ISRAEL JOURNAL OF MATHEMATICS, Vol. 51, No. 4, 1985

ON THE SPRINDŽUK–WEISSAUER APPROACH TO UNIVERSAL HILBERT SUBSETS

BY

M. FRIED†

Department of Mathematics, The University of California at Irvine, Irvine, CA 92717, USA

ABSTRACT

The works of both Sprindžuk (1979–80) and Weissauer (1980) consider the relation between Hilbert subsets of **Q** and sets consisting of powers of primes. A comparison of their results leads to generalizations and new proofs devoid of either p-adic diophantine approximation or of nonstandard arithmetic (§3 and §4). Results of Weissauer, giving new Hilbertian infinite extensions of every Hilbertian field, receive short direct standard proofs, and a negative answer is given to a question of Roquette on the relation between Hilbert sets and value sets.

Introduction

Let R be an integral domain with quotient field K. For $f_1, \dots, f_l \in K[X, Y]$ let

$$H_R(f_1, \dots, f_l) = H_R(\boldsymbol{f})$$
$$= \{x(0) \in R \mid f_i(x(0), Y) \text{ is irreducible in } K[Y],\ i = 1, \dots, l\}$$

be the *Hilbert set* of $\boldsymbol{f}$ in R. Similarly, let

$$V_R^l(\boldsymbol{f}) = \{x(0) \in R \mid f_i(x(0), Y) \text{ has no zero in } K,\ i = 1, \dots, l\}.$$

Consider such sets only if f_i is irreducible and of degree at least 2 in Y, $i = 1, \dots, l$. The field K is *Hilbertian* if $H_K(\boldsymbol{f})$ is infinite for each such $\boldsymbol{f}$. For simplicity we take K to be a countable field of characteristic zero, with a fixed algebraic closure $\bar{K}$.

Recent investigations have concentrated on two topics. First, for a given Hilbertian field K, infinite subextensions of $\bar{K}/K$ are given that are Hilbertian.

† Partially supported by a Fulbright–Hays research grant at Helsinki University, Fall semester, 1982.

Received November 21, 1983 and in revised form August 15, 1984

Weissauer's thesis [22] contains a nonstandard proof of the following result. Suppose that $K \subset M \subset M_1 \subset \bar{K}$, that M_1 is not in the Galois hull of M/K, and that M_1/M is finite. Then M_1 is Hilbertian. Our proof of this (Corollary 1.4) follows from two Galois theoretic lemmas. As an immediate corollary, the solvable closure of a Hilbertian field (which happens to be a non-Hilbertian field) has all of its proper finite extensions Hilbertian.

Second, for a given Hilbertian field K, some of the subsets H of K, that are contained in "many" Hilbert sets, are described. Call H a *universal Hilbert subset* (§3) if H is infinite and, up to finite sets, contained in every Hilbert subset of K. Gilmore and Robinson [9] nonconstructively demonstrate that universal Hilbert subsets exist. But, even if $K = \mathbf{Q}$, their explicit production is no simple matter.

Sprindžuk [18] considers the set $H^* = \{p^t \mid p \text{ is prime}, t \in \mathbf{N}\}$. He states two conditions that guarantee for $f \in \mathbf{Q}[X, Y]$ that $H^* - H_{\mathbf{Q}}(f)$ is an explicitly computable finite set. His intricate proof is based on p-adic diophantine approximation. Theorem 3.2 observes that the qualitative part of his result follows quickly from Siegel's celebrated theorem [17]. This starts the main story of the paper — the remarkable connection between [18] and [22].

Zerofinite sets (§4) are a standard version of the nonstandard *polefinite elements* of [22]. The proof of Theorem 3.2 consists primarily of noting that H^* is a zerofinite subset of $\mathbf{Q}$ with *zero bound* 1. Let H be a zerofinite subset of K. Theorem 4.2 gives a direct standard proof that every Hilbert set of K has infinite intersection with some transform of H by a Mobius transformation of K, a nonstandard deduction of [22]. Our standard proof of Weissauer's result, that fields with a product formula are Hilbertian, uses the *distributions* that go back to Weil's thesis [21]. Although much of the short proof of Proposition 4.5 consists of a reminder about these objects, at this point the indirect nonstandard proof is quite slick, and difficult to compare with ours. We concentrate on the reproof of both the qualitative and quantitative results of [18] without either nonstandard arithmetic or diophantine approximation. The approach is distinct from that of [11] which also removes the nonstandard arithmetic from this result, but remains true to the original ideas. Finally (Theorem 4.9) we outline how Sprindžuk [20] goes from this point to demonstrate that $\{[\exp(\sqrt{\log(\log(m))}] + m!2^m,\ m = 1, 2, \ldots\} = H$ is a universal Hilbert subset of $\mathbf{Q}$.

A subtheme of the paper considers connections between the sets $V'_K(f)$ and $H_K(f)$. A question of Roquette (§2) has a negative answer: There are Hilbert sets $H_{\mathbf{Q}}(f)$ (defined by one polynomial) that do not contain sets of form $V'_{\mathbf{Q}}(h)$ (also defined by one polynomial). A positive answer would have simplified

properties of zerofinite sets (§3). This leads to a series of observations on the role of the special value sets $V'_K(h_1(Y)-X\cdot h_2(Y))$ in testing K for Hilbertianity. Proposition 3.4, in particular, applies the *Mordell conjecture* [5] to show that there are infinite sets H for which $H - V'_{\mathbf{Q}}(h_1(Y)-X\cdot h_2(Y))$ is finite for each pair $h_1, h_2 \in \mathbf{Q}[Y]$ with $h_1\cdot h_2$ of positive degree, but H is *not* a universal Hilbert subset.

Finally, here is a version of a problem in [13; p. 142] that we have not considered in this paper. Is there a unique factorization domain R with infinitely many principal prime ideals $(\pi(1)),(\pi(2)),\dots$ for which $H_R^* = \{\pi(i)^t, i = 1,2,\dots; t\in\mathbf{N}\}$ is *not* a zerofinite set?

Comments by Moshe Jarden account for much of the improvement between the original and final version of this manuscript. The proof of Theorem 4.9 evolved from correspondence between the author and V. G. Sprindžuk.

§1. A standard proof of a result of Weissauer

First we rephrase Hilbert's observations [10] relating his irreducibility theorem to questions about realizing groups as Galois groups. For simplicity assume throughout this paper that the Hilbertian field K is of characteristic 0. For $h_1,\dots,h_l\in K[X,Y]$, denote by $V'_K(\boldsymbol{h}) = V'_K(h_1,\dots,h_l)$ the set $\{x_0\in K \mid h_i(x_0,Y)$ has no zero, $i=1,\dots,l\}$. Then, each Hilbert set of K contains a Hilbert set of form $V'_K(\boldsymbol{h})$ with $h_1,\dots,h_l$ absolutely irreducible polynomials of degree at least 2 in Y. The examples of §2 show that we cannot assume that $l=1$. Finally, denote by $G(f(Y),K)$ the Galois group of the splitting field of $f(Y)$ over the field K. Then, for $f\in K[X,Y]$, $\{a\in K \mid G(f(a,Y),K) = G(f(X,Y),K(X))\}$ contains a Hilbert set of K.

Our next results produce many infinite extensions of K that are Hilbertian.

Let $K\subset L\subset\Omega$ with Ω/K a Galois extension. The next lemma is an immediate consequence of the fundamental theorem of Galois theory.

