TRANSACTIONS
AMERICAN MATHEMATICAL SOCIETY
Volume 197, 1974

CONSTRUCTIONS IN ALGEBRA

BY

A. SEIDENBERG[1]

ABSTRACT. It is shown how to construct a primary decomposition and to find the associated prime ideals of a given ideal in a polynomial ring. This is first done from a classical, and then from a strictly constructivist, point of view.

An early high point in the tradition of constructive mathematics often associated with the name of Kronecker is the paper [1] of Hermann, in which the various ideal-theoretic notions in a polynomial ring $k[X_1, \cdots, X_n]$ over a field k are considered. For example, given ideals A and B, Hermann shows how to construct $A \cap B$ and $A : B$. Here the ideals A and B are given via (finite) bases, and the problem is to construct bases for $A \cap B$ and $A : B$. It is assumed that one can carry out the field operations in k (in one step per operation), in other words, that k is *explicitly given* (cf. [11]); throughout we assume, sometimes tacitly, that k is explicitly given.

Hermann has also considered the problem of constructing the associated primes of a given ideal A. The simplest case of this problem comes to showing how to construct the complete factorization in $k[X]$ of any given polynomial in one letter X. If k is a field for which this can be done, we say that the *factorization theorem* holds for k, or that k satisfies *condition* (F). Unfortunately, Hermann persuaded herself that any explicitly given field satisfies (F). In [10], van der Waerden pointed out the error; moreover, he showed, with a slight qualification, that it is impossible to prove that (F) holds for an arbitrary explicitly given field. Thus to get Hermann's Theorem 11, which asserts the constructibility of the associated primes, one has to assume at least that the base field k satisfies (F); but even this, as we have shown in [6], does not suffice.

Van der Waerden did not go on to examine the repercussions in Hermann's paper

Received by the editors April 27, 1973.

AMS (MOS) subject classifications (1970). Primary 02E99, 13F20, 13E05.

Key words and phrases. Constructive mathematics, polynomial ideals.

[1] Member of the Centro Interdisciplinare di Scienze Matematicoe Loro Applicazioni of the Accademia Nazionale dei Lincei, Rome, Italy, Fall 1972.

of the error mentioned, and since (hopefully) there is no further overt error,[2] one might well be left with the impression that all the constructions hold for any explicitly given k satisfying (F). This notion has also entered the literature. Thus in [9] Stolzenberg has sought to construct the integral closure of a finite integral domain $k[x_1, \cdots, x_n]$; here k is assumed to satisfy (F) (and $k(x_1, \cdots, x_n)$ is also assumed to be separable over k). In [6], however, we have shown that the construction does not hold with the generality claimed. The difficulty goes back to Hermann's Theorem 11, which, as already mentioned, requires more than condition (F).

In the proof of Theorem 10, in making an induction on n, the number of indeterminates, Hermann adjoins an (algebraic) element x_1 to k to get a new base field $k(x_1)$. But condition (F) may no longer hold for $k(x_1)$! This error could not impinge on Hermann's attention, since she thought (F) was automatic.

In [5], we introduced a condition (P) for a field k of given characteristic p: we recall the definition below and merely remark here that it allows us to tell for any $a_1, \cdots, a_s$ in k whether $[k^p(a_1, \cdots, a_s) : k^p] = p^s$, and is, roughly, equivalent to this. As we will show, all of our constructions hold for a field k satisfying (F) and (P).

Because of the errors in [1] and the resulting confusion, we have often thought it would be well if this work would be redone; Hermann's paper is a historically important, and also admirable, work, but its usefulness as a reference is somewhat diminished. Our first object, then, is to supply a new reference for the ideal-theoretic constructions in $k[X_1, \cdots, X_n]$. We are not content, however, to assume (F) and (P) at the outset, but want to show which conditions enter a given construction. For example, an ideal A can be written as the intersection of unmixed ideals for any explicitly given field k; (F) is sufficient to get a primary decomposition; and (F) and (P) are necessary and sufficient to get the associated primes. We also consider some constructions not taken up by Hermann. For example, we show

