) \cdot \alpha^{-1}$ for $\sigma \in G$. For $\sigma \in G$, write $T(\sigma) = \prod_{j=1}^{u} \beta(\sigma, j)$ as a product of disjoint cycles in S_n, where $|\beta(\sigma, j)| = s(j)$ denotes the order of $\beta(\sigma, j)$. By abuse, we sometimes write $T(\sigma) = (s(1),..., s(u))$. Then $\mathrm{ind}(T(\sigma))$ (called the index of σ) is the sum $\sum_{j=1}^{u} (|\beta(\sigma, j)| - 1)$. Let $\sigma(1),..., \sigma(r) \in G$ be such that $\prod_{i=1}^{r} \sigma(i) = \mathrm{Id}$. Then $g(\sigma(1),..., \sigma(r))$ (called the genus of the r-tuple $(\sigma(1),..., \sigma(r))$) is computed from

(1.8) $2(n + g(\sigma(1),..., \sigma(r)) - 1) = \sum_{i=1}^{r} \mathrm{ind}(T(\sigma(i)))$ (the Riemann–Hurwitz formula).

COROLLARY 2. *Let $h \in \mathbf{Q}[y]$ be an indecomposable polynomial. Assume that $S(h, \mathbf{Z})$ is infinite. Then, the group $G(\Omega_{h-x}/\mathbf{Q}(x))$ has two faithful transitive permutation representations T_1 and T_2 having the following properties*:

(1.9) *T_1 is a doubly transitive representation of degree $n = \deg h$;*

(1.10) *T_2 is a representation of degree $2n$ which is not doubly transitive; there exist generators $\sigma(1),..., \sigma(r)$ of $G(\mathbf{Q}^* \cdot \Omega_{h-x}/\mathbf{Q}^*(x))$ for which $\prod_{i=1}^{r} \sigma(i) = \mathrm{Id}$.;*

(1.11) *$T_1(\sigma(r)) = (n)$(an n-cycle) and $T_2(\sigma(r)) = (n)(n)$ the product of two n-cycles);*

(1.12) (a) $\sum_{i=1}^{r} \mathrm{ind}\ T_1(\sigma(i)) = 2(n - 1)$,
(b) $\sum_{i=1}^{r} \mathrm{ind}\ T_2(\sigma(i)) = 2(2n - 1)$: *and*

(1.13) (a) *$G(T_1, 1)$ contains none of the groups $G(T_2, 1),..., G(T_2, 2n)$,*
(b) *the restriction of T_2 to $G(T_1, 1)$ is an intransitive group.*

Proof. Since h is indecomposable and $S(h, \mathbf{Z})$ is infinite, Corollary 1 (with the remarks preceeding it) implies that

$$S(h, \mathbf{Z}) \subseteq \left(\bigcup_{j=1}^{t} V(g(\beta(j)), Z) \right) \cup \overline{V}$$

(as in expression (1.7)) where $g(\beta(1)),\ldots, g(\beta(t))$ are the rational functions in the list $g(1),\ldots, g(l)$ (expression (1.6)) satisfying the third of the three conditions of (1.3). Let $g(\beta(1), y)$ be denoted henceforth as $g(y)$. Using the fact that h is indecomposable, Proposition 1 implies that $\Omega_{h-x} = \Omega_{g-x}$. We remind the reader that h is not composite with g (from Theorem 1).

Let $y_1,\ldots, y_n$ be the zeros of $h(y) - x$; $z_1,\ldots, z_m$ the zeros of $g(z) - x$. Consider the representations T_1 (respectively T_2) obtained from the action of $G(\Omega_{h-x}/\mathbf{Q}(x))$ on $y_1,\ldots, y_n$ (respectively, $z_1,\ldots, z_m$). Let

$$\sigma(1),\ldots, \sigma(r) \in G(\mathbf{Q}^* \cdot \Omega_{h-x}/\mathbf{Q}^*(x))$$

be a description of the branch cycles for the field extension $\mathbf{Q}^* \cdot \Omega_{h-x}/\mathbf{Q}^*(x)$ (as in [6], say). Thus, $\sigma(1),\ldots, \sigma(r)$ generate $G(\mathbf{Q}^* \cdot \Omega_{h-x}/\mathbf{Q}^*(x))$; $\prod_{i=1}^{r} \sigma(i) = \mathrm{Id.}$; and we assume that $\sigma(r)$ is the branch cycle corresponding to $x = \infty$. Since the field extensions $\mathbf{Q}^*(y_1)$ and $\mathbf{Q}^*(z_1)$ are of genus zero, the Riemann–Hurwitz formula gives (1.12a and b). As $h(y) - g(z)$ is reducible, Galois Theory shows that $G(\Omega_{h-x}/\mathbf{Q}(y_1))$ is not transitive on $z_1,\ldots, z_m$. This gives (1.13b), and (1.13a) follows (from the fact that h is not composite with g). The branch cycle for $h(y) - x = 0$ over $x = \infty$ is an n-cycle (that is, $T_1(\sigma(r)) = (n)$). In particular, $\sigma(r)$ is of order n. The places of $\mathbf{Q}^*(z_1)$ over $x = \infty$ correspond to the poles of $g(y)$. Since $g(y)$ satisfies the third of the conditions (1.3), $T_2(\sigma(r)) = (m/2)(m/2)$. But, as $\sigma(r)$ is of order n, we must have $m/2 = n$ or $m = 2 \cdot n$. Thus, we have (1.11).

From Lemma 9 of [6] the representation T_1 is doubly transitive, unless h is a cyclic or a Chebychev polynomial (see comment below Definition 2.) In the former case $\mathbf{Q}^*(y_1) = \Omega_{h-x}$, and in the latter case

$$[\mathbf{Q}^* \cdot \Omega_{h-x} : \mathbf{Q}^*(y_1)] = 2.$$

Since g is of degree 2n, and h is not composite with g, each of these cases is ruled out. Therefore, we have demonstrated (1.9).