LEMMA 1.1. *For $x\in\Omega$, here is the exact condition that $L(x)\subset L\cdot M_1$ with M_1/K Galois and $L\cap M_1 = K$. For some normal subgroup H of $G(\Omega/K)$, $G(\Omega/L(x))\supseteq G(\Omega/L)\cap H$ where H and $G(\Omega/L)$ generate $G(\Omega/K)$.*

Let L/K be a finite separable extension of K and let $h_1,\dots,h_m\in L[T,X]$ be absolutely irreducible polynomials with $\deg_X(h_i)>1$, $i=1,\dots,m$. Let α be a primitive generator for L/K and replace h_i by $H_i = h_i(T_1+\alpha\cdot T_2, X)\in L[T_1,T_2,X]$. Note that H_i is also absolutely irreducible, $i=1,\dots,m$. List the distinct conjugates $\alpha=\alpha^{(1)},\dots,\alpha^{(n)}$ of α and denote the

jth conjugate of $h_i(T_1+\alpha\cdot T_2, X)$ by $H_i^{(j)}$. Let $\hat{L}=K(\alpha^{(1)},\dots,\alpha^{(n)})$ and let $g_i=\prod_{j=1}^{n} H_i^{(j)}$, an irreducible element of $K[T_1, T_2, X]$. Consider, also, the splitting field, $\Omega(g_i, \boldsymbol{T})$, of g_i over $K(T_1, T_2)=K(\boldsymbol{T})$. It contains $\hat{L}(\boldsymbol{T})$. Also, let $\Omega(H_i^{(j)}, \boldsymbol{T})$ be the splitting field of $H_i^{(j)}$ over $\hat{L}(\boldsymbol{T})$. Denote by $\Omega(\boldsymbol{g}, \boldsymbol{T})$ the composition of $\Omega(g_1, \boldsymbol{T}),\dots,\Omega(g_m, \boldsymbol{T})$, and by $\hat{L}(\boldsymbol{g})$ the algebraic closure of K in $\Omega(\boldsymbol{g}, \boldsymbol{T})$.

LEMMA 1.2. *For each fixed i, there exists no field $M^{(i)}\subset\Omega(g_i, \boldsymbol{T})$ with $M^{(i)}/K(\boldsymbol{T})$ Galois, $L(\boldsymbol{T})\cap M^{(i)}=K(\boldsymbol{T})$ and $L(\boldsymbol{T})\cdot M^{(i)}\supset L(\boldsymbol{T}, x^{(i)})$ where $x^{(i)}$ is some zero of H_i.*

PROOF. Suppose the conclusion is incorrect. With no loss, change K to $K'=\hat{L}(\boldsymbol{g})\cap M^{(i)}$. Thus, the hypotheses imply that $x^{(i)}$ is contained in the Galois extension $\hat{L}(\boldsymbol{T})\cdot M^{(i)}/K(\boldsymbol{T})$. Therefore $\hat{L}(\boldsymbol{T})\cdot M^{(i)}$ contains all conjugates of $x^{(i)}$ over $K(\boldsymbol{T})$. It is therefore $\Omega(g_i, \boldsymbol{T})$. Identify its group with

$$G(\hat{L}/K)\times G(M^{(i)}/K(\boldsymbol{T}))=G(\hat{L}(\boldsymbol{T})/K(\boldsymbol{T}))\times G(\Omega(g_i, \boldsymbol{T})/\hat{L}(\boldsymbol{T})). \tag{1.1}$$

Identify $G(\Omega(g_i, \boldsymbol{T})/\hat{L}(\boldsymbol{T}))$ with a subgroup of the product of isomorphic groups

$$\prod_{k=1}^{n} G(\Omega(H_i^{(k)}, \boldsymbol{T})/\hat{L}(\boldsymbol{T})). \tag{1.2}$$

In (1.2), $G(\hat{L}/K)$ acts on the product by permuting the factors transitively. Also, from (1.1), it commutes with the image of $G(\Omega(g_i, \boldsymbol{T})/\hat{L}(\boldsymbol{T}))$. Thus for each $k\neq 1$, we may assume with no loss that $\hat{L}(\boldsymbol{T}, x^{(i)})=\hat{L}(\boldsymbol{T}, x_k^{(i)})$ with $x_k^{(i)}$ some zero of $H_i^{(k)}$. Now apply the algebraic independence of $T_1+\alpha\cdot T_2$ and $T_1+\alpha^{(k)}\cdot T_2$. Thus $L_1=\hat{L}(T_1+\alpha\cdot T_2, x^{(i)})$ and $L_2=\hat{L}(T_1+\alpha^{(k)}\cdot T_2, x_k^{(i)})$ are regular and linearly disjoint extensions of $\hat{L}$. In particular, $[L_2:\hat{L}(T_1+\alpha^{(k)}\cdot T_2)]=[L_1\cdot L_2:\hat{L}(\boldsymbol{T}, x^{(i)})]>1$, contrary to the above. This concludes the lemma. ■

THEOREM 1.3. *Let M be a Galois extension of an Hilbertian field K. For L, a finite proper extension of K such that $M\cap L=K$, let $N=L\cdot M$. Then N is an Hilbertian field. Moreover, every Hilbert set of N contains elements of L.*

PROOF. Return to the notation prior to the lemma. From standard reductions we have only to show that there exist $t_1, t_2\in K$ such that $h_i(t_1+\alpha\cdot t_2, X)$ has no zero in $L\cdot M$, $i=1,\dots,m$. Choose t_1, t_2 such that the composite of the splitting fields of $g_i(t_1+\alpha\cdot t_2, X)$, $i=1,\dots,m$ has Galois group isomorphic to $G(\Omega(\boldsymbol{g}, \boldsymbol{T})/K(\boldsymbol{T}))$. Now apply the Galois theoretic criteria of Lemma 1.1 to the conclusion of Lemma 1.2 to deduce that no zero of $h_i(t_1+\alpha\cdot t_2, X)$ is in a field of

the form $L \cdot M_i$ with $L \cap M_i = K$ and M_i/K Galois, $i = 1, \ldots, m$. In particular this applies to M_i any subfield of M. ■

COROLLARY 1.4 [22]. *Let M be an algebraic extension of an Hilbertian field K, and let M_1 be a proper finite extension of M. If M_1 is not contained in the Galois hull, $\hat{M}$, of M/K, then M_1 is Hilbertian.*

PROOF. With no loss replace M by $M_1 \cap \hat{M}$. With $M_1 = M(\alpha)$, put $L_1 = K(\alpha)$ and $K_1 = L_1 \cap \hat{M}$. Exchange K_1 for K, L_1 for L and $\hat{M}$ for M in Theorem 1.3. Therefore $M_1' = \hat{M} \cdot L_1 (= \hat{M} \cdot M_1)$ is Hilbertian, and each Hilbertian set contains elements of L_1 and therefore M_1. Thus M_1 is Hilbertian. ■

Notice that the maximal solvable extension $\mathbf{Q}_{\text{sol}}$ of $\mathbf{Q}$ is not Hilbertian; there exists no $a \in \mathbf{Q}_{\text{sol}}$ such that $Y^2 - a$ is irreducible in $\mathbf{Q}_{\text{sol}}$. But Corollary 1.4 implies that every proper finite extension of $\mathbf{Q}_{\text{sol}}$ is Hilbertian.