[2] Professor G. Stolzenberg has kindly informed us of an error in Hermann's Satz 4. Let $m = (f_1, \cdots, f_t)$ be a given ideal in $R = k[X_1, \cdots, X_n]$ and $q = \max\{\deg f_i\}$. Let $1 \leq r \leq n$, let $g \in R$, and let $g^* = g$ homogenized with respect to $X_1, \cdots, X_r$, i.e., $g^* = X_0^s g(X_1/X_0, \cdots, X_r/X_0, X_{r+1}, \cdots, X_n)$, where $s =$ degree of g in $X_1, \cdots, X_r$. In the proof (p. 754), Hermann claims to compute an integer k depending only on n, r and q such that $X_0^k g^* \equiv 0 \ (f_1^*, \cdots, f_t^*)$ for any $g \equiv 0 \ (m)$. This claim will be seen to be unjustified if one thinks of a g having small degree in $X_1, \cdots, X_r$ relative to its degree in all the variables. However, such an exponent k does exist: in fact, take k to be such that $(f_1^*, \cdots, f_t^*) : X_0^k = (f_1^*, \cdots, f_t^*) : X_0^{k+1}$. Moreover, one can compute k by 20, below. Then arguing as Hermann does, one can construct polynomials $f_{r1}, \cdots, f_{rt_r}$ in m such that any $g \equiv 0 \ (m)$ can be written in the form $g = \Sigma g_i f_{ri}$ with $[g_i f_{ri}]_r \leq [g]_r$ for every $g_i \neq 0$, where $[\cdot\cdot]_r =$ degree in $X_1, \cdots, X_r$.

how for a given ideal A in $k[X_1, \cdots, X_n]$ and in the presence of (F) to construct $A \cap k[X_1, \cdots, X_{n-1}]$; if A is primary, this can even be done for any explicitly given base field.[3]

Something still has to be said on what is meant by a construction. 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 operations is known." This is obscure, really, since one has to *construct* the bounds, so the question of what a construction is remains; but the intention seems clear enough in the situations actually dealt with. Moreover in many cases Hermann writes down bounds which are simple functions of the numerical data, and presumably could have done so in all.

It may be well to give an example of an argument which some authors would consider constructive but which Hermann does not, nor (for the present) do we. Let $A = (f_1, \cdots, f_r)$ and $B = (g_1, \cdots, g_s)$ be two ideals in $k[X_1, \cdots, X_n]$: to find a ρ such that $A : B^\rho = A : B^{\rho+1}$. That there is such a ρ follows from the ascending chain condition in $k[X_1, \cdots, X_n]$; and Hermann in no way takes exception to the classical reasoning giving us its existence. To actually find ρ we could proceed as follows: We compute $A : B$ and compare it with A. If $A = A : B$, then $\rho = 0$ is a desired solution. If $A \neq A : B$, then we compute $A : B^2$ and compare it with $A : B$. If $A : B = A : B^2$, then $\rho = 1$ is a desired solution. If $A : B < A : B^2$, we repeat the procedure, getting a chain $A < A : B < A : B^2 < \cdots$. This procedure must terminate, and when it does, we have the desired ρ. But, as said, Hermann does not allow this to count as a construction.

In the first part of the following work (1–72) we adopt a simple classical point of view and will consider the above remarks as sufficiently indicating our intent. In every case, formulae giving the bounding functions are written down (or sufficient indications are given for doing so). The functions are referred to as *multi-recursive*. The exact definition of this term is not important: the only thing important about the bounding functions is that they should be defined without reference to existence. This will be seen to be the case for all the functions occurring in our proofs.

Although we were initially guided by Hermann's remarks, we have already some time ago (cf. [5], [8]) come to the view that her position is untenable. The constructions are, of course, finite in nature, but the underlying theory is not. If one accepts the classical reasoning whereby one first gets the *existence* of the

[3] Subsequently, we have shown that condition (F) can be removed; see footnote 4.

desired object, then we can see no reason for not accepting the above considerations for finding a ρ such that $A : B^{\rho} = A : B^{\rho+1}$ as a construction. At the same time we maintained a lively conviction that the considerations should *not* count as a construction! The way out is to reject the classical mode of reasoning. This requires, of course, a radical shift in point of view. The essential point of this second view is that existence can only be guaranteed by a construction (and not, as often classically, by an axiom). Construction comes first, then the declaration of existence.

In the second part of the work (73–96), we have gone over our constructions from the new point of view. The result is that we get not only our constructions but also the whole theory of polynomial ideals over a field in strictly finite terms.