To conclude our proof, we show that T_2 is not a doubly transitive representation. If T_2 were doubly transitive, then $G = G(\Omega_{h-x}/\mathbf{Q}(x))$ is a doubly transitive group (where $\deg T_2 = 2 \cdot n$) with an intransitive subgroup $H = G(T_1, 1)$ of index less than $2 \cdot n$. It is (well) known that this is impossible. ∎

COROLLARY 3. *Let $h \in \mathbf{Q}[y]$ be a polynomial of prime degree, p, for which $S(h, \mathbf{Z})$ is infinite. Then $2p - 1$ is a square. Also, we have either $p = 5$ or $p > 333$.*

Proof. In the notation of Corollary 2 we will show that T_2 (on

$G(\Omega_{h-x}/\mathbf{Q}(x)))$ is a primitive representation. Thus, T_2 is a primitive (not doubly transitive) representation of degree $2p$ with p a prime (containing an element $\sigma(r)$ with $T_2(\sigma(r)) = (p)(p)$). This contradicts the results of [18] if $2p - 1$ is not a square; and it contradicts the results of [16] if $5 < p < 333$.

If T_2 is not primitive then there exists a group $\bar{G}$ with $G(T_2, 1) \subseteq \bar{G} \subseteq G$. From the fundamental theorem of Galois theory we conclude that the fixed field in Ω_{h-x} of $\bar{G}$ is a proper subfield of $\mathbf{Q}(z_1)$. Thus, $g(y) = \bar{g}_1(\bar{g}_2(y))$ where $\deg \bar{g}_1, \deg \bar{g}_2 > 1$. Since $\deg g = 2 \cdot p$ and $(\deg \bar{g}_1) \cdot (\deg \bar{g}_2) = \deg g$; either $\deg \bar{g}_1$ or $\deg \bar{g}_2$ is 2. Let $\mathscr{Y}(1),\ldots, \mathscr{Y}(u)$ be the places of $\bar{g}_1(z) - x = 0$ over $x = \infty$. Let k_i be the number of places of $\bar{g}_2(z) - x = 0$ over the place given by $x = \mathscr{Y}(i)$, $i = 1,\ldots, u$. Since $g(z) - x = 0$ has 2 places, with ramification index p, over $x = \infty$, we have $\sum_{i=1}^{u} k_i = 2$. Thus, either

$$(1.14) \quad u = 2 \quad \text{and} \quad k_1 = k_2 = 1, \quad \text{or}$$

$$(1.15) \quad u = 1 \quad \text{and} \quad k_1 = 2.$$

In the case (1.15), by a linear fractional change of the variable z (over $\mathbf{Q}$) we may assume that the place of $\bar{g}_1(z) - x = 0$ over $x = \infty$ is $z = \infty$. So $\bar{g}_1(z) \in \mathbf{Q}[z]$. Since the ramification indices of the places of $\bar{g}_2(z) - x = 0$ over $x = \infty$ times the degree of $\bar{g}_1(z)$ is equal to p (the ramification indices of the places of $g(z) - x = 0$ over $x = \infty$) we have $\deg \bar{g}_1 = p$. We have $\Omega_{\bar{g}_1-x} \subseteq \Omega_{h-x}$. In fact, since $G(\Omega_{h-x}/\mathbf{Q}(y_1))$ has order relatively prime to p, this group cannot be transitive on the p zeros of $\bar{g}_1(z) - x = 0$. As in the proof of Corollary 2, we conclude that $h(y) - \bar{g}_1(z)$ is reducible (as a polynomial in two variables). Since $h(y), \bar{g}_1(y) \in \mathbf{Q}[y]$, this contradicts the last line of Proposition 1. We have eliminated (1.15).

Now consider case (1.14). Then $\bar{g}_2(z) - x = 0$ has two totally ramified places (over $x = \mathscr{Y}(1)$ and $x = \mathscr{Y}(2)$). Therefore, we may assume (by a change of variable over Q^* sending $\mathscr{Y}(1) \to 0$ and $\mathscr{Y}(2) \to \infty$) that $\bar{g}_2(z)$ is a cyclic polynomial (comment following Definition 2). Using, as above, the multiplicativeness of the ramification indices in the layer $\mathbf{Q}^*(z_1) \supset \mathbf{Q}^*(\bar{g}_2(z_1)) \supset \mathbf{Q}^*(x)$ over the place $x = \infty$, we conclude that $\deg \bar{g}_2 = p$. The branch cycles for the cover $g(z) - x = 0$ (of the x-sphere) are therefore $\sigma(1)$ and $\sigma(2)$ of order 2 corresponding to the branch points of $\bar{g}_1(z) - x = 0$ ($\deg \bar{g}_1 = 2$), and $\sigma(3)$ of order p corresponding to $x = \infty$. Since $\Omega_{h-x} = \Omega_{g-x}$, the characterization of Chebychev polynomials shows that $h(y)$ is a Chebychev polynomial (step 3 of Lemma 9 of [6]). Thus, $[\mathbf{Q}^* \cdot \Omega_{h-x} : \mathbf{Q}^*(x)] = 2 \cdot p$. Therefore, $\mathbf{Q}^* \cdot \Omega_{h-x} = \mathbf{Q}^*(z_1)$ and contrary to assumption h is composite with g (Definition 2). We have excluded case (1.14), and this finishes the proof of the corollary. ∎

Remark 1. Let $h(y) \in \mathbf{Q}[y]$ be such that $G(\Omega_{h-x}/\mathbf{Q}(x))$ is the symmetric group (respectively, alternating group) of degree n (denoted S_n; respectively A_n) in its action on the zeros, $y_1, \ldots, y_n$, of $h(y) - x$. If $n \neq 5$, then $S(h, \mathbf{Z})$ if finite. This follows from Corollary 2 (expression (1.13)) as follows. The representation T_2 corresponding to $g(z) - x = 0$ (as in the proof of Corollary 2) corresponds to the action of S_n (respectively, A_n) on the unordered subsets of $\{1, 2, \ldots, n\}$ of cardinality k, for some fixed integer $1 < k < n$ (dependent on T_2). On the other hand, since S_n' (respectively A_n) is transitive on these subsets, the number of such subsets must be $2n = \deg T_2$. But the number of such subsets is $\binom{n}{k}$. Thus, $k = 2$ and $n = 5$. As example 2 shows, the case $n = 5$ is truly exceptional.

