TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 174, December 1972

CONSTRUCTIVE PROOF OF HILBERT'S THEOREM ON ASCENDING CHAINS

BY

A. SEIDENBERG(1)

ABSTRACT. In a previous note it was shown that if a bound $f(i)$ is placed on the degrees of the elements in some basis of an ideal A_i in the polynomial ring $k[X_1, \cdots, X_n]$ over an explicitly given field k, $i = 0, 1, 2, \cdots$, then a bound can be (and was) constructed for the length of a strictly ascending chain $A_0 < A_1 < \cdots$. This result is now obtained using a strictly finitist argument. A corollary is a finitist version of Hilbert's theorem on ascending chains.

An early high point in the tradition of constructive mathematics often associated with the name of Kronecker is the paper [1] of Hermann, which treats the various ideal-theoretic notions in polynomial rings. Although the paper contains errors and obscurities, still it does make considerable contributions to the problems posed.

According to Hermann, "the assertion that a computation can be carried through in a finite number of steps shall mean that an upper bound for the number of operations needed for the computation can be given. Thus it does not suffice, for example, to give a procedure for which one can theoretically verify that it leads to the goal in a finite number of operations, so long as no upper bound for the number of these operations is known." This is obscure, really, though the intention seems clear enough in the situations actually dealt with.

In [4] we posed the following problem: A bound $f(i)$ is placed on the degrees of the elements in some basis of an ideal A_i in the polynomial ring $k[X_1, \cdots, X_n]$ over the field k, $i = 0, 1, 2, \cdots$: place a bound on the length of a strictly ascending chain $A_0 < A_1 < \cdots$. It will be convenient to regard f as having been given multi-recursively. In [4] we give a bound which is multi-recursively defined in terms of the data f and n. Our bound, unlike those given by Hermann, does not appear to be primitive recursive, but that is probably due to the problem being more complex than any dealt with by Hermann; the essence of the matter is, we say, that a *multi-recursively defined bound on the number of*

Received by the editors November 16, 1971.
AMS (MOS) subject classifications (1970). Primary 02E99, 13F20, 13E05.
Key words and phrases. Constructive mathematics, polynomial ideals, ascending chain condition.
(1) Supported in part by an NSF Grant. Written in Rome, Italy, Summer 1971.

steps needed should be given. We will not recall the definition of *multi-recursively defined* (see [2, p. 272 ff.]), but will merely remark that it in no way involves the notion of existence, either explicitly or tacitly, with the possible exception of the notion that no matter how far we count, we can count one further.

Remark. As bounding functions one could use any functions constructed without reference to existence. Consider (1) the constant functions, (2) the functions I_{nk} defined by $I_{nk}(x_1, \cdots, x_n) = x_k$, and (3) the successor function S, defined by $S(x) = x + 1$. Starting from some basic stock of functions, for example, those just mentioned, we construct further functions using only two principles: (a) substitution, and (b) induction. In particular, starting from the functions (1), (2), (3), we may construct other functions as follows: (4) $f(n_1, \cdots, n_k)$ and $g_1, \cdots, g_k$ having been constructed, we construct $f(g_1, \cdots, g_k)$; (5) functions $g(m, n_1, n_2, \cdots, n_k)$ and $h(n_2, \cdots, n_k)$ having been constructed, we construct $f(n, n_2, \cdots, n_k)$ by placing $f(0, n_2, \cdots, n_k) = h(n_2, \cdots, n_k)$ and $f(Sn, n_2, \cdots, n_k) = g(f(n, n_2, \cdots, n_k), n, n_2, \cdots, n_k)$. With this restricted scheme we get the so-called *primitive recursive functions*. More complicated schemes lead to *doubly recursive functions*, etc. Allowing arbitrary (constructed) functions to enter the scheme, we get *function-functionals*. All the bounding functions and function-functionals occurring in our proof, of which there are only a finite number, will be seen to be constructable in the above sense.