§2. Testing Hilbertianity — one value set does not suffice

For $h \in K[X, Y]$, an absolutely irreducible polynomial, call the set $V_K(h) = \{x_0 \in K \mid h(x_0, Y) \text{ has a zero}\}$ the *value set* of h (with respect to X). Denote by $V_K'(h)$ the complement of this set — as in §1. We observed, in the opening paragraph of §1, that every Hilbert set contains an intersection of a finite number of complements of value sets. P. Roquette has asked this:

QUESTION 2.1. *Does each Hilbert set of K contain a set of the form $V_K'(h) - U$ where U is a finite set and h is an irreducible polynomial of degree at least 2 in Y?*

We now give examples to show that the question has a negative answer even in the case that $K = \mathbf{Q}$. There is additional motivation and elaboration in §3.

Consider $f \in \mathbf{Q}[X, Y]$ and $h_1, h_2 \in \mathbf{Q}[Z]$ with these properties:

(2.1) (a) f is absolutely irreducible;
(b) $f(h_1(Z), Y)$ and $f(h_2(Z), Y)$ are both reducible; and
(c) there exists no rational functions g, g_1 and $g_2 \in \boldsymbol{Q}(Z)$ with $\deg(g) > 1$, $h_1(Z) = g(g_1(Z))$ and $h_2(Z) = g(g_2(Z))$.

LEMMA 2.2. *If (2.1) holds, then $H_{\mathbf{Q}}(f)$ contains no set of form $V_{\mathbf{Q}}'(h) - U$ where U is finite and h is an irreducible polynomial of degree at least 2 in Y.*

PROOF. Suppose the lemma is false and there is an $h \in \mathbf{Q}[X, Y]$ with properties contrary to the conclusion. Then $V_{\mathbf{Q}}(h) \supset V_{\mathbf{Q}}(h_1(Y) - X)$ and $V_{\mathbf{Q}}(h) \supset V_{\mathbf{Q}}(h_2(Y) - X)$, excluding in either containment some finite set. Now consider $\bar{h}_i(Z, Y) = h(h_i(Z), Y)$, $i = 1, 2$. For each $z_0 \in \mathbf{Q}$, there exists $y_0^{(i)} \in \mathbf{Q}$

such that $\bar{h}_i(z_0, y_0^{(i)}) = 0$, $i = 1, 2$. An application of Hilbert's irreducibility theorem(!) shows that $\bar{h}_i(Z, Y)$ has a factor $Y - m_i(Z)$ of degree 1 in Y and at least degree 1 in Z, $i = 1, 2$. We rewrite this in terms of field theory.

Let x be an indeterminate, y a zero of $h(x, Y)$, and $z^{(i)}$ a zero of $y - m_i(Z)$. Then $\bar{h}_i(z^{(i)}, y) = 0$. With no loss we may assume that $x = h_1(z^{(1)})$. And, from the equation $h(x, y) = h(h_2(z^{(2)}), y) = 0$ (and the irreducibility of $h(X, y)$ over $\mathbf{Q}(y)$) there exists a $\mathbf{Q}(y)$-isomorphism σ such that $\sigma(h_2(z^{(2)})) = h_2(\sigma(z^{(2)})) = x$. Replace $z^{(2)}$ by $\sigma(z^{(2)})$ to conclude that we have a chain of fields $\mathbf{Q}(z^{(i)}) \supset \mathbf{Q}(x, y) \supset \mathbf{Q}(x)$, $i = 1, 2$. Apply Luroth's theorem: $\mathbf{Q}(x, y) = \mathbf{Q}(y')$ for some element y' with $g(y') = x = g(g_i(z^{(i)})) = h_i(z^{(i)})$ for some g, $g_i \in \mathbf{Q}(Z)$, $i = 1, 2$. Since $g(Y) - X$ is of degree 1 in X, it is irreducible. From Gauss' lemma, $g(Y) - x$ is irreducible over $\mathbf{Q}(x)$. Thus $[\mathbf{Q}(y') : \mathbf{Q}(x)] = \deg_Y(h) = \deg(g)$. Conclude the lemma by noting that this contradicts (2.1)(c). ■

From Lemma 2.2 a negative answer to Question 2.1 requires only that we produce f, h_1 and h_2 with the properties of expression (2.1). Take $f = 4 \cdot Y^4 + 4 \cdot Y^2 + 1 - X$, $h_1(Z) = 4 \cdot Z^4 + 4 \cdot Z^2 + 1$ and $h_2(Z) = -Z^4 - Z^2$. Calculate that

$$\begin{aligned} &Z^4 + Z^2 + 4 \cdot Y^4 + 4 \cdot Y^2 + 1 \\ &\quad = (Z^2 + 2 \cdot Z \cdot Y + 2 \cdot Y^2 + 1) \cdot (Z^2 - 2 \cdot Z \cdot Y + 2 \cdot Y^2 + 1). \end{aligned} \tag{2.2}$$

If $h_i(Z) = g(g_i(Z))$ with $\deg(g) > 1$, $i = 1, 2$, then one of the factors in (2.2) would be divisible by $g_1(Z) - g_2(Y)$. Clearly, this does not happen, and (2.1)(c) holds. Expression (2.2) appears in [6; p. 93] as a linear change of variables, so as to put its coefficients in $\mathbf{Q}$, of an example from [4].

Unfortunately, such examples over $\mathbf{Q}$ do not come easily. If, however, we allow h_2 to be a rational function, instead of a polynomial, and we take $f = h_1(Y) - X$, then [8; Example 7] gives examples in which f is of all possible degrees greater than 3 in Y. If we allow K to be a number field there are examples of degree 7, 11, 12, 15, 21 and 31 where h_1 and h_2 are *indecomposable* polynomials and $f(X, Y) = h_1(Y) - X$ [8; especially the discussion after Example 7]. As a consequence of the classification of finite simple groups, these are known to be the only possible degrees under these conditions. Lemma 3.1 (§3) shows why it makes sense to seek examples where f is of the form $h_1(Y) - X$.

§3. Sprindžuk's theorem and universal Hilbert subsets

Let K be a countable Hilbertian field, and let $f_1(X, Y), f_2(X, Y), \ldots$ be an ordering of the irreducible elements of $K[X, Y]$. For each integer i choose

$x(i) \in K$ for which $f_1(x(i), Y), \ldots, f_l(x(i), Y)$ are irreducible in $K[Y]$. Then the infinite set $H = \{x(1), x(2), \ldots\}$ has the *universal Hilbert subset property*:

$$\begin{aligned} &H - H_K(g_1, \ldots, g_l) \text{ is finite for each collection} \\ &\{g_1, \ldots, g_l\} \text{ of irreducible polynomials in } K[X, Y]. \end{aligned} \tag{3.1}$$

This is a paraphrase of an observation from [9]. But, even in the case that $K = \mathbf{Q}$, how do we explicitly produce an infinite universal Hilbert subset? Note that finite unions of sets with propery (3.1) also have property (3.1).