EXAMPLE 1. *A polynomial $h \in \mathbf{Q}[y]$ for which $S(h, Z)$ has exponential density.* Let $h(y) = y^4 + y^2$. Then $R_h(Z) = V_h(Z) \cup V_g(Z) \cup \overline{V}$ where $\overline{V}$ is a finite set and $g(y) = -4y^4 - 4y^2 - 1$. This can be seen from Theorem 1 and some simple computations after observing that

$$h(y) - g(z) = (y^2 + 2yz + 2z^2 + 1)(y^2 - 2yz + 2z^2 + 1).$$

As in the discussion preceding Corollary 1, there exist constants $c_1, c_2 > 0$ for which $c_2 \cdot N^{1/4} < |S(h, \mathbf{Z}, N)| < c_1 \cdot N^{1/4}$.

EXAMPLE 2. *A polynomial $h \in \mathbf{Q}[y]$ (of degree 5) for which $S(h, \mathbf{Z})$ has logarithmic density.* This is the exceptional case in Corollary 3. Our discussion uses tools discussed carefully in [10], to which the reader is referred for notation and deeper considerations.

Let $G = S_5$; T_1 the standard representation of S_5; and $\sigma(1) = (1\ 2)(3\ 4)$, $\sigma(2) = (1\ 5)$, $\sigma(3) = (5\ 3)$, $\sigma(4) = (1\ 5\ 4\ 3\ 2)$. Let T_2 be the representation of S_5 on the set of unordered pairs $z_1 = \{1, 2\}$, $z_2 = \{1, 3\}$, $z_3 = \{1, 4\}$, $z_4 = \{1, 5\}$, $z_5 = \{2, 3\}$, $z_6 = \{2, 4\}$, $z_7 = \{2, 5\}$, $z_8 = \{3, 4\}$, $z_9 = \{3, 5\}$, $z_{10} = \{4, 5\}$. If we replace the letters $z_1, \ldots, z_{10}$ by the numbers $1, 2, \ldots, 10$ we obtain:

$$T_2(\sigma(1)) = (2\ 6)(3\ 5)(4\ 7)(9\ 10); \qquad T_2(\sigma(2)) = (1\ 7)(2\ 9)(3\ 10);$$
$$T_2(\sigma(3)) = (2\ 4)(5\ 7)(8\ 10); \qquad T_2(\sigma(4)) = (1\ 4\ 10\ 8\ 5)(2\ 7\ 3\ 9\ 6).$$

We verify that the Riemann–Hurwitz conditions (1.12a and b) are satisfied. Thus, Riemann's existence theorem implies there exist genus zero covers $Y_1 \xrightarrow{\varphi_1} \mathbf{P}^1(\mathbf{C})$ and $Y_2 \xrightarrow{\varphi_2} \mathbf{P}^1(\mathbf{C})$ of projective space $(\mathbf{P}^1(\mathbf{C}))$ such that $\sigma(1), \ldots, \sigma(4)$ are a description of the branch cycles for φ_1 and $T_2(\sigma(1)), \ldots, T_2(\sigma(4))$ are a description of the branch cycles for φ_2. If we assume that $\sigma(4)$ is the branch cycle over ∞ on $\mathbf{P}^1(\mathbf{C})$, then (Y_1, φ_1) corresponds to a

polynomial $h(y) \in \mathbf{C}[y]$; (Y_2, φ_2) corresponds to a rational function $g(y) \in \mathbf{C}[y]$. Also we have: $\mathbf{C} \cdot \Omega_{h-x} = \mathbf{C} \cdot \Omega_{g-x}$; and all the conditions of Corollary 2 are satisfied. The biggest problem is to demonstrate that we can choose the branch cycles of $h(y) - x = 0$ so that h and g can be defined over $\mathbf{Q}$. For problems like this we have the techniques of [10; especially Sections V and VI]. The idea, is to form a total family of covers (Hurwitz scheme) of $\mathbf{P}^1$ containing all covers of $\mathbf{P}^1$ with a description of their branch cycles given by $\sigma(1),\ldots, \sigma(4)$ (called $\mathscr{T}^{\text{symm}}$ in [10]). Then the subscheme consists of those covers of $\mathbf{P}^1$ with 3 fixed branch points (say 0, 1, ∞) can in this case (as in [10; Section VI.3)]) be shown to be parametrized by an affine open subset of $\mathbf{P}^1(C)$. In addition, in this case, the subscheme is easily seen to be defined over $\mathbf{Q}$. For a specialization of the parameter we get h and g defined over $\mathbf{Q}$. ∎

Remark 2. *Let L be a number field. For $h(y) \in L[y]$ we may consider the set*

$$T(h, L) = \{x_0 \in L \mid h(y) - x_0 \text{ is reducible over } L\}.$$

This leads us to consider when the curve $\mathscr{C}_M$, in the proof of Theorem 1, has infinitely many L-rational points. There are two questions to be concerned with here. The *Mordell Conjecture* asserts that any curve of genus larger than 1 has only finitely many L-rational places. There is no known curve $\mathscr{C}$ that has been proven to have the property: *if $\mathscr{C}$ is defined over L, then $\mathscr{C}$ has finitely many L'-rational places for every finite extension L' of L.*

Assuming the Mordell Conjecture is true, there is still the problem of characterizing polynomials $h(y)$ for which $\mathscr{C}_M$ has genus greater than 1.

2. Non-regular Analogue of the Čebotarev Density Theorem and Value Sets of Polynomials over Finite Fields

We now prove an analogue of the Čebotarev density theorem. The proof is completely analogous to the classical proof except that we do not restrict ourselves to regular extensions. Let $k = \mathbf{F}(q)$ (the finite field with q elements), and let x be indeterminate over k. Let L be a finite Galois extension of $k(x)$. Let the algebraic closure of k in L be $\hat{k}$ (we have need for the case $\hat{k} \neq k$). The group $G(\hat{k}/k) =^{\text{def}}$ the Galois group of $\hat{k}/k$, has a canonical generator called the Frobenius symbol, which we denote by F_k. Let $G =^{\text{def}} \{\sigma \in G(L/k(x)) \mid \sigma \text{ restricted to } \hat{k} \text{ is } F_k\}$. The set G was introduced by S. Cohen in [4]. For each prime $\mathfrak{p}$ of $k(x)$ there exists a conjugacy class of elements, $(\mathfrak{p}^{L/k(x)})$, of $G(L/k(x))$ such that $\sigma \in (\mathfrak{p}^{L/k(x)})$