For our proof, we need a class of constructable functions which shall include the functions occurring in the proof: we take the class of functions occurring in the proof. (This is like taking $\epsilon = \epsilon/3$ in some proofs in analysis.) This class allows us to make the main point. In applications, a larger class may enter, and the point will be made again in the same way. The point of this round about way of putting things is that in this way we avoid defining *constructable function.* Anyway, it would be hopeless to construct all functions which may reasonably be regarded as constructable, as if one could list all constructable functions of one variable, $f_1, f_2, \cdots$, the function $n \mapsto f_n(n) + 1$, which would be constructable, would not be on the list.

From this point of view, the bounding functions are seen not to be of the essence of the matter: they serve as a safeguard (just as computing a bound on the cardinal number of the sets occurring in a classical set-theoretic argument serves as a safeguard). The essential point is that the existence of sets is always assured by a construction, and not, for example, by an axiom.

In [5] we considered the problem of constructing the integral closure of a finite integral domain $k[x_1, \cdots, x_n]$; assume for the moment that k is the rational number field. We first showed how to decide whether $k[x] = k[x_1, \cdots, x_n]$ is integrally closed; and, if not, how to construct an element in $k(x_1, \cdots, x_n)$ integral over $k[x]$ but not in it. Since the integral closure of $k[x]$ is a finite $k[x]$-module and $k[x]$ is Noetherian, the construction can be repeated at most a finite number of times and so would terminate in the integral closure of $k[x]$. Have we, then, given a construction for the integral closure? As we said in [5], "if one takes the view, as Hermann did, that a construction is not well-founded unless an *a priori* bound has been put on the number of steps, then the argument $\cdots$ is not complete, though it will become so in a moment. However, we cannot see that this view is justified, unless one also takes a thorough-going finitist view not only of the constructions but also of the underlying theory [though the problem of placing such a bound retains its interest even from a classical point of view]."

In the present note we are going to take precisely this thorough-going finitist view.

All of the construction problems here considered have positive outcomes. In the case of a positive resolution of a construction problem, the question of what a construction is is not, as has been said, urgent. Yes, provided we agree on the underlying theory. But here the underlying theory is an issue.

What is a construction? Since our main contributions here are some finesses in the theory of polynomial ideals, we enter reluctantly into this question. But it is a question which does have to be faced somewhat.

Following Hermann, we say that an ideal in the polynomial ring $k[X_1, \cdots, X_n]$ is given if a finite basis $f_1, \cdots, f_s$ of the ideal is given (and correspondingly, to construct an ideal is to construct for it a finite basis). If we ask how a finite basis gives an ideal, the answer surely is that we can present to ourselves the elements of the ideal under the form $g_1 f_1 + \cdots + g_s f_s$, where the g_i are polynomials. Then we must be able to present to ourselves s-tuples of elements in $k[X] = k[X_1, \cdots, X_n]$, the elements in $k[X]$, too, of course, and eventually the elements of the field k. The field k is *given*. If we ask how it is given, an answer may be that it is given by symbols which are presented to us multi-recursively, say by the integers in the range of a monotonically increasing multi-recursively defined function f having the natural numbers $0, 1, 2, \cdots$ as domain. We also want to be able to carry out the field operations. We recall that according to van der Waerden [6, p. 134], "We say that a field is *explicitly given* if its elements are uniquely represented by distinguishable symbols with which addition, subtraction, multiplication, and division can be performed in a finite number of steps." This is not good enough for us, for we must say what is meant by "can be performed...". We mean, then, that the sum $f(i) + f(j)$, for example, is a multi-recursively defined function of i, j. And similarly for subtraction, multiplication, and division a/b for $b \neq 0$. (One can find the zero element.) This definition is like, but not the same as, one given in [0].

The object of our somewhat recondite definition of explicitly given field is to prevent what we consider nonconstructive notions from entering already into the base of our considerations. In effect, however, it merely says that the field operations are to be regarded as negligible as far as construction is concerned.

An ideal could be thought of as given by a list: this would be a minimal definition—we require more.

Let $\mathfrak{A}$ be a given ideal. We may define the complement as made up of the elements not in $\mathfrak{A}$; but we do not regard a definition as a guarantee for existence. We regard the complement as existing if we can give a list of the elements not in $\mathfrak{A}$. As we shall see, it is possible to decide for any given poly-

nomial g whether g is in $\mathfrak{A}$. This yields the existence of the complement of $\mathfrak{A}$. Thus comp($\mathfrak{A}$), the complement, is a list constructed according to certain instructions. When we say g is in comp ($\mathfrak{A}$), we understand that we also have instructions for locating g in comp($\mathfrak{A}$). This can easily be arranged and will be understood.