Notation. A set of subscripted letters is often abbreviated by the same letter without a subscript: thus the n-tuple $X_1, \cdots, X_n$ is abbreviated to X. Capital letters are reserved for indeterminates: thus the $X_1, \cdots, X_n$ in $k[X_1, \cdots, X_n]$ are indeterminates.

Constructions holding for an arbitrary explicitly given base field k.

1. Given a system of homogeneous equations $f_{i1}g_1 + \cdots + f_{is}g_s = 0$, $i = 1, \cdots, r$, $f_{ij} \in k[X_1, \cdots, X_n] = k[X]$, one can construct a $k[X]$-module basis for the solutions $(g_1, \cdots, g_s)$, $g_j \in k[X]$. Moreover, this can be done in a number of steps depending only on n, r, s, and $d = \max \deg f_{ij}$ (or, also, only on a bound for these). By a *step* is meant a field operation in k.

Proof. Let u be an indeterminate over k and suppose $(g_1(u; X), \cdots, g_s(u; X))$ is a solution over $k(u)$. Multiply the $g_i(u; X)$ by a common denominator, so that one may suppose the $g_i(u, X)$ are in $k[u, X]$. Now in the $g_i(u, X)$ consider the coefficients of any power of u. Then this gives a solution. Hence from a basis of solutions over $k(u)$ one can get a basis over k. *So k may be assumed infinite.*

We may suppose the r equations are linearly independent over $k(X)$, and by notation that

$$\Delta = \begin{vmatrix} f_{11} \cdots f_{1r} \\ \vdots \\ f_{r1} \cdots f_{rr} \end{vmatrix} \neq 0.$$

Moreover, since k is infinite, by a nonsingular homogeneous linear transformation we may assume that Δ is *regular in* $(X_1, \cdots, X_n)$ i.e., the coefficient of the highest power of X_n in Δ is free of $X_1, \cdots, X_{n-1}$. Then we can bring the equations to the equivalent form:

$$\begin{aligned} \Delta g_1 &= (\,\cdot\,\cdot\,)g_{r+1} + \cdots + (\,\cdot\,\cdot\,)g_s \\ &\;\vdots \\ \Delta g_r &= (\,\cdot\,\cdot\,)g_{r+1} + \cdots + (\,\cdot\,\cdot\,)g_s, \end{aligned}$$

where the $(\cdot\cdot)$ are in $k[X]$. Now we note the existence of solutions

$$(g_{11},\cdots,g_{1r};\Delta,0,\cdots,0),\cdots,(g_{s1},\cdots,g_{sr};0,\cdots,0,\Delta).$$

These permit us to bound the degrees in X_n of the sought $g_{r+1},\cdots,g_s$, and hence also the degrees of $g_1,\cdots,g_r$. Now one can rewrite the equations in terms of $X_1,\cdots,X_{n-1}$.

As to the number of steps, it is clear from the proof so far that the number ϕ of steps needed is a function only of n, r, s, and d (and not of the coefficients of the f_{ij}). Moreover, $\phi=\phi(n,r,s,d)$ may be assumed to be monotone increasing in each of its variables. In fact, if, for example, $\phi=\phi(r)$ is a function of say one variable that is to serve as a bound, we may suppose $\phi(r)$ is monotone increasing by replacing $\phi(r)$ by $r+\phi(r)+\phi(r-1)+\cdots+\phi(0)$. Thus we may suppose $\phi=\phi(n,r,s,d)$ is monotone increasing in each variable. If $b\geq\max\{n,r,s,d\}$, then $\phi(b,b,b,b)$ will also be a desired bound.

Remark. The proof does not hold for the ring of integers Z at the base instead of k. For we would need not merely that coefficient of the highest power of X_n in Δ should be free of $X_1,\cdots,X_{n-1}$, but that it should be a *unit* in Z. Thus our problems remain unsolved for the ring of integers at the base.

2. Given two ideals $A=(f_1,\cdots,f_r)$, $B=(f_{r+1},\cdots,f_s)$ in $k[X_1,\cdots,X_n]$, one can construct $A\cap B$.

Proof. Obviously, it suffices to find the $(g_1,\cdots,g_s)$ such that $g_1f_1+\cdots+g_rf_r=g_{r+1}f_{r+1}+\cdots+g_sf_s$.