induces F_k on the residue class field of some prime of L lying over $\mathfrak{p}$ (p. 164 of [3]). In addition, $\left(\frac{L/k(x)}{\mathfrak{p}}\right)$ is uniquely determined by this property if $\mathfrak{p}$ is unramified in L. In the case when $\mathfrak{p}$ is of degree 1 in $k(x)$ and $\mathfrak{p}$ is tamely ramified in L (p. 29 of [3]) we can describe $\left(\frac{L/k(x)}{\mathfrak{p}}\right)$ quite explicitly. Let α be a primitive generator for $L/k(x)$, and let $\alpha^{(1)},\ldots, \alpha^{(n)}$ be the conjugates of α over $k(x)$. Then each of $\alpha^{(i)}$ can be expressed as a Taylor series in $\mathfrak{p}^{1/t}$ (for some integer t; the Puisseux expansions about $\mathfrak{p}$). The action of F_k on the coefficients of these Taylor series yields a permutation of $\alpha^{(1)},\ldots, \alpha^{(n)}$ representing $\left(\frac{L/k(x)}{\mathfrak{p}}\right)$.

PROPOSITION 2. *For $\sigma \in G(L/k(x))$ let $\langle\sigma\rangle$ denote the conjugacy class of σ. Let $B(\sigma)$ = number of degree 1 primes $\mathfrak{p}$ of $k(x)$ such that $\left(\frac{L/k(x)}{\mathfrak{p}}\right) = \langle\sigma\rangle$. Then*

$$B(\sigma) = \begin{cases} \dfrac{|\langle\sigma\rangle|}{|\hat{G}|} \cdot |k| + O(|k|^{1/2}) & \text{if } \sigma \in \hat{G}. \\ 0 \text{ otherwise} \end{cases}$$

Here $|\ |$ denotes the order of a set and $O(\alpha)$ for $\alpha > 0$ signifies a quantity $\leqslant C \cdot \alpha$ where C is an explicitly determinable constant (in this case, dependent only on the genus of L).

Note. It makes no difference as to whether we take conjugacy classes in G or $\hat{G}$.

Proof. Let ρ be a finite dimensional irreducible representation of $G(L/k(x))$. We have

$$\log\left(\frac{1}{\mathrm{Det}(I - \rho(\mathfrak{p})\, t^{\deg \mathfrak{p}})}\right) = -\mathrm{tr}(\log(I - \rho(\mathfrak{p})\, t^{\deg \mathfrak{p}}))$$

(for $\mathfrak{p}$ any prime of $k(x)$), where $\rho(\mathfrak{p})$ denotes any representative of $\rho\left(\left(\frac{L/k(x)}{\mathfrak{p}}\right)\right)$. We obtain from this:

$$\frac{d}{dt}\log \mathscr{L}_\chi(L/k(x), t) = \sum_{n=1}^{\infty}\left(\sum_{\substack{\deg \mathfrak{p} \mid n \\ \mathfrak{p} \text{ prime of } k(x)}} (\deg \mathfrak{p}) \cdot \chi(\rho(\mathfrak{p})^{n/\deg \mathfrak{p}})\right) t^{n-1},$$

where $\mathscr{L}_\chi(L/k(x), t)$ is the L-series corresponding to the character χ of ρ (see [17], Chapter V). Following Dirichlet's well-known argument, for each $\sigma \in G(L/k)x))$, we form

$$\sum_{\text{irreducible } \chi}\left(\frac{d}{dt}\log \mathscr{L}_\chi(L/k(x), t)) \cdot \chi(\sigma^{-1})\right) \overset{\text{def.}}{=} M(\sigma, t). \tag{2.1}$$

By inspection, the constant term of $M(\sigma, t)$ is seen to be:

$$(2.2)\quad \sum_{x}\ \sum_{\mathfrak{p}\text{ of deg 1 of }k(x)} \chi(\rho(\mathfrak{p}))\cdot\chi(\sigma^{-1}) \overset{\text{def.}}{=} A(\sigma).$$

From the orthogonality relations: if $\rho(\mathfrak{p}) \neq \rho(\sigma)$, then $\sum_x \chi(\rho(\mathfrak{p}))\,\chi(\sigma^{-1}) = 0$; while if $\rho(\mathfrak{p}) = \rho(\sigma)$, then $\sum_x \chi(\sigma)\,\chi(\sigma^{-1}) = |\,G\,|/|\langle\sigma\rangle|$. Thus,

$$B(\sigma)\cdot|\,G\,|/|\langle\sigma\rangle = A(\sigma).$$

We now estimate $A(\sigma)$ from the Riemann hypothesis for curves.

Let $Z_{L,k}$ be the zeta-function for L. Then:

$$Z_{L,k} = \prod_{x} \mathscr{L}_x(L/k(x), t).$$

Let $L' = \hat{k}(x)$, and let χ' run over the irreducible (one dimensional) characters of $G(\hat{k}(x)/k(x))$.

Since $Z_{L',k} = 1/(1 - t^{[\hat{k}:k]})(1 - |\,\hat{k}\,|\,t^{[\hat{k}:k]}) = \prod_{x'} \mathscr{L}_{x'}(L'/k(x), t)$, if we extend each χ' to a character χ'' of $G(L/k(x))$ such that χ'' is trivial on $G(L/L')$ we obtain

$$(2.3)\quad Z_{L,k} = Z_{L,\hat{k}}(t^{[\hat{k}:k]}) = \Big(\prod_{x''} \mathscr{L}_{x''}(L/k(x), t)\Big)\cdot\Big(\prod_{x\notin\{x''\}} \mathscr{L}_x(L/k(x), t)\Big).$$

The function $Z_{L,k}$ is a rational function in t with denominator

$$(1 - t^{[\hat{k}:k]})(1 - |\,\hat{k}\,|\,t^{[\hat{k}:k]}).$$

The numerator of $Z_{L,k}$ is a polynomial of degree equal to $2g$, where g is the genus of L. This polynomial has zeros of absolute value

$$(|\,\hat{k}\,|^{1/2[\hat{k}:k]})^{-1} = |\,k\,|^{-1/2}$$

(by the Riemann hypothesis for curves over finite fields.) Thus, if $\chi \notin \{\chi''\}$, $\mathscr{L}_x(L/k(x), t)$ has zeros of absolute value $|\,k\,|^{-1/2}$, and (utilizing standard notation) we write:

$$(2.4)\quad \mathscr{L}_x(L/k(x), t) = \prod_{i=1}^{c_x} (1 - \alpha_i t) \text{ where } |\,\alpha_i\,| = |\,k\,|^{1/2} \text{ for } \chi \notin \{\chi''\}.$$