Our proof of a constructive version of Hilbert's theorem on ascending chains of ideals now comes to going over our paper [4] with the new point of view in mind. There is only one difficulty, Lemma 4, which says that *if* $A = (f_1, \cdots, f_s)$ *is a given ideal in* $k[X_1, \cdots, X_n]$ *and if at least one of the* f_i *is regular in* $X_1, \cdots, X_n$ (i.e., contains a term $c_i X_n^{\deg f_i}$ with $c_i \in k - 0$), *then one can construct an* X_n^ρ *and the ideal* $A : X_n^\rho$ *such that* $A : X_n^\rho = A : X_n^{\rho+1}$; *and one can do this in a number of steps depending only on* n, s, *and* $d = \max\{\deg f_i\}$. Actually, a somewhat weaker assertion, in which one introduces n^2 indeterminates u_{ij} and works with the "transformed" variables $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$ and the extended ideal $k(u)[X]A$ over the field $k(u) = k(\cdots, u_{ij}, \cdots)$, is sufficient.

In [4], we merely said this was known from [1]. This, from our present point of view, cannot now be said to be the case; and, indeed, it is the crux of the matter.

1. **The constructive proof.** Given ideals $\mathfrak{A}$, $\mathfrak{B}$ in $k[X_1, \cdots, X_n]$ via bases $f_1, \cdots, f_s$ and $g_1, \cdots, g_t$, we shall want to construct $\mathfrak{A} \cap \mathfrak{B}$ and $\mathfrak{A} : \mathfrak{B}$. Given an element b in $k[X_1, \cdots, X_n]$, we shall want to be able to decide whether b is in $\mathfrak{A} = (f_1, \cdots, f_s)$, and if it is, to find $b_1, \cdots, b_s$ in $k[X] = k[X_1, \cdots, X_n]$ such that $b = b_1 f_1 + \cdots + b_s f_s$. These things are known from [1], and since the proofs occur at an early stage, we may safely refer to [1] for the technical details. Here k is, of course, explicitly given, and the constructions are to be done in a number of steps recursively defined in terms of n, the number of polynomials given, and their degrees. Here by a *step* we mean a field operation in k; if instead we wish *step* to mean an operation with the natural numbers, then the number of steps will depend recursively on the coefficients of the given polynomials.

Let $n \geq 2$ and place $R = k[X_1, \cdots, X_n]$, $S = k(X_1)[X_2, \cdots, X_n]$, $R_n = k[X_1, \cdots, X_{n-1}]$, $S_n = k(X_1)[X_2, \cdots, X_{n-1}]$. Consider a free R-module with $Z_1, \cdots, Z_s$ as free generators. Let $l_i = f_{i1}Z_1 + \cdots + f_{is}Z_s$, $i = 1, \cdots, t$, with the f_{ij} in $k[X_1, \cdots, X_n]$, and consider the R-module m generated by $l_1, \cdots, l_t$. We are interested in computing $S \cdot m \cap \Sigma R Z_j$. Let the matrix $\|f_{ij}\|$ be of rank p. We say that the basis $l_1, \cdots, l_t$ is *regular with respect to* $X_1, \cdots, X_n$ if at least one of the p-rowed subdeterminants is regular in $X_1, \cdots, X_n$; and that m is *regular with respect to* $X_1, \cdots, X_n$ if m has a basis $l_1, \cdots, l_t$ of the kind mentioned

Let $N \geq 0$ be an integer and consider the R_n-module n generated by $l_1, \cdots, l_t$, $X_n l_1, \cdots, X_n l_t, \cdots, X_n^N l_1, \cdots, X_n^N l_t$. Place $\zeta_{i+sj} = Z_i X_n^j$. Then n is con-

tained in the free R_n-module generated by the ζ_{i+sj}, $j = 0, \cdots, N+q$, where $q \geq \max\{\deg f_{ij}\}$. In [3, p. 381] we proved the following:

Lemma. *If m is regular with respect to $X_1, \cdots, X_n$ $(n \geq 2)$, then*

$$S \cdot m \cap \sum_1^s R \cdot Z_i = m + R \cdot \left(S_n n \cap \sum_1^g R_n \zeta_i \right),$$

where we suppose $l_1, \cdots, l_t$ to be a given regular basis, $N = qt$, and $g = s + s(N+q)$.