Remark. Here, as throughout this section, one can make a statement as in 1 on the number of steps.

3. Similarly, one can construct $A:B$.

4. Given a system of nonhomogeneous equations

$$f_{i1}g_1+\cdots+f_{is}g_s=b_i,\quad i=1,\cdots,r,\ f_{ij},\ b_i\in k[X_1,\cdots,X_n]=k[X],$$

one can decide whether the system has a solution in $k[X]$, and if it does, one can find one.

Proof. As in the homogeneous case, we may assume k is infinite. We may as well assume that rank of coefficient matrix = rank of augmented matrix, or that the system has a solution in $k(X)$. Then we may assume the system to be in the form:

$$\begin{aligned}\Delta g_1&=(\cdot\cdot)g_{r+1}+\cdots+(\cdot\cdot)g_s+c_1\\&\ \vdots\\\Delta g_r&=(\cdot\cdot)g_{r+1}+\cdots+(\cdot\cdot)g_s+c_s,\end{aligned}$$

where the $(\cdot\cdot)$ are in $k[X]$. Since k is infinite, we may assume Δ to be regular. Subtracting solutions of the corresponding homogeneous system, we may bound the degrees of the g_i in X_n. Then we can rewrite the system in terms of $X_1, \cdots, X_{n-1}$.

5. Given an ideal $A = (f_1, \cdots, f_s)$ and an element b in $k[X_1, \cdots, X_n]$, one can decide whether b is in A, and if it is, one can find $g_1, \cdots, g_s$ in $k[X]$ such that $b = g_1 f_1 + \cdots + g_s f_s$. In particular, one can decide whether $A = (1)$.

This is an immediate application of 4.

6. By the *dimension* of a prime ideal P in $k[X_1, \cdots, X_n]$ one means the degree of transcendency of $k[X]/P$ over k. By the *dimension* of any ideal $A \neq (1)$ one means the maximum of the dimensions of the associated primes. Thus $\dim A = \max\{r \mid X_{i_1}, \cdots, X_{i_r}$ are algebraically independent over k mod $A\}$. For $A = (1)$ one places $\dim A = -1$.

Given $A = (f_1, \cdots, f_s)$ in $k[X_1, \cdots, X_n]$, one can decide whether $X_1, \cdots, X_r$ are algebraically independent over k mod A. In particular, one may find $\dim A$, the dimension of A. If $X_1, \cdots, X_r$ are algebraically dependent over k mod A, one can find an $f \in k[X_1, \cdots, X_r] - 0$ such that $f \in A$.

Proof. One has but to consider the ideal $k(X_1, \cdots, X_r)[X_{r+1}, \cdots, X_n]A$.

7. If A is 0-dimensional, one can put a bound on the dimensions of $k[X]/k[X]A$ as a k-linear space.

Proof. By 6, one can find $f_i \in k[X_i] - 0$, $i = 1, \cdots, n$, such that $f_i(X_i) \in A$. Then Π degree f_i is a desired bound.

8. Let $X = X_1$ (i.e., $n = 1$), $R = k[X]$, $S = k(X)$, $RZ_1 + \cdots + RZ_s$ a free R-module with $Z_1, \cdots, Z_s$ as free generators, $m = (l_1, \cdots, l_t)$ a submodule; here $l_i = f_{i1}(X)Z_1 + \cdots + f_{is}(X)Z_s$, with $f_{ij} \in k[X]$. Then one can construct $Sm \cap \Sigma\, RZ_i$.

Proof. Let rank $\|f_{ij}\| = r$. By the so-called "Elementarteilersatz" (cf. [12]), one can find free generators $Z_1', \cdots, Z_s'$ of $\Sigma\, RZ_i$ and a new basis $l_1', \cdots, l_r'$ of m such that $l_i' = g_i(X)Z_i'$ with $g_i \in k[X]$. Then, clearly, $Sm \cap \Sigma\, RZ_i = (Z_1', \cdots, Z_r')$.

Remark. Here we need a constructive form of the "Elementarteilersatz," and not merely a statement of existence, but the familiar proof of [12] is already of the desired form.