Sprindžuk [18; Theorem 1] uses p-adic approximation to produce explicit infinite sets H with this property: $H - H_{\mathbf{Q}}(f)$ is finite for each absolutely irreducible polynomial $f(X, Y) \in \mathbf{Q}[X, Y]$ where

$$\begin{aligned} &\text{(a)} \quad f(0, Y) \text{ has a } \mathbf{Q}\text{-zero, } y(0); \text{ and} \\ &\text{(b)} \quad \frac{\partial}{\partial Y}(f)\Big|_{(0, y(0))} \neq 0. \end{aligned} \tag{3.2}$$

For example $H^* = \{p^t \mid p \text{ is prime}, t \in \mathbf{N}\}$ is such a set. It is unlikely that the essence of condition (3.2)(a) can be dropped. Indeed, if $g(Y)$ is any polynomial of degree greater than 1 that assumes infinitely many positive prime values over $\mathbf{Z}$, then the irreducible polynomial $g(Y) - X$ has the property that $H^* - H_{\mathbf{Q}}(g(Y) - X)$ is infinite. Apparently it is unknown if there is such a polynomial $g(Y)$ [14], but each irreducible polynomial in $\mathbf{Z}[Y]$, whose values on $\mathbf{Z}$ form a set with greatest common divisor 1, seems to be a reasonable candidate [2].

Therefore it is reasonable to ask if there is some simple procedure by which, given an irreducible polynomial $f \in \mathbf{Q}[X, Y]$, we can alter the infinite set H^* to a set $H^*(f)$ so that $H^*(f) - H_{\mathbf{Q}}(f)$ is finite. In this way we would be giving an "explicit proof" of Hilbert's irreducibility theorem. Recall (§2) that since $H_{\mathbf{Q}}(f)$ contains $V'_{\mathbf{Q}}(h_1, \ldots, h_l) = V'_{\mathbf{Q}}(\boldsymbol{h})$, with $h_1, \ldots, h_l$ absolutely irreducible elements of $\mathbf{Z}[X, Y]$ that are monic in Y, we need only find an alteration of H^* to $H^*(\boldsymbol{h})$ which is, up to a finite set, contained in $V'_{\mathbf{Q}}(\boldsymbol{h})$. Note first that for the case $l = 1$ this is relatively easy.

For h an absolutely irreducible polynomial of $\mathbf{Q}[X, Y]$, either the equation $h(X, Y) = 0$ has an infinite number of $\mathbf{Z}$-valued points $(x(0), y(0))$ with

$$\frac{\partial}{\partial Y}(h)\Big|_{(x(0), y(0))} \neq 0,$$

or it does not. In the former case choose one of these, $(x(0), y(0))$, and let $H^*(h) = \{p^t - x(0) \mid p \text{ is prime}, t \in \mathbf{N}\}$, and in the latter case let $H^*(h) = H^*$. Of course, testing which of these holds requires a result such as [17]. Since [17] tells

us that a nonsingular projective model of the curve $h(X, Y) = 0$ is of genus zero, it is then theoretically possible to *explicitly* change coordinates for the curve to find a conic in $\mathbf{P}^2$ birational to it. Legendre's method (e.g., [1; p. 73]) then produces $(x(0), y(0))$.

Unfortunately, according to §2, the case $l = 1$ is not suitably general. In §4 we compare Sprindžuk's result with the process by which Weissauer [22] shows that any field K, with a *product formula*, is Hilbertian.

Next we show that the *qualitative* part of Sprindžuk's theorem is an easy consequence of Siegel's theorem [17]. The use of the Thue–Siegel–Roth theorem in [17], unlike Sprindžuk's method, excludes effective computation of the finite set $H^* - H_{\mathbf{Q}}(f)$. Let $f \in \mathbf{Q}[X, Y]$ be an irreducible polynomial, and with x an indeterminate, let Ω_f be the splitting field of $f(Y) - x$ over $\mathbf{Q}(x)$.

LEMMA 3.1. *There exists* $g_1, \dots, g_l \in \mathbf{Q}(Y)$ *with these properties*:

(3.3) (a) $H_{\mathbf{Z}}(f) \cup U_1 = V'_{\mathbf{Z}}(g_1(Y) - X) \cap \cdots \cap V'_{\mathbf{Z}}(g_l(Y) - X) \cup U_2$ *where* U_1 *and* U_2 *are finite sets*;

(b) *for each* i *either* $g_i(Y) \in \mathbf{Q}[Y]$, *or* $g_i(Y) = h_i(Y)/(m_i(Y))^{n(i)}$ *with* h_i, $m_i \in \mathbf{Q}[Y]$, m_i *an irreducible quadric and* $\deg(h_i) = 2 \cdot n(i)$.

(c) $\Omega_f \supseteq \Omega_{g_i}$; *and*

(d) $f(g_i(Z), Y)$ *is reducible* (*over* $\mathbf{Q}(Z)$), $i = 1, \dots, l$.

OUTLINE OF PROOF [7, Theorem 1]. List the minimal subfields $L_1, \dots, L_l$ of Ω_f with the following properties: $L_i \supset \mathbf{Q}(x)$; L_i is of genus 0 and has a $\mathbf{Q}$-rational place; $G(\Omega_f / L_i)$ is intransitive in its action on the zeros of $f(x, Y)$; and the place $x = \infty$ is either totally ramified in L_i or there are two conjugate places of L_i over $x = \infty$, each M_i-rational with $[M_i : \mathbf{Q}] = 2$ and $M_i \subseteq \mathbf{R}$, i = 1, . . . , l.

Under these conditions $L_i = \mathbf{Q}(z_i)$ and there exists $g_i \in \mathbf{Q}(Z)$ such that $g(z_i) = x$, $i = 1, \dots, l$. The conditions on the places of L_i over $x = \infty$ give condition (b) and condition (d) follows, by Galois theory, from the intransitivity of $G(\Omega_f / L_i)$ on the zeros of $f(x, Y)$, $i = 1, \dots, l$. Thus we have only to establish condition (a). But this is exactly the Galois theoretic interpretation of [17; p. 51] whose set up consumes most of the proof of [7; Theorem 1]. ■

THEOREM 3.2. *For* $H^* = \{p^t \mid p \text{ is prime}, t \in \mathbf{N}\}$, $H^* - H_{\mathbf{Q}}(f)$ *is finite for each* f *satisfying condition* (3.2).

PROOF. Suppose that f satisfies (3.2). Let $g_1, \dots, g_l$ be the rational functions that arise from Lemma 3.1. For any one of these, say g, we need only show that $H^* - V'_{\mathbf{Z}}(g(Y) - X)$ is finite. Now we show that, in either circumstance of

expression (3.3)(b), the numerator of $g(Y)$ — call it $h(Y)$ — has a proper irreducible factor that appears with multiplicity one.

Let x be an indeterminate, and let $y = y(0) + \sum_{i=1}^{\infty} a_i \cdot x^i$ be the Puiseux expansion for the zero of $f(x, Y)$ with center $y(0)$. The coefficients $a_1, a_2, \ldots$, are in $\mathbf{Q}$ and the expansion requires no fractional exponents precisely because of (3.2)(b). Denote the zeros of $g(Y) - x$ by $z(1), \ldots, z(n)$. The series may have fractional exponents in x. Their constant terms are the zeros of $h(Z)$. Let y be a zero of $f(x, Y)$ and let $z(1), \ldots, z(k)$ denote an orbit of the action of $G(\Omega_f/\mathbf{Q}(y))$ on $\{z(1), \ldots, z(n)\}$. From condition (3.3)(d), $k < n$. Thus the elementary symmetric functions in $z(1), \ldots, z(k)$ are in $\mathbf{Q}(y)$. So the elementary symmetric functions in $z(1), \ldots, z(k)$ have Puiseux expansions without fractional exponents in x, and the elementary symmetric functions in the constant terms of $z(1), \ldots, z(k)$ are in $\mathbf{Q}$. The stated property of $h(Y)$, in the paragraph above, follows immediately.