This was written from a simple classical point of view (we may also remark that in [3] the base field k had been extended by an indeterminate r to a base field $k(r)$, but this played no role in the lemma). From a constructivist point of view, we can say that the left-hand side can be constructed if $S_n \cdot n \cap \Sigma R_n \zeta_i$ can; otherwise, we have gotten nowhere. Now to construct $S_n \cdot n \cap \Sigma R_n \zeta_i$ we would need a regularity condition on n, and in fact on a chain of similar modules. Assume for a moment that k is infinite. Then by a homogeneous nonsingular linear transformation on $X_1, \cdots, X_n$ we can go over to variables $X_1', \cdots, X_n'$ such that m is regular with respect to $X_1', \cdots, X_n'$; then by a homogeneous nonsingular linear transformation of $X_1', \cdots, X_{n-1}'$ we go over to variables $X_1'', \cdots, X_{n-1}'', X_n'$ such that n is regular with respect to $X_1'', \cdots, X_{n-1}''$ and m is still regular with respect to $X_1'', \cdots, X_{n-1}'', X_n'$. And so on with further transformations, to get the other regularity conditions. Thus for some change of the variables, we could construct $S \cdot m \cap \Sigma RZ_i$.

Dropping the assumption on k, we proceed as follows. We adjoin n^2 indeterminates u_{ij} to k to get $k(u) = k(\cdots, u_{ij}, \cdots)$, let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, and place $R^u = k(u)[X_1', \cdots, X_n']$, $S^u = k(u, X_1')[X_2', \cdots, X_n']$, $R_n^u = k(u)[X_1', \cdots, X_{n-1}']$, $S_n^u = k(u, X_1')[X_2', \cdots, X_{n-1}']$. One checks that m is regular with respect to $X_1', \cdots, X_n'$. To get the regularity condition for n (now an R_n^u-module), we could introduce further indeterminates and another linear transformation, probably without creating any difficulty, but we may as well note, at least for notational simplicity, that n already is regular with respect to $X_1', \cdots, X_{n-1}'$. Let $\Delta = d(u, X_1', \cdots, X_{n-1}')$ be one of the determinants whose regularity is in question. Let v_{ij}, $i, j = 1, \cdots, n-1$, be $(n-1)^2$ further indeterminates and place $X_i'' = v_{i1}X_1' + \cdots + v_{in-1}X_{n-1}'$, $i = 1, \cdots, n-1$, $X_n'' = X_n'$. Let $v_{n1} = \cdots = v_{n,n-1} = 0$, $v_{1n} = \cdots = v_{n-1,n} = 0$, $v_{nn} = 1$. Let $V = \|v_{ij}\|$, $U = \|u_{ij}\|$, $W = \|w_{ij}\| = VU$. Clearly $\Delta = d(w, X_1'', \cdots, X_{n-1}'')$, for the same d. (The substitution $X \to X'$ leads from m to $\Delta = d(u, X_1', \cdots, X_{n-1}')$; the substitution $X \to X''$ correspspondingly leads from m to $\Delta' = d(w, X_1'', \cdots, X_{n-1}'')$. On the other hand, the substitution $X \to X''$ can be effected in two steps, $X \to X'$ and $X' \to X''$, the

second of which is a transformation from $X_1', \cdots, X_{n-1}'$ to $X_1'', \cdots, X_{n-1}''$, so Δ does not change, i.e., $\Delta' = \Delta$.) If $G(X, V, W) = G(X, V, VU) = 0$, then $G(X, V, VV^{-1}U) = G(X, V, U) = 0$. Hence the substitution $u_{ij} \to w_{ij}$ yields an isomorphism $k(U, V)/k(X) \to k(W, X)/k(X)$. $\Delta = d(w; X_1'', \cdots, X_{n-1}'')$ is obviously regular in $X_1'', \cdots, X_{n-1}''$. Hence by isomorphism $d(u, X_1', \cdots, X_{n-1}'')$ is also regular in $X_1', \cdots, X_{n-1}'$. Q.E.D.