We return to (2.2) to estimate $A(\sigma)$ by using (2.1) to obtain:

$$(2.5)\quad A(\sigma) = \sum_{x''} \frac{d}{dt} \log \mathscr{L}_{x''}(L/k(x), t)\cdot\chi''(\sigma^{-1})|_{t=0} + O(|\,k\,|^{1/2}).$$

The first term on the right side of (2.5) remains exactly the same if we replace χ'' by χ'. Explicitly, we have

$$\mathscr{L}_{\chi'}(L'/k(x), t) = \prod_{\mathfrak{p}} \left(\frac{1}{1 - \chi'(F_{k(\mathfrak{p})})\, t^{\deg \mathfrak{p}}}\right)$$

where $F_{k(\mathfrak{p})}$ is the Frobenius element corresponding to the residue class field $k(\mathfrak{p})$ of $\mathfrak{p}$. Therefore

$$A(\sigma) = \sum_{\mathfrak{p} \text{ of degree } 1} \left(\sum_{\chi'} \chi'(F_k) \cdot \chi'(\sigma^{-1})\right) + O(|\, k \,|^{1/2});$$

or

(2.6) $A(\sigma) = [\hat{k} : k] \cdot |\, k \,| + O(|\, k \,|^{1/2})$ if $\sigma \in \hat{G}$, and
$A(\sigma) = O(|\, k \,|^{1/2})$ otherwise. Thus,
$B(\sigma) = (|\langle\sigma\rangle|[\hat{k} : k]/|\, G \,|)\, |\, k \,| + O(|\, k \,|^{1/2})$ if $\sigma \in \hat{G}$.

Since $|\, G \,|/[\hat{k} : k] = |\, \hat{G} \,|$, this concludes the lemma as $B(\sigma) = 0$ if $\sigma \notin \hat{G}$ (restriction of a Frobenius symbol to $k(x)$ must be given by the action of F_k on $\hat{k}$). ∎

Let A be an elementary (diophantine) statement which can be interpreted over all (or all but a finite number) of residue class fields of a number field. Proposition 2 (and its generalizations) can be utilized to give a primitive recursive procedure for deciding the subset of those finite fields for which A is true. We now give an example to illustrate this (compare with [4] and [5]). For this we need a lemma. Consider the following notation:

K is an algebraic number field with ring of integers $\mathfrak{o}_K$; $f(x, y) \in \mathfrak{o}_K[x, y]$; Ω_f is the splitting field of f over $K(x)$; $f(\mathfrak{p})$ is the polynomial obtained by reduction of f modulo $\mathfrak{p}$ for prime ideals $\mathfrak{p}$ of $\mathfrak{o}_K$; $k(\mathfrak{p})$ is the residue class field $\mathfrak{o}_K/\mathfrak{p}$ of the prime $\mathfrak{p}$; $\Omega_{f(\mathfrak{p})}$ is the splitting field of $f(\mathfrak{p})$ over $k(\mathfrak{p})(x)$; $\hat{K}$ is the algebraic closure of K in Ω_f; $\hat{\mathfrak{p}}$ is (for each $\mathfrak{p}$) a choice of a prime of $\mathfrak{o}_{\hat{K}}$ lying over $\mathfrak{p}$; and $K^{(\mathfrak{p})}$ is the fixed field in $\hat{K}$ of the element $[\frac{\hat{K}/K}{\hat{\mathfrak{p}}}] \in G(\hat{K}/K)$.

LEMMA 1. *Excluding a finite set of (effectively computable) primes* $\mathfrak{p}$, *there is a canonical isomorphism*

(2.7) $G(\Omega_f/K^{(\hat{\mathfrak{p}})}(x)) \simeq G(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(x))$.

Proof. Let $B_1 = \{\mathfrak{p} \mid \mathfrak{p} \text{ is ramified in } \hat{K}\}$. Then, if $\mathfrak{p} \notin B_1$,

$$[\hat{K} : K^{(\hat{\mathfrak{p}})}] = [\hat{K}(x) : K^{(\hat{\mathfrak{p}})}(x)] = [k(\hat{\mathfrak{p}})(x) : k(\mathfrak{p})(x)].$$

Thus, to prove (2.7) we are reduced to showing

(2.8) $G(\Omega_f/\hat{K}(x)) \simeq G(\Omega_{f(\mathfrak{p})}/k(\hat{\mathfrak{p}})(x))$.

Let $\mathfrak{o}_{\Omega_f}$ be the integral closure of $\mathfrak{o}_{\hat{K}}[x]$ in Ω_f. Thus, $\mathfrak{o}_{\Omega_f} = \mathfrak{o}_{\hat{K}}[x, y]/I$ where $I \otimes \hat{K}$ is an absolutely irreducible ideal over $\hat{K}$. We show that (excluding a finite set of primes), the quotient field of $S(\hat{\mathfrak{p}}) =^{\text{def}} \mathfrak{o}_{\Omega_f} \otimes k(\hat{\mathfrak{p}})$ is $\Omega_{f(\mathfrak{p})}$. The action of $G(\Omega_f/\hat{K}(x))$ on $\Omega_{f(\mathfrak{p})}$ is obtained from its action on $S(\hat{\mathfrak{p}})$. We know that $S(\hat{\mathfrak{p}})$ is an integral domain for almost all $\hat{\mathfrak{p}}$ by Noether's lemma ([6], p. 48). Let B_2 be the exceptional set of primes.

Let $y_1, \ldots, y_n$ be the zeros of $f(x, y)$ regarded as a polynomial in y. There exists $\beta \in \mathfrak{o}_{\hat{K}}[x]$ such that $\beta y_i \in \mathfrak{o}_{\Omega_f}$ for $i = 1, \ldots, n$. Let $B_3 = \{\hat{\mathfrak{p}} \mid \beta \equiv 0 \bmod \hat{\mathfrak{p}}\}$. If we exclude $\hat{\mathfrak{p}} \in B_3$, we prove (2.8) under the assumption that $y_1, \ldots, y_n \in \mathfrak{o}_{\Omega_f}$.