There are now two cases corresponding to (3.3)(b): Either

(3.4) (a) $g(Z) = h^{(1)}(Z) \cdot h^{(2)}(Z)$ with $h^{(1)}, h^{(2)} \in \mathbf{Q}[Z]$ relatively prime polynomials of positive degree; or

(b) $g(Z) = h^{(1)}(Z) \cdot h^{(2)}(Z)/(m(Z))^{n/2}$ with $h^{(1)}, h^{(2)}, m \in \mathbf{Q}[Z]$ relatively prime in pairs and of positive degree, and m irreducible of degree 2.

First consider (3.4)(a). Let $c(i)/d(i)$, $i = 1, 2, \ldots$ be a sequence of distinct rational numbers with $(c(i), d(i)) = 1$, $c(i), d(i) \in \mathbf{Z}$ and $g(c(i)/d(i)) = p(i)^{t(i)}$, a prime integer power. The $d(i)$ can be bounded independently of i, and $h^{(1)}(c(i)/d(i))$ (resp., $h^{(2)}(c(i)/d(i))$) can be written as $e^{(1)} \cdot p(i)^{r(i)}$ (resp., $e^{(2)} \cdot p(i)^{s(i)}$) with $e^{(1)}$ and $e^{(2)}$ running over a finite list of rational numbers and $r(i) + s(i) = t(i)$ with $r(i), s(i) \geqq 0$. Note that neither $r(i)$ nor $s(i)$ is a bounded function of i.

From the euclidean algorithm, however, $m^{(1)}(Z) \cdot h^{(1)}(Z) + m^{(2)}(Z) \cdot h^{(2)}(Z) = 1$ with $m^{(1)}, m^{(2)} \in \mathbf{Q}[Z]$. Conclude that the numerator of the left side of this expression evaluated at $c(i)/d(i)$ is divisible by arbitrarily high powers of primes as a function of i. This contradiction concludes the possibility of (3.4)(a). Albeit, a bit more complicated, a contradiction arises from (3.4)(b) similarly once it is noted that, instead of bounding $d(i)$, we may write $m(c(i)/d(i))$ as $e \cdot (d(i))^{-2}$ where e runs over a finite list of rational numbers. The details are part of [17], and thus we conclude the proof. ■

REMARK 3.3. Note that condition (3.4) is considerably weaker than the conclusion we drew from condition (3.2), which is that $h^{(1)}(Z)$ could be taken to

be irreducible over $\mathbf{Q}$. That this weaker condition suffices for the conclusion of the proof will be part of the argument at the end of §4 by which we construct universal Hilbert subsets explicitly.

Let $H = \{x(1), x(2), \dots\}$ be an infinite subset of $\mathbf{Q}$. It is tempting, from Lemma 3.1, to test if H is a universal Hilbert subset (property (3.1)) by considering only whether $H - V'_{\mathbf{Q}}(g(Y) - X)$ is finite for each $g \in \mathbf{Q}(Y)$ of degree at least 2. As our next result shows, this test fails as a consequence of the recent proof of the *Mordell conjecture* [5]. For the next proposition only, switch the X and Y coordinates in the usual definition of an *affine Weierstrass equation*: $f(X, Y) = 0$ has the form $X^2 - m(Y) = 0$ with $\deg(m) = 3$.

PROPOSITION 3.4. *Let $f(X, Y) = 0$ be an affine Weierstrass model for an elliptic curve over $\mathbf{Q}$ having infinitely many $\mathbf{Q}$-rational points. Let $H = \{x(1), x(2), \dots\}$ be the X-coordinates of the $\mathbf{Q}$-rational points on this equation. Then $H - V'_{\mathbf{Q}}(g(Y) - X)$ is finite for each $g \in \mathbf{Q}(Y)$ of degree at least 2. Clearly, however, since $V'_{\mathbf{Q}}(f) \cap H$ is empty, H is not a universal Hilbert subset.*

PROOF. Suppose, on the contrary, that $H \cap V_{\mathbf{Q}}(g(Y) - X)$ is infinite. Let x be an indeterminate, y a zero of $f(x, Y)$ and z a zero of $g(Z) - x$. The function field $\mathbf{Q}(y, z)$ contains $\mathbf{Q}(y, x)$, and so it is of genus at least one. Since $\mathbf{Q}(x, z) = \mathbf{Q}(z)$ is of genus zero, conclude that, no matter what choice we took for z, $\mathbf{Q}(y, z)$ is a degree 3 extension of $\mathbf{Q}(z)$. For each $x' \in H \cap V_{\mathbf{Q}}(g(Y) - X)$ there is a $\mathbf{Q}$-rational specialization $(x, y) \to (x', y')$ and $(x, z) \to (x', z')$. Since $[\mathbf{Q}(y, x) : \mathbf{Q}(x)] = 3 = [\mathbf{Q}(y, z); \mathbf{Q}(z)]$, $\mathbf{Q}(y, x)$ is linearly disjoint from $\mathbf{Q}(z)$ over $\mathbf{Q}(x)$. Thus $(x, y) \to (x', y')$ extends to $(x, y, z) \to (x', y', z')$ to give infinitely many $\mathbf{Q}$-rational places for the function field $\mathbf{Q}(y, z)$. This, however, is contrary to the Mordell conjecture if the genus of $\mathbf{Q}(y, z)$ exceeds 1. And this, it surely does, if $\mathbf{Q}(y, z)$ is a *ramified* extension of $\mathbf{Q}(y, x)$. The remainder of the proof consists of demonstrating this ramification property.

For some value $z(0)$, the $\bar{\mathbf{Q}}$-rational place of $\mathbf{Q}(z)$ corresponding to the specialization $z \to z(0)$ is ramified over a finite place of $\mathbf{Q}(x)$ corresponding to the specialization $x \to x(0)$. But, there is at least one $\bar{\mathbf{Q}}$-rational place $p(0)$ of $\mathbf{Q}(x, y)$, lying over the place $x \to x(0)$, that is unramified over $\mathbf{Q}(x)$. Thus, the place of $\mathbf{Q}(y, z)$ extending both $p(0)$ and $\mathbf{z} \to z(0)$ is ramified over $\mathbf{Q}(y, x)$. ■

§4. Comparison of the Weissauer and Sprindžuk results

Weissauer [22] shows that any field K with a *product formula* is Hilbertian. For simplicity of discussion we assume that K is a countable field (of characteris-

tic 0 — as before). A *place* of a function field over K is a valuation corresponding to a K-conjugacy class of primes of the field.

Denote by ${}^*K$ a nontrivial *ultraproduct* of a countable product of copies of K. The essential point of [9] is that a universal Hilbert subset H (expression (3.1)) gives a representative $(x(1), x(2), \dots)$ of an element $x(H) \in {}^*K$ with this property:

(4.1) $K(x(H))$ is algebraically closed in ${}^*K$.

Indeed, the existence of $x' \in {}^*K$ for which $K(x')$ is algebraically closed in ${}^*K$ is equivalent to Hilbertianity for K.

Weissauer starts with a generalization of the Gilmore–Robinson observation. Here is an analogue of his *polefinite* definition to match the discussion in §3.