Similarly, the other regularity conditions obtain without further transformations. Hence we have:

Lemma 1. *The module* $S^u \cdot m \cap \Sigma_1^s R^u Z_i$ *can be constructed.*

Corollary. *Let* $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, *with the* u_{ij} n^2 *indeterminates, and let* $\mathfrak{A}$ *be a given ideal in* $k[X_1, \cdots, X_n]$. *Then one can construct* $k(u, X_1')[X_2', \cdots, X_n']\mathfrak{A} \cap k(u)[X_1, \cdots, X_n]$.

This is just the case $s = 1$ of the lemma.

Lemma 2. *Let the notation be as in Lemma* 1, *corollary. Then*

$$\mathfrak{B} = k(u, X_1')[X_2', \cdots, X_n']\mathfrak{A} \cap k(u)[X_1, \cdots, X_n]$$

has a basis (which we can construct) in $k[X_1, \cdots, X_n]$.

Proof. We have a basis of $\mathfrak{B}$ in $k(u)[X_1, \cdots, X_n]$ and may suppose it to be in $k[u, X_1, \cdots, X_n]$. Let $g(u, X)$ be one of the basis elements and consider one of the u_{ij}. We have an $E(u, X)$ in $k[u, X_1']$ such that Eg is in $k[u, X]\mathfrak{A}$. Then also $(\partial E/\partial u_{ij})g + E\partial g/\partial u_{ij}$ and $E^2\partial g/\partial u_{ij}$ are in $k[u, X]\mathfrak{A}$. Hence $\partial g/\partial u_{ij}$ is in $\mathfrak{B}$. If k is of characteristic zero, we see in this way that the coefficients of g written as a polynomial in u_{ij} are in $\mathfrak{B}$. In characteristic $p > 0$, we see likewise that if g is written as a linear combination of $1, u_{ij}, \cdots, u_{ij}^{p-1}$ with coefficients involving u_{ij} only to powers divisible by p, then these coefficients are in $\mathfrak{B}$. So we may assume g involves u_{ij} only to powers divisible by p. Now we have $E^p g$ is in $\mathfrak{A}$ for suitable E. Place $v = u_{ij}^p$. Then $E^p \partial g/\partial v$ is in $\mathfrak{A}$. Hence we may suppose g involves u_{ij} only to powers divisible by p^2; etc., so we may suppose g devoid of u_{ij}; and similarly for all the u_{ij}. The lemma is proved.

Remark. If we had the primary decomposition theorem, Lemma 2 would be immediate, as $\mathfrak{B}$ is nothing but the extension to $k(u)[X_1, \cdots, X_n]$ of the intersection of the primary components of positive dimension in a normal decomposition of $\mathfrak{A}$.

Quite generally, if R and S are rings with $R \subset S$ and $\mathfrak{A}$ is an ideal with $S\mathfrak{A} \cap R = \mathfrak{A}$ we can often without confusion denote the ideal $S\mathfrak{A}$ by $\mathfrak{A}$. In particular, if $R = k[X_1, \cdots, X_n]$ and we extend the base field k by some indeterminates u to get $S = k(u)[X_1, \cdots, X_n]$, we will do this. Then if $\mathfrak{A}$ is an ideal in S which has a basis in R, we can denote the contraction $R \cap \mathfrak{A}$ also by $\mathfrak{A}$. In particular, if $\mathfrak{B}$ is the ideal of Lemma 2, we also use $\mathfrak{B}$ to denote $\mathfrak{B} \cap k[X_1, \cdots, X_n]$. In the case $R = k[X_1, \ldots, X_n]$, $S =$

$k(u)[X_1, \cdots, X_n]$, where u is an indeterminate, if $\mathfrak{A}$, $\mathfrak{B}$ are arbitrary R-ideals, then $S(\mathfrak{A} \cap \mathfrak{B}) = S\mathfrak{A} \cap S\mathfrak{B}$ and $S\mathfrak{A} : S\mathfrak{B} = S(\mathfrak{A} : \mathfrak{B})$, so no confusion will arise by denoting these ideals by $\mathfrak{A} \cap \mathfrak{B}$ and $\mathfrak{A} : \mathfrak{B}$.