Let $\alpha = \sum_{i=1}^{n} c_i y_i$ for some choice of $c_1, \ldots, c_n \in \mathfrak{o}_{\hat{K}}$ so that $\sigma(\alpha) \not\equiv \alpha$ for each $\sigma \in G(\Omega_f/\hat{K}(x))$. Then, ([13], p. 44), α is a primitive generator of Ω_f over $\hat{K}(x)$. Let $h(x, y) \in \mathfrak{o}_{\hat{K}}[x, y]$ be absolutely irreducible and such that $h(x, \alpha) \equiv 0$.

Modulo I we have $\partial h/\partial y(\alpha) \equiv \prod_{\sigma \neq 1} (\alpha - \sigma(\alpha))$. Also, there exist polynomials $\{r_i(x, y)\}_1^n$ and $\{t_i(x, y)\}_1^n \subseteq \mathfrak{o}_{\hat{K}}[x, y]$ for which $y_i = r_i(x, \alpha)/t_i(x, \alpha)$, $i = 1, \ldots, n$.

Let $B_4 = \{\hat{\mathfrak{p}} \mid r_i(x, y) \equiv 0 \bmod \hat{\mathfrak{p}}$ or $t_i(x, y) \equiv 0 \bmod \hat{\mathfrak{p}}$ for some integer $i = 1, \ldots, n\}$. Let $B_5 = \{\hat{\mathfrak{p}} \mid \partial h/\partial y \bmod \hat{\mathfrak{p}} \in I \otimes k(\hat{\mathfrak{p}})\}$.

From the usual discriminant theory we can compute the finite set B_5. For $\hat{\mathfrak{p}} \notin B_5$, $\alpha \bmod \hat{\mathfrak{p}}$ has $|G(\Omega_f/\hat{K}(x))|$ conjugates over $\hat{K}(\mathfrak{p})(x)$, and the action of $G(\Omega_f/\hat{K}(x))$ on $S(\hat{\mathfrak{p}})$ is faithful. For $\hat{\mathfrak{p}} \in B_4$, the quotient field of $S(\hat{\mathfrak{p}})$ is $\Omega_{f(\mathfrak{p})}$. Thus, for $\hat{\mathfrak{p}} \notin \bigcup_{i=1}^{5} B_i$, (2.7) is established. ∎

Let K be a number field, and let $h(y), g(y) \in \mathfrak{o}_K[y]$. For $\mathfrak{p}$ a prime of $\mathfrak{o}_K$, let $V_{\mathfrak{p}}(h) = \{x_0 \in \mathfrak{o}_K/\mathfrak{p} \mid$ there exists $y_0 \in \mathfrak{o}_K/\mathfrak{p}$ with $h(y_0) = x_0\}$. Assume that

(2.9) $V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$ for all but finitely many primes $\mathfrak{p}$. As in Section 1, let $\Omega_x = \Omega_{h-x} \cdot \Omega_{g-x}$, and let $y_1, \ldots, y_n$ (respectively, $z_1, \ldots, z_n$) be the zeros of $h(y) - x$ (respectively, $g(z) - x$). We denote $(h(y) - x)(g(y) - x)$ by $f(x, y)$, in order to apply Lemma 1. Let σ_{x_0} be a representative of the conjugacy class of the Frobenius symbol for the degree 1 prime $x - x_0$ of $k(\mathfrak{p})[x]$. Excluding the finite (computable) set of x_0 such that $x - x_0$ is ramified in $\Omega_{f(\mathfrak{p})}$, then (2.9) imples that

$$\sigma_{x_0} \in \hat{G}(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(y_1)) \qquad \text{iff} \quad \sigma_{x_0} \in \hat{G}(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(z_j))$$

for some j (see the discussion preceding Proposition 2). Excluding a finite

set of primes $\mathfrak{p}$ (those for which the order of $k(\mathfrak{p})$ is "too small") Proposition 2 implies that every element of $G(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(x))$ is of the form σ_{x_0} for some $x_0 \in k(\mathfrak{p})$. Thus, (2.9) implies (in fact, is essentially equivalent to):

$$(2.10) \quad \bigcup_{i=1}^{n} \hat{G}(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(y_j)) = \bigcup_{j=1}^{m} \hat{G}(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(z_j)).$$

There exist infinitely many primes $\mathfrak{p}$ (see Lemma 2 of Section 3 for an explicit construction) such that $K^{(\hat{\mathfrak{p}})} = \hat{K}$ (in the notation preceding Lemma 1.) Then $k(\mathfrak{p}) = k(\hat{\mathfrak{p}})$ and (by Lemma 1)

$$G(\Omega_f/\hat{K}(x)) = G(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(x)) = G(\Omega_{f(\mathfrak{p})}/k(\mathfrak{p})(x))$$

Thus, (2.10) implies that

$$(2.11) \quad \bigcup_{i=1}^{n} G(\Omega_f/\hat{K}(y_j)) = \bigcup_{j=1}^{m} G(\Omega_f/\hat{K}(z_j)).$$

THEOREM 2. *Let $h(y), g(y) \in \mathbf{Z}[y]$ where either; h is an indecomposable polynomial (Definition 1); or deg h is an odd prime-power. Assume that $V_p(h) = V_p(g)$ for all but a finite set of primes $\mathfrak{p}$* (a.a. $\mathfrak{p}$). *Then h and g are linearly related (Definition 2.).*

Proof. From the preceding discussion (2.11) holds with $K = \mathbf{Q}$. It is easy to show from Galois Theory (Proposition 3 of [9]) that (2.11) implies that $\Omega_h = \Omega_g$ and $h(y) - g(z)$ is reducible. When deg h is an odd prime-power, the Theorem follows from the result of [7]; when h is indecomposable, we conclude the theorem from Proposition 1. ∎

Remark 3. As pointed out in the introduction (or see [10; Section VI]) there exist number fields K and pairs of indecomposable polynomials $h, g \in K[y]$ for which

$$V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$$

for almost all primes $\mathfrak{p}$ of $\mathfrak{o}_K$. It is believed, however, that the examples where deg h is one of 7, 11, 13, 15, 21, or 31 are the only possible examples (with h indecomposable).