DEFINITION 4.1. Call a set $H = \{x(1), x(2), \dots\}$ of K *zerofinite* if there is an integer m (a *zero bound*) such that for each irreducible $f \in K[X, Y]$, $H - V_K'(f)$ infinite implies that the curve $f(X, Y) = 0$ has at most m places lying over the place $X = 0$ in the X-line. For $\alpha \in \text{Möb}(K)$, Möbius (i.e., linear fractional) transformations with coefficients in K, denote by $H(\alpha)$ the transformed set $\{\alpha(x(1)), \alpha(x(2)), \dots\}$. For simplicity just discard ∞ if it occurs in this set.

In analogy with the discussion following expression (3.2), the next result demonstrates explicitly the Hilbertianity of K from the existence of a zerofinite set. This standard proof does, however, use the existence of a nontrivial maximal ultrafilter on $\mathbf{N}$.

THEOREM 4.2. *Let H be a zerofinite subset of K. Then, for each Hilbert set $H_K(f)$, there exists $\alpha \in \text{Möb}(K)$ with $H(\alpha) \cap H_K(f)$ infinite.*

PROOF. As stated at the opening of §1, it suffices to show, for $h_1, \dots, h_l \in K[X, Y]$, absolutely irreducible and of degree at least 2 in Y, that there is an $\alpha \in \text{Möb}(K)$ with $H(\alpha) \cap V_K'(h_1, \dots, h_l)$ infinite. For each $a \in K$ and $h \in K[X, Y]$ denote by $h^{(a)}$ the polynomial $X^{\deg_X(h)} \cdot h(a + (1/X), Y)$, and by $H(a)$ the set $\{a + (1/x(1)), a + (1/x(2)), \dots\}$. Clearly $H(a) \cap V_K'(h_1, \dots, h_l)$ is infinite if and only if $H \cap V_K'(h_1^{(a)}, \dots, h_l^{(a)})$, is infinite. Let $\mathcal{U}$ be a nontrivial maximal ultrafilter on $\mathbf{N}$ and for $U \in \mathcal{U}$ denote by $H(U)$ the set $\{x(i) \mid i \in U\}$. The proof proceeds by contradiction: Assume that $H \cap V_K'(h_1^{(a)}, \dots, h_l^{(a)})$ is finite for each $a \in K$.

Thus, for each $a \in K$, there exists $i(a) \in \{1, 2, \dots, l\}$ for which $H - V_K'(h_{i(a)}^{(a)})$ is infinite and equal to $H(U_a)$ for some $U_a \in \mathcal{U}$. Let m be the integer of Definition 4.1. The remainder of the proof consists of finding — explicitly, if K is given

explicitly — an integer m' and m' values of a, $a(1),\dots,a(m')$, for which it is impossible that

$$H \cap V_K(h_{i(a(1))}^{(a(1))}) \cap \cdots \cap V_K(h_{i(a(m'))}^{(a(m'))}) = H(U_{a(1)} \cap \cdots \cap U_{a(m')})$$

is infinite. This contradiction concludes the theorem.

Indeed, let x be an indeterminate and let $y^{(j)}$ denote a zero of $h_{i(a(j))}^{(a(j))}(x, Y)$. Choose $a(j)$ inductively so that the discriminant locus of the field extension $K(x, y^{(j)})/K(x)$ is disjoint, excluding possibly 0, from the discriminant locus of the field extension $K(x, y^{(1)},\dots, y^{(j-1)})/K(x)$. Since putting an "$a$" superscript on $h(X, Y)$ shifts the corresponding discriminant locus of $X^{\deg_X(h)} \cdot h(1/X, Y)$ by a, this is clearly possible. If $\mathrm{char}(K) = 0$ each extension of $K(x)$ is ramified over some value of $x \neq 0$. See Remark 4.3 for the adjustment in the case that $\mathrm{char}(K) \neq 0$. From the discriminant assumption, $K(x, y^{(j)})$ intersects the Galois closure of $K(x, y^{(1)},\dots, y^{(j-1)})/K(x)$ in $K(x)$. Thus an induction shows that the field $L^{(j)} = K(x, y^{(1)},\dots, y^{(j)})$ has degree $\deg_Y(h_{i(1)}) \cdots \deg_Y(h_{i(j)})$ over $K(x)$. Also, let p_i be a prime over $x = \infty$ of the splitting field of $h_i(x, Y)$ over $K(x)$, $i = 1,\dots, l$. The residue class field of any prime of $K(x, y^{(k)})$ over $x = 0$ is contained in one of the residue class fields of $p_1,\dots, p_l$, for any $k = 1,2,\dots$. Thus, independent of j, the residue class fields of primes of $L^{(j)}$ over $x = 0$ have degree bounded by $\bar{n} = n(1) \cdots n(l)$, with $n(i)$ the degree of the residue class field of p_i, $i = 1,\dots, l$.

Therefore, $[L^{(m')}: K(x)]$ is at least $2^{m'}$. As each prime of $L^{(m')}$ over $x = 0$ has degree bounded by $\bar{n}$, $L^{(m')}$ has more than m places over $x = 0$ if $2^{m'}/\bar{n}$ exceeds m. In addition, $L^{(m')}$ has a K-rational place over every place $x = x'$ with $x' \in H(U_{a(1)} \cap \cdots \cap U_{a(m')})$. It is now standard to find a primitive generator y for $L^{(m')}/K(x)$ for which the irreducible polynomial $f(X, Y) \in K[X, Y]$ satisfies $f(x, y) = 0$ and the infiniteness of $H - V_K'(f)$ contradicts Definition 4.1. ∎

REMARK 4.3. If K is infinite and $\mathrm{char}(K) \neq 0$, there are many extensions of $K(x)$ that are ramified *only* over the place $x = 0$. Thus, in order to use the argument of the last two paragraphs of the proof of Theorem 4.2 in this case, we must assume that the function field for $h_i(X, Y) = 0$ is unramified over the place $x = \infty$, $i = 1,\dots, l$. Change X to $\alpha(X)$ for some $\alpha \in \mathrm{Möb}(K)$ to achieve this.

Let S be a nonempty set of primes (i.e., rank 1 valuations) of field K. We say that S *satisfies a product formula* if for each $p \in S$ we may choose an additive absolute value $v(p)$ corresponding to p with this property. For each $0 \neq a \in K$

$$\{p \in S \mid v(p)(a) \neq 0\} \text{ if finite, and } \sum_{p \in S} v(p)(a) = 0. \tag{4.2}$$

Weissauer proves that a field K is Hilbertian if it has a set of primes with a product formula. We interpret his result to say this:

PROPOSITION 4.4. *Assume that S, a set of primes on a field K, satisfies a product formula. Let m be an integer and $H = \{x(1), x(2), \ldots\}$ a subset of K with this property: For each i, $|\{p \in S \mid \nu(p)(x(i)) > 0\}| \leqq m$. Then H is zerofinite, and m is a suitable zero bound. Thus Theorem 4.2 implies that K is Hilbertian.*

First compare Proposition 4.4, in the case $K = \mathbf{Q}$, $H = H^* = \{p^t \mid p$ is prime, $t \in \mathbf{N}\}$ and $m = 1$ with Theorem 3.2. Here is the conclusion of Proposition 4.4. For $f \in \mathbf{Q}[X, Y]$, absolutely irreducible of degree at least 2 in Y, and y a zero of $f(x, Y)$, if $\mathbf{Q}(x, y)$ has at least two distinct places over the place $x = 0$, then $H^* - V_{\mathbf{Q}}^1(f)$ is finite. The proof of Theorem 3.2 demonstrates this for those simple polynomials f arising from expression (3.4). Our next result shows this for general $f(X, Y)$. Write $f(X, Y) = h(Y) + X^r \cdot m(X, Y)$, where $h \in \mathbf{Q}[Y]$ and $m(X, Y)$ are relatively prime polynomials and $X \nmid m(X, Y)$. Now write $h(Y)/m(0, Y)$ as $\prod_{i=1}^{u} f_i(Y)^{e(i)} / \prod_{j=1}^{v} h_j(Y)^{f(j)}$ with f_i, $h_j \in \mathbf{Q}[Y]$ polynomials that are relatively prime in pairs. Notice that $u \geqq 2$ expresses that $\mathbf{Q}(x, y)$ has at least two places over $x = 0$.