Unloading some superfluous u_{ij} in Lemma 2, we get

Corollary. $k(u_{11}, \cdots, u_{1n}, X_1')[X_1, \cdots, X_n]\mathfrak{A} \cap k(u_{11}, \cdots, u_{1n})[X] = k(u_{11}, \cdots, u_{1n})[X]\mathfrak{B}$.

Let the notation be as in the preceding corollary. We can find an E_1 in $k[u_{11}, \cdots, u_{1n}, X_1']$ such that $E_1\mathfrak{B} \subset \mathfrak{A}$, so $\mathfrak{B} \subset \mathfrak{A} : E_1$ (in $k(u_{11}, \cdots, u_{1n})[X]$). Now also $\mathfrak{A} : E_1 \subset \mathfrak{B}$, since if $g \in k(u_{11}, \cdots, u_{1n})[X]$ and $gE_1 \in \mathfrak{A}$, then obviously g is in $\mathfrak{B}$. So $\mathfrak{A} : E_1 = \mathfrak{B}$. Note also that $\mathfrak{B} : E_1 = \mathfrak{B}$, since if $gE_1 \in \mathfrak{B}$, then $gE_1^2 \in \mathfrak{A}$ and $g \in \mathfrak{B}$. Now we say $(\mathfrak{A}, E_1) \cap \mathfrak{B} = \mathfrak{A}$. In fact, the right-hand side is obviously in the left; conversely, let $g \in (\mathfrak{A}, E_1) \cap \mathfrak{B}$. Then $g = bE_1 + a$, with $b, a \in k(u_{11}, \cdots, u_{1n})[X]$ and $a \in \mathfrak{A}$. Since $g \in \mathfrak{B}$, $gE_1 \in \mathfrak{A}$, whence $bE_1^2 \in \mathfrak{A}$. From this $bE_1 \in \mathfrak{B}$ and $b \in \mathfrak{B}$. Hence $bE_1 \in \mathfrak{A}$ and $g \in \mathfrak{A}$, so equality is proved.

Now extend the base field with the further indeterminates $u_{21}, \cdots, u_{2n}$ and repeat the argument. Then $(\mathfrak{A}, E_1, E_2) \cap \mathfrak{B}_1 = (\mathfrak{A}, E_1)$; here $E_2 = E_2(X_2')$ and $\mathfrak{B}_1 : E_2 = \mathfrak{B}_1$. The equality $(\mathfrak{A}, E_1) \cap \mathfrak{B} = \mathfrak{A}$ continues to hold in the extended ring, so $(\mathfrak{A}, E_1, E_2) \cap \mathfrak{B}_1 \cap \mathfrak{B} = \mathfrak{A}$. Repeating the argument several times we get $(\mathfrak{A}, E_1, E_2, \cdots, E_n) \cap \mathfrak{B}_{n-1} \cap \cdots \cap \mathfrak{B} = \mathfrak{A}$; here we are in the ring $k(u)[X_1, \cdots, X_n]$; $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$; $E_i = E_i(X_i')$; and $\mathfrak{B}_{i-1} : E_i = \mathfrak{B}_{i-1}$.

We noted that $\mathfrak{B} : E_1 = \mathfrak{B}$, but the same proof shows that $\mathfrak{B} : F_1 = \mathfrak{B}$ for any $F_1 \neq 0$ in $k(u_{11}, \cdots, u_{1n})[X_1']$. Similarly $\mathfrak{B}_1 : F_2 = \mathfrak{B}_1$ for any $F_2 \neq 0$ in $k(u_{11}, u_{21}, \cdots, u_{n1}, u_{n2})[X_2']$. Now also, however, $\mathfrak{B} : F_2 = \mathfrak{B}$. In fact, let $bF_2 \in \mathfrak{B}$. Consider the automorphism of $k(u_{11}, u_{21}, \cdots, u_{n1}, u_{n2})/k$ obtained by interchanging u_{i1}, u_{i2}, $i = 1, \cdots, n$. Then b goes over into b' and F_2 into F_2', while $\mathfrak{B}$, since it is an extended ideal, remains invariant. Then $b'F_2' \in \mathfrak{B}$. Since X_2' goes over into X_1', $F_2' = F_2'(X_1')$. Now one finds, for example, $(\partial b'/\partial u_{21})F_2'^2 \in \mathfrak{B}$, and arguing as before we get $b' \in \mathfrak{B}$. Applying the automorphism again, $b \in \mathfrak{B}$. Similarly we get