9. Let $n \geq 2$. Place

$$R = k[X_1, \cdots, X_n], \qquad S = k(X_1)[X_2, \cdots, X_n],$$

$$R_n = k[X_1, \cdots, X_{n-1}], \qquad S_n = k(X_1)[X_2, \cdots, X_{n-1}].$$

Consider a free R-module, with $Z_1, \cdots, Z_s$ as free generators. Let $l_i = f_{i1}Z_1 + \cdots + f_{is}Z_s$, $i = 1, \cdots, t$, $f_{ij} \in k[X]$, and consider the R-module m generated by $l_1, \cdots, l_t$. Let the matrix (f_{ij}) be of rank r and assume (by notation) that $D = \det |f_{ij}|$, $i, j = 1, \cdots, r$, is $\neq 0$. Moreover assume that D is regular with respect to $X_1, \cdots, X_n$. 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 $\zeta_{i+sj} = Z_i X_n^j$ and let $q \geq \max\{\deg f_{ij}\}$. Then n

is contained in the free R_n-module generated by the ζ_{i+sj}, $j = 0,\cdots, N+q$. Place $N = qt - 1$. Now we claim:

$$S \cdot m \cap \sum RZ_j = m + \left(S_n \cdot n \cap \sum R_n\zeta_k\right).$$

Proof (cf. [1]). There are elements in m of the form $DZ_i + (\cdot\cdot)Z_{r+1} + \cdots + (\cdot\cdot)Z_s$, $i = 1,\cdots, r$, where the $(\cdot\cdot)$ are in $k[X]$. Hence any element in $RZ_1 + \cdots + RZ_s$ is congruent mod m to an element $g_1Z_1 + \cdots + g_sZ_s$ ($g_i \in k[X]$ with $\deg g_i < \deg D$, $i = 1,\cdots, r$; here as throughout the proof, deg stands for degree in X_n). Thus given an element $l = g_1Z_1 + \cdots + g_sZ_s$ in $S \cdot m \cap \Sigma RZ_i$, we may first suppose $\deg g_i < \deg D$, $i = 1,\cdots, r$. Now l in $S \cdot m \cap \Sigma RZ_i$ implies that there exists an $F(X_1)$ in $k[X_1] - 0$ such that $F(X_1)l = a_1l_1 + \cdots + a_tl_t$ with the a_i in $k[X]$. Since $Dl_{r+i} \in Rl_1 + \cdots + Rl_r$, we may suppose (by redistributing the terms) that $\deg a_{r+i} < \deg D \leq qt = N+1$ for $i > 0$. We have $F(X_1)g_i = \Sigma_{j=1}^t a_jf_{ji}$. Consider these for $i = 1,\cdots, r$, multiply by the cofactors F_{ki} of the kth row of

$$\left\|\begin{matrix} f_{11} \cdots f_{1r} \\ \vdots \\ f_{r1} \cdots f_{rr}\end{matrix}\right\|,$$

$k = 1,\cdots, r$, and sum to get $\Sigma_{i=1}^r F(X_1)g_iF_{ki} = Da_k + \Sigma_{i=1}^r \Sigma_{j>r} a_jf_{ji}F_{ki}$. From this one concludes that also $\deg a_j \leq N$ for $j \leq r$, hence for all j. Hence $F(X_1)l \in \Sigma R_n\zeta_k$ and $l \in m + (S_n \cdot n \cap \Sigma R_n\zeta_k)$. The opposite inclusion is immediate.

Remark. The same statement with the same proof holds if S and S_n are replaced by

$$k(X_1,\cdots, X_m)[X_{m+1},\cdots, X_n] \quad\text{and}\quad k(X_1,\cdots, X_m)[X_{m+1},\cdots, X_{n-1}],$$

respectively, with $1 \leq m < n$.

10. Let $n \geq 1$. Place $R = k[X_1,\cdots, X_n]$, $S = k(X_1)[X_2,\cdots, X_n]$. Consider a free R-module, with $Z_1,\cdots, Z_s$ as free generators. Let $l_i = f_{i1}Z_1 + \cdots + f_{is}Z_s$, $i = 1,\cdots, t$, $f_{ij} \in k[X]$, and consider the R-module m generated by $l_1,\cdots, l_t$. Let the matrix (f_{ij}) have rank r and assume that $D = \det|f_{ij}|$, $i, j = 1,\cdots, r$, is $\neq 0$. Assume that k is infinite. Then for some homogeneous nonsingular linear transformation $X_i' = c_{i1}X_1 + \cdots + c_{in}X_n$ over k, one can construct