Proposition 4.5 therefore includes a reproof of Theorem 3.2. Since it is effective, however, it does give Sprindžuk's result — both quantitatively and qualitatively — including also the generalizations that appear in [19].

PROPOSITION 4.5. *Use the notation of the above paragraph. If $u \geqq 2$, then $H^* - V_{\mathbf{Q}}^1(f)$ is finite, and a bound on this set can be found explicitly.*

PROOF. With no loss assume that f is monic in Y. This means that if x is an indeterminate and y is a zero of $f(x, Y)$, then y is integral over $\mathbf{Q}[x]$. In particular, the places of the function field $\mathbf{Q}(x, y)$ that are poles of y, or of any polynomial in y, are among the places that are poles in x. For $g \in \mathbf{Q}(x, y)$ use the multiplicative notation

$$(g) = p(1, g) \cdots p(t, g)/q(1, g) \cdots q(s, g)$$

to express the divisor of g as a product of places of $\mathbf{Q}(x, y)$.

Recall the main consequence of Weil's *theory of distributions* ([21] or [13; p. 132–3]). To each place p of $\mathbf{Q}(x, y)$ we may attach a function, $\delta(p) = \delta(p)(*)$, from $\mathbf{Q}$-rational places of $\mathbf{Q}(x, y)$ to $\mathbf{Z}$-ideals with the following properties. If $\delta'(p)$ are two such functions attached to p, then $\delta(p)/\delta'(p)$ takes values in a finite set of explicitly computable fractional $\mathbf{Q}$-ideals (see Remark 4.6). The same is true for $\gcd(\delta(p), \delta'(p))$, the function whose value at each $\mathbf{Q}$-rational place is the

greatest common divisor of the values of $\delta(p)$ and $\delta'(p)$ at that place. For $g \in \mathbf{Q}(x, y)$ denote by $[g]$ the function from $\mathbf{Q}$-rational places of $\mathbf{Q}(x, y)$ to fractional ideals of $\mathbf{Q}$ that maps the point (x_0, y_0) (representing a place) to the fractional ideal generated by $g(x_0, y_0)$. The main theorem of this topic [21] is that

$$[g] \cdot \delta(q(1, g)) \cdots \delta(q(s, g))/\delta(p(1, g)) \cdots \delta(p(t, g)) \tag{4.3}$$

takes values in a finite set of explicitly computable fractional $\mathbf{Q}$-ideals, as the argument runs over $\mathbf{Q}$-rational places of $\mathbf{Q}(x, y)$. For A any $\mathbf{Q}$-rational divisor on $\mathbf{Q}(x, y)$ and δ any distribution, multiply the distributions of the constituents of A to obtain $\delta(A)$.

Suppose that $u \geqq 2$, but that $H^* - V'_{\mathbf{Q}}(f)$ is infinite. Then the set $J = \{(p', a) \mid p' \in H^* \text{ and } f(p', a) = 0\}$ constitutes an infinite set of $\mathbf{Q}$-rational places of $\mathbf{Q}(x, y)$. Let $f^{(1)}$ and $f^{(2)}$ be two of the relatively prime irreducible factors of the numerator of $h(Y)/m(0, Y)$, as above. Then $(f^{(i)}) = p(i)/A(i)$ where $p(i)$ is an irreducible $\mathbf{Q}$-rational divisor and $A(i)$ is a $\mathbf{Q}$-rational divisor whose support is contained in the support of the divisor of poles of x, and $p(1)$ and $p(2)$ are contained in the support of the divisor of zeros of x. Apply expression (4.3) to x. Conclude that the distributions attached to poles of x, and to all but one of the zeros of x, must be finite valued on some infinite subset J' of J. Thus one of $f^{(1)}$ or $f^{(2)}$, say $f^{(1)}$, has a divisor whose support is among places whose distributions are finite valued on J'. Conclude from an application of (4.3) to $f^{(1)}$ that $f^{(1)}(x, y)$ is finite valued on J'. With this contradiction the proof is complete. ■

REMARK 4.6. The effectiveness part of the proof of Proposition 4.5 requires an effective computation of the distribution functions. If p is a place of $K(x, y)$, construct $\delta(p)$ as follows: Find $g^{(1)}$ and $g^{(2)} \in K(x, y)$ for which $(g^{(1)})$ and $(g^{(2)})$ have as common support only the divisor p, which appears as a pole of multiplicity one in both $g^{(1)}$ and $g^{(2)}$. Explicit construction of $g^{(1)}$ and $g^{(2)}$ is part of [3]. Then, for (x^0, y^0) a point on $f(X, Y) = 0$, $\delta(p)(x^0, y^0)$ is defined to be the common divisor (as an ideal) of the dominators of the fractional ideals generated by $g^{(1)}(a, b)$ and $g^{(2)}(a, b)$.

It is possible to imitate the proof of Proposition 4.5 to give an effective version of Proposition 4.4. Also, one of the founding papers of nonstandard arithmetic [15] seems clearly motivated by [21]. Certainly, however, an application of Weissauer's nonstandard method is quicker and slicker; especially since it is only for special fields with a product formula that one may expect an *explicitness* result. The reader should now be convinced that Proposition 4.4 is a substantial generalization of Sprindžuk's result.

We want, however, to conclude this paper with a discussion of the explicit construction of universal Hilbert subsets like those that appear in [20]. This analysis contains a p-adic analysis subtlety that is, perhaps, a bit deeper than the ideas of the proofs of Theorems 3.2 and 4.2 and Proposition 4.5.

We need the following result from [20]. We adopt the usual notations for heights of polynomials over $\mathbf{Q}$. Ordinary absolute value of $a \in \mathbf{Q}$ is denoted $|a|$, and

$$\mathrm{Ht}(a) = \left(\prod_p \max(1, p^{-\mathrm{ord}_p(a)})\right) \cdot \max(1, |a|).$$

Finally, $\mathrm{Ht}(f)$ is the maximum of the $\mathrm{Ht}(a)$ as a runs over the nonzero coefficients of f.