On the other hand, we do not know to what extent Theorem 2 may be improved. In fact, we have no examples where $V_{\mathfrak{p}}(h) = V_{\mathfrak{p}}(g)$ for a.a. p. (of $\mathbf{Q}$) and h and g are not linearly related. The technique of proof of Theorem 2 shows that h and g have non-trivial composition factors which are linearly related. ∎

3. A Proof of the Irreducibility Theorem

For the standard comments and reduction of cases in Hilbert's Irreducibility Theorem see ([21], Chapter 5). There it is shown that the essential case to consider is $f(x, y) \in \mathbf{Z}[x, y]$ where $f(x, y)$ is irreducible as a polynomial in two variables over $\mathbf{Q}$. For simplicity we restrict ourselves to this situation. However, our proof can be applied directly to the case when f is defined over any number field (see [10; Section IV.1)] where this is done without appeal to any of the standard reduction arguments).

Theorem 3. *Let $f(x, y) \in \mathbf{Z}[x, y]$ be irreducible over $\mathbf{Q}$. Then there exists an (explicitly) computable arithmetic progression of integers I such that:*

(3.1) *for $x_0 \in I$, $f(x_0, y)$ is irreducible as a polynomial in one variable over Q.*

We need a Lemma which, in spite of its basic nature, seems to be unavailable in the literature.

Lemma 2. *Let M/K be number fields. Then there is an inductively constructable infinite set of primes $\mathfrak{p}$ of $\mathfrak{o}_K$ such that*

$$[\mathfrak{o}_M/\mathfrak{p}^* : \mathfrak{o}_K/\mathfrak{p}] = 1 \text{ for each prime } \mathfrak{p}^* \text{ of } \mathfrak{o}_M \text{ over } \mathfrak{o}_K .$$

Proof. By the multiplicative property of the degrees of residue class fields we can consider the case when $K = \mathbf{Q}$ and (by considering the Galois closure of M over $\mathbf{Q}$) M is Galois over $\mathbf{Q}$. Let $\theta \in \mathfrak{o}_M$ be a separable generator for $M/\mathbf{Q}$, and let $f(x) \in \mathbf{Z}[x]$ be its monic irreducible polynomial.

From Kummer's Theorem ([3], p. 92) we are reduced to inductively finding primes p (not dividing the discriminant of $f(x)$) such that $f(x) \equiv 0$ modulo p has at least one solution. Since $M/\mathbf{Q}$ is Galois; this will imply that $f(x)$ splits completely modulo p. Let $f(0) = C$. Let $p_1, \ldots, p_n$ be the first n primes p obtained for which $f(x) \equiv 0 \bmod p$ has a solution. Include the primes dividing C in the list. Then we form p_{n+1} by taking a prime (different from $p_1, \ldots, p_n$) dividing $m = f(C \cdot (\prod_1^n p_i)^l)$ where l is selected so that m is not zero. ∎

Proof of Theorem 3. Factor $f(x, y)$ over an algebraically closed extension of $\mathbf{Q}(x)$ to obtain

(3.2) $f(x, y) = c \cdot \prod_{i=1}^n (y - y_i)$, for some constant c.

We refer now to the notation of the proof of Theorem 1. For each partition $M \cup N$ of $\{1, 2,..., n\}$ there exists $\xi_j^{(M)}$ such that $\xi_j^{(M)} \notin \mathbf{Q}(x)$. Upon multiplying $\xi_j^{(M)}$ by an element of $\mathbf{Z}[x]$ we may assume $\xi_j^{(M)}$ is integral over $\mathbf{Z}[x]$. Suppose $x_0 \in \mathbf{Z}$ and $\xi_j^{(M)}(x_0) \notin \mathbf{Z}$. Then no factorization of $f(x_0, y)$ over $\mathbf{Q}$ corresponds to the subset M. Let $f_M(x, y)$ be the irreducible monic polynomial for $\xi_j^{(M)}$ over $\mathbf{Z}[x]$.

The above argument shows that if $x_0 \in \mathbf{Z}$ is such that for each M as above

(3.3) $f_M(x_0, y) = 0$ has no solution for $y \in \mathbf{Z}$,

then $f(x_0, y)$ is irreducible over $\mathbf{Q}$.

We now show that we can produce an arithmetic progression P such that for $x_0 \in P$, (3.3) holds. Fix M for some preliminary considerations. If $f_M(x, y)$ is not absolutely irreducible, then there exists only finitely many $(x_0, y_0) \in \mathbf{Z} \times \mathbf{Z}$ such that $f_M(x_0, y_0) = 0$ because such a point would be an intersection point of the curves defined by two absolutely irreducible components of $f_M(x, y)$. Thus, we may assume $f_M(x, y)$ is absolutely irreducible. By Noether's Lemma ([6], p. 48) $f_M(x, y)$ remains absolutely irreducible modulo p for almost all primes p. Suppose there exists A_M, an infinite set of primes such that for $p \in A_M$:

(3.4) there exists $x_0(p, M) = x_0$ with $f_M(x_0, y) \equiv 0 \mod p$, has no solution.

Then we can conclude the proof of the Theorem as follows. Let $p(M) \in A_M$, so that $p(M)$, running over distinct subsets M of $\{1, 2,..., n\}$, consists of distinct primes. By the Chinese remainder theorem, there is an integer $\bar{x}_0 \in \mathbf{Z}$ such that $\bar{x}_0 \equiv x_0(p(M), M) \mod p(M)$ for each M. Let $n_0 = \prod_M p(M)$. Consider the arithmetic progression: $P = \{\text{integers of form } \bar{x}_0 + m \cdot n_0 \text{ for } m \in \mathbf{Z}\}$. If, for some $x_0 \in P$ and some index M we had $f_M(x_0, y_0) = 0$ for some $y_0 \in \mathbf{Z}$, then by reduction modulo $p(M)$ we contradict (3.4).