$$(\mathfrak{B}_{n-1} \cap \cdots \cap \mathfrak{B}) : F = \mathfrak{B}_{n-1} \cap \cdots \cap \mathfrak{B}$$

for any F in $k(u)[X_n'] - 0$.

Remark. If we had the normal decomposition theorem, etc., at our disposal, we could note that the $\mathfrak{B}_i$ have no 0-dimensional components. This would make the argument a little more transparent.

In particular, we have the above equality for $F = X_n'$. Hence to find a ρ such that $\mathfrak{A} : X_n'^{\rho} = \mathfrak{A} : X_n'^{\rho+1}$ comes to finding a ρ such that

$$(\mathfrak{A}, E_1, \cdots, E_n) : X_n'^{\rho} = (\mathfrak{A}, E_1, \cdots, E_n) : X_n'^{\rho+1}.$$

Now, however, $k(u)[X]/(\mathfrak{A}, E_1, \cdots, E_n)$ is obviously a finite $k(u)[X]$-module of length at most $\Sigma \deg E_i$. Hence $\Sigma \deg E_i$ gives us a desired ρ. Thus we have proved

Theorem 1. *Let $\mathfrak{A}$ be a given ideal in the polynomial ring $k[X_1, \cdots, X_n]$ and let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, where the u_{ij} are indeterminates. Then one can compute a ρ such that $\mathfrak{A} : X_n'^{\rho} = \mathfrak{A} : X_n'^{\rho+1}$.*

In Lemma 4 of [4], given an ideal $\mathfrak{A}$ in $k[X_1, \cdots, X_n]$ we sought a ρ such that $A : X_n^{\rho} = A : X_n^{\rho+1}$. However, as far as the application is concerned, we could just as well have extended the base field and worked with the transformed variables $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, n$. With this remark, the proof is complete.

In [4], we gave two solutions of the problem posed, the second of which was a free treatment of a solution communicated by the referee. It will be well to compare these two solutions. First, the second solution first gets the existence of the bound, then proceeds to its construction, whereas our view is that existence can only be guaranteed via a construction. Second, the second solution uses Hilbert's ascending chain theorem (and Zorn's lemma), thus typically nonconstructive arguments, whereas ours on the contrary (with the present supplements) yields a constructive version of Hilbert's theorem. Third, we actually have formulae for computing the bound, whereas the second solution proposes to get a bound by a probing process. Finally, from our present point of view, one, however, which was already roughly indicated in [4], the second solution begs the question.

In spite of these defects, the referee's solution has a very appealing element, namely, it gives the existence of the desired bound with an immediacy which the first solution cannot match. On the other hand, the construction assertion is somewhat less than appealing: it uses a notion of construction which was devised for negative purposes, but which is, as we see it, incorrect or incomplete for positive ones.

REFERENCES

A. Frölich and J. C. Shepherdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. London Ser. A. **248** (1956), 407–432. MR **17**, 570.

G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math Ann. **95** (1926), 736–788.

2. S. C. Kleene, *Introduction to metamathematics*, Van Nostrand, Princeton, N. J., 1952. MR **14**, 525.

3. A. Seidenberg, *The hyperplane sections of normal varieties*, Trans. Amer. Math. Soc. **69** (1950), 357–386. MR **12**, 279.

4. ———, *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. **29** (1971), 443–450. MR **43** #6193.

5. ———, *Construction of the integral closure of a finite integral domain*, Rend. Semi. Mat. Fis. Milano **40** (1970), 1–22.

6. B. L. van der Waerden, *Moderne Algebra*, Vol. 1, 2nd ed., Ungar, New York, 1937.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720