LEMMA 4.7. *Let $f(X, Y) \in \mathbf{Q}[X, Y]$ be irreducible. Suppose that $\deg_Y(f) = n \geqq 2$ and that $f(0, Y)$ has a simple root and is reducible. Then there exists an explicit constant $c(\deg(f)) = c$ such that $f(a, Y)$ has no linear factor for all a for which*

(4.4) (a) $$|a| \geqq (\mathrm{Ht}(f)+1)^{c(\deg(f))}; \quad \textit{and}$$

(b) *there exists a prime p for which $p^{\mathrm{ord}_p(a)} > |a|^{1-1/n^2}$.*

For example, (4.4) *holds for all but a finite computable number of the elements of the set $H^* = \{p^t \mid p \text{ is prime}, t \in \mathbf{N}\}$.*

COMMENTS. Previous arguments of this paper suffice to give the qualitative aspects of this proof. Consider, for example, the discussion after expression (3.4) and Remark 3.3. But the production of $c(\deg(f))$ with property (4.4)(a) seems more delicate, and it is (4.4)(a) that is crucial to the remainder of our discussion. ■

Let $A = \{a_m\}_{m=1}^{\infty}$ be a sequence of integers with the following properties:

(4.5) (a) for each m, a_m has a prime divisor p with $p^{\mathrm{ord}_p(a_m)} = |a_m|^{1-\chi(m)}$ where $\lim_{m\to\infty} \chi(m) = 0$; and

(b) for each prime q there exists an integer $m_0(q)$ for which q is a divisor of a_m for $m \geqq m_0(q)$.

Let $p_1 < p_2 < \cdots$ be the list of primes. Here are two sets that satisfy (4.5). Let $A_1 = \{m! \cdot 2^{m^2}\}_{m=1}^{\infty}$, where we use the prime 2 for each integer m and compute $\chi(m)$ from the formula

$$2^{\mathrm{ord}_2(m!)+m^2} = 2^{(\log_2(m!)+m^2)(1-\chi(m))}.$$

Clearly $\operatorname{ord}_2(m!) \leqq \Sigma_{r=1}^{\infty} m/2^r = m$ and by Sterling's formula $\log_2(m!) \leqq C \cdot m \log_2(m)$. Conclude that $\lim_{m\to\infty} \chi(m) = 0$. Let $A_2 = \{p^t \cdot p_1 \cdots p_{r(p)} \mid$ where for each prime p and each $t \in \mathbf{N}$, $r(p)$ is the largest integer such that $p_1 \cdots p_r < (p^t)^{1/\sqrt{\ln(p^t)}}\}$.

For a sequence A satisfying (4.5), consider $g(X, Y) \in \mathbf{Q}[X, Y]$, monic in Y, for which $g(0, Y)$ is *irreducible.* Then, by a well known consequence of the Čebotarev density theorem there exists a prime q for which $g(0, Y)\operatorname{mod}(q)$ is defined and has no linear factor. Since $g(a_m, Y) \equiv g(0, Y)\operatorname{mod}(q)$ for $m \geqq m_0(q)$,

(4.6) $g(a_m, Y)$ has no linear factor for m sufficiently large.

For the next lemma assume that $m_0(q) \leqq q^u$ for some $u > 0$ and all q.

LEMMA 4.8. *In the notation above, assume that $g(X, Y)$ is irreducible and monic in Y, and that $g(0, Y)$ is irreducible. Then there exists an explicit constant $c(\deg(g)) = c$ such that $g(a_m, Y)$ has no linear factor if $|m| \geqq (\operatorname{Ht}(g) + 1)^{c(\deg(g))}$.*

PROOF. From [12] the smallest prime q for which $g(0, Y)\operatorname{mod}(q)$ has no linear factor can be bounded by an explicit power (independent even of $\deg(g)$) of the discriminant of $g(0, Y)$. Simple estimates for a bound on the discriminant of $g(0, Y)$ in terms of $\operatorname{Ht}(g)$ give the conclusion of the lemma from (4.6). ■

THEOREM 4.9. *The set $H = \{[\exp(\sqrt{\log\log(m)})] + m!2^m,\ m = 1, 2, \ldots\}$ is a universal Hilbert subset.*

PROOF. Let $g \in \mathbf{Q}[X, Y]$, with $\deg_Y(g) \geqq 2$, be an irreducible polynomial. Let $b_m = [\exp(\sqrt{\log\log(m)})]$ and $a_m = m!2^m$, $m = 1, 2, \ldots$. It suffices to show that $g(b_m + a_m, Y)$ has no linear factor for m sufficiently large.

For m sufficiently large, $g(b_m, Y) = f(0, Y; b_m)$ has a simple zero (i.e., $X = 0$ is not a branch point of $f(X, Y; b_m)$). This explains why we need b_m to be nonconstant as a function of m.

Also, from the "slow" growth of b_m compared to a_m, it is a simple computation to show that $|m| \geqq (\operatorname{Ht}(f(X, Y; b_m)) + 1)^c$ for any $c = c(\deg(g))$ and m sufficiently large. There are two cases. If m is sufficiently large and $f(0, Y; b_m)$ is *reducible,* then Lemma 4.7 shows that $f(a_m, Y; b_m) = g(b_m + a_m, Y)$ has no linear factor. If, on the other hand, $f(0, Y; b_m)$ is irreducible, Lemma 4.8 gives the same conclusion.

Thus the usual reduction of Hilbert's irreducibility theorem to consider sets $V'_{\mathbf{Q}}(g)$ (as at the beginning of §1) allows us to conclude the theorem.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

2. Bouniakowski, *Sur les diviseurs numeriques invariables des fonctions rationelles entieres*, Mem. Acad. Sci. St. Petersburg **6** (1857), 305–329.

3. J. Coates, *Construction of rational functions on a curve*, Proc. Camb. Phil. Soc. **68** (1970), 105–123.

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

5. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

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

7. M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.

8. M. Fried, *Irreducibility results for separated variables equations*, preprint.

9. P. C. Gilmore and A. Robinson, *Mathematical consideration of the relative irreducibility of polynomials*, Can. J. Math. **7** (1955), 483–489.

10. D. Hilbert, *Über die Irreduzibilität ganzer ratzionaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. **110** (1892), 194–229.

11. van Rolf Klein, *Über Hilbertsche Körper*, J. Reine Angew. Math. **337** (1982), 171–194.

12. J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, *The bound for the least prime ideal in the Čebotare density theorem*, Invent. Math. **54** (1979), 271–296.

13. S. Lang, *Diophantine Geometry*, Interscience Publishers, New York, 1962.

14. K. S. McCurley, *Prime values of polynomials and irreducibility testing*, Bull. Am. Math. Soc. **11** (1984), 155–158.

15. A. Robinson, *Nonstandard points on algebraic curves*, J. Number Theory **5** (1973), 201–327.

16. P. Roquette, *Nonstandard aspects of Hilbert's irreducibility theorem*, in *Model Theory and Algebra, Memorial Tribute to Abraham Robinson*, Lecture Notes in Math. **498**, Springer-Verlag, Berlin, 1975, pp. 231–275.

17. C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. **1** (1929), 14–67.

18. V. G. Sprindžuk, *Reducibility of polynomials and rational points on algebraic curves*, Seminar on Number Theory, Paris, 1979–80.

19. V. G. Sprindžuk, Dokl. Akad. Nauk SSSR **250** (1980) = Soviet Math. **21** (1980), 331–334.

20. V. G. Sprindžuk, *Diophantine equations involving unknown primes*, Trudy MIAN SSR **158** (1981), 180–196.

21. A. Weil, *L'arithmetique sur les courbes algébriques*, Thèse, Paris, 1928 = Acta Math. **52** (1928), 281–315.

22. R. Weissauer, *Hilbertsche Körper*, Thesis, Heidelberg, 1980.