Now we establish the existence of the set A_M. Let Ω_{f_M} be the splitting field of f_M over $\mathbf{Q}(x)$. Let $\hat{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in Ω_{f_M}. Let A_M^{**} be the set of primes p satisfying the conclusion of Lemma 2 (for $K = \mathbf{Q}$, $M = \hat{\mathbf{Q}}$), and let $A_M{}^*$ be the subset of A_M^{**} such that expression (2.7) of Section 2 holds. Then we have $G(\Omega_{f_M}/\hat{\mathbf{Q}}(x)) = G(\Omega_{f_M(\mathfrak{p})}/k(p)(x))$, and the algebraic closure of $k(p)$ in $\Omega_{f_M(\mathfrak{p})}$ is just $k(p)$. Since $f_M(x, y)$ is absolutely irreducible there exists $\sigma \in G(\Omega_{f_M}/\hat{\mathbf{Q}}(x))$ with $\sigma(y_i) \neq y_i$ for $i = 1,..., n$ (where $y_1,..., y_n$ are the zeros of $f_M(x, y)$).

Let A_M be the subset of $A_M{}^*$ consisting of primes p of $A_M{}^*$ for which the image of the element σ (selected above) in $G(\Omega_{f_M(\mathfrak{p})}/k(p)(x))$ is the

Frobenius symbol for some first degree prime $x - x_0$ of $k(p)[x]$ (as in Proposition 2). Then (from the discussion proceeding Proposition 2) $f_M(x_0, y) \equiv 0 \bmod p$ has no solution for $p \in A_M$. This concludes the proof. ∎

Remark 4. Our proof of Theorem 3 started out with a procedure (due to Hilbert) whereby we are reduced to limiting the integral points on a collection of curves (defined by $f_M(x, y)$ in the notation of the proof). We could have proceeded more directly, and thereby have eliminated this reduction of the problem (as in [10; Section VI.4)]). In fact, let $f(x, y)$ be the polynomial (absolutely irreducible) for which we desire to demonstrate the conclusion of Theorem 3. For each σ in $G(\Omega_f/\hat{\mathbf{Q}}(x))$ let x_σ and p_σ be given (by the proof of Theorem 3) satisfying: $\{p_\sigma\}_{\sigma \in G}$ is a distinct set of primes;

$$G(\Omega_f(Q(x)) \cong G(\Omega_{f(p)}(k(p)(x)); \qquad \text{and} \quad \left(\frac{\Omega_{f(p)}/k(p)(x)}{x - x_0}\right) = \langle\sigma\rangle,$$

where $x - x_\sigma$ is a first degree prime of $k(p)[x]$. By the Chinese remainder theorem, solve for x_0 so that $x_0 \equiv x_\sigma \bmod p_\sigma$ for each $\sigma \in G(\Omega_f/\mathbf{Q}(x))$. The proof of Theorem 3 shows that $P = \{x_0 + m \cdot \prod_{\sigma \in G} p_\sigma \mid m \in \mathbf{Z}\}$ is the desired arithmetic progression.

The group $G(\Omega_f/\mathbf{Q}(x))$ is a permutation group when represented on the n zeros of $f(x, y)$. If $\sigma \in G(\Omega_f/\hat{\mathbf{Q}}(x))$ is an n-cycle in this representation, then $f(x_\sigma, y) \bmod p_\sigma$ is an irreducible polynomial in one variable over $k(p_\sigma)$. Thus for integers $x_0 \in P_\sigma = \{x_\sigma + mp_\sigma \mid m \in \mathbf{Z}\}$, $f(x_0, y)$ is an irreducible polynomial in one variable over $\mathbf{Q}$. Hence we obtain

THEOREM 4. *Let $f(x, y) \in \mathbf{Z}[x, y]$ be irreducible over $\mathbf{Q}$. Assume that (in the previous notation) $G(\Omega_f/\hat{\mathbf{Q}}(x))$ contains an n-cycle in the representation of this group on the collection $y_1, \ldots, y_n$ of the zeros of $f(x, y)$. Then there exists an arithmetic progression I of prime modulus such that the conclusion of Theorem 3 holds.*

REFERENCES

1. J. AX, The elementary theory of finite fields, *Ann. of Math., 2nd Ser.* **88** (1968), 239–271.
2. E. BOMBIERI, Seminaire Bourbaki talk, to appear, 1974.
3. J. CASSELS AND A. FRÖHLICH, "Algebraic Number Theory," Thompson Book Co., Washington, D. C., 1967.
4. S. COHEN, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 259–273.

5. M. FRIED, Arithmetical properties of value sets of polynomials (I), *Acta Arith.* **15** (1969), 91–115.
6. M. FRIED, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.
7. M. FRIED, The diophantine equation $h(y) - x$. *Acta Arith.* **19** (1971), 78–87.
8. M. FRIED, On a theorem of Ritt and related diophantine problems, *Crelles J.* (1974).
9. M. FRIED, The field of definition of function fields and a problem in the reducibility of polynomials, *Illinois J. Math.* **17** (1973), 128–146.
10. M. FRIED AND D. J. LEWIS, "Solution Spaces of Diophantine Problems," Invited talk, B.A.M.S., to appear, 1975.
11. M. JARDEN, Elementary statements over large algebraic fields, *Trans. Amer. Math. Soc.* **164** (1972), 67–91.
12. S. LANG, "Diophantine Geometry," Interscience tracts, New York, 1966.
13. W. LEVEQUE, "Topics in Number Theory," Vol. II, Addison–Wesley, Reading, MA, 1957.
14. C. L. SIEGEL, Über einige Anwendungen diophantischer Approximationen, *Abh. Preus. Akad. Wiss. Phys.—Math. Kl.* **1** (1929), 14–67.
15. A. SCHINZEL, On Hilbert's irreducibility theorem, *Ann. Polon. Math.* **16** (1965), 333–340.
16. L. SCOTT, "Uniprimitive Permutation Groups," Theory of Finite Groups, A Symposium at Harvard University, W. A. Benjamin Inc., pp. 55–62, 1972.
17. A. WEIL, "Sur les Courbes et les Variétés qui s'en Déduisent," (Hermann and Cie, Ed.), Paris, 1948 (especially pp. 79–84).
18. H. WIELANDT, Primitive Permutations gruppen von Grad, II, *Math. Z.* **63** (1956).
19. S. LANG, Sur les séries L d'une variété algébrique, *Bull. Soc. Math. France* **84** (1956), 385–407.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.