$$k(X_1')[X_2',\cdots, X_n'] \cdot m \cap \sum RZ_i.$$

Proof. For $n = 1$, we already have the result from 8, so let $n \geq 2$ and make an induction on n. Since k is infinite, after an appropriate homogeneous nonsingular linear transformation, D becomes regular in the new variables; notationally, we may suppose this to be so already for $X_1,\cdots, X_n$. Hence from 9, we have

$$S \cdot m \cap \sum RZ_j = m + \left(S_n \cdot n \cap \sum R_n\zeta_k\right).$$

To complete the construction, however, we must still construct $S_n \cdot n \cap \Sigma R_n\zeta_k$. We have not asserted that this can be done, but by induction, after an appropriate linear transformation $X_i' = c_{i1}X_1 + \cdots + c_{in-1}X_{n-1}$, $i = 1, \cdots, n-1$, we can construct $k(X_1')[X_2', \cdots, X_{n-1}'] \cdot n \cap \Sigma R_n\zeta_k$: this transformation does not change m, n, $\Sigma R_n\zeta_k$, D, nor is the regularity condition on D lost. What is changed is that $X_1, \cdots, X_{n-1}$ must be replaced by $X_1', \cdots, X_{n-1}'$ (and in particular, X_1 by X_1'); then one can write:

$$k(X_1')[X_2', \cdots, X_{n-1}', X_n] \cap \sum RZ_j = m + \left(k(X_1')[X_2', \cdots, X_{n-1}'] \cdot n \cap \sum R_n\zeta_k\right),$$

and since one can construct the right-hand side, the proof is complete.

Remark. One can arrange to have $X_1' = c_1X_1 + c_2X_2 + \cdots + c_nX_n$ with $c_1 \neq 0$, where $X_1, \cdots, X_n$ are the originally given variables. Then $k[X_1', X_2', \cdots, X_n'] = k[X_1', X_2, \cdots, X_n]$ and $k(X_1')[X_2', \cdots, X_n'] = k(X_1')[X_2, \cdots, X_n]$.

11. Let R, m be as in 10, except that k may be finite. Let $u_1, \cdots, u_n$ $(= u)$ be indeterminates and place $X_1' = u_1X_1 + \cdots + u_nX_n$. Then one can construct

$$k(u, X_1')[X_2, \cdots, X_n] \cdot m \cap \sum k(u)[X]Z_i.$$

Proof. Let t be a single indeterminate and let

$$l \in k(t, X_1)[X_2, \cdots, X_n] \cdot m \cap \sum k(t)[X]Z_i.$$

Write l in the form $l = (l^{(r)}t^r + l^{(r+1)}t^{r+1} + \cdots)/d(t)$, where the $l^{(i)}$ are in $\Sigma\, k[X]Z_i$ and $d(t) \in k[t]$. Then the l_i are in $k(X_1)[X_1, \cdots, X_n] \cdot m \cap \Sigma\, RZ_i$. In fact, since $d(t)l$ is in $k(t, X_1)[X_2, \cdots, X_n] \cdot m \cap \Sigma\, k(t)[X]Z_i$, we may as well suppose $d(t) = 1$. There exists an $F(t, X_1) \in k(t)[X_1] - 0$ such that

$$F(t, X_1)l = a_1(t, X)l_1 + \cdots + a_t(t, X)l_t, \tag{1}$$

where the $a_i(t, X)$ are in $k(t)[X]$. Clearing denominators, we may suppose F and the a_i are in $k[t, X]$. Let $F = F_st^s + F_{s+1}t^{s+1} + \cdots$, with the F_i in $k[X]$ and $F_s \neq 0$. Comparing the coefficients of t^{r+s} of the two sides of (1), we see that $l^{(r)} \in k(X_1)[X_2, \cdots, X_n] \cap \Sigma\, RZ_i$. Subtracting $l^{(r)}t^r$ from l, we see that $l^{(r+1)} \in k(X_1)[X_2, \cdots, X_n] \cap \Sigma\, RZ_i$; etc. Hence from a basis of $k(t, X_1)[X_2, \cdots, X_n] \cdot m \cap \Sigma\, k(t)[X]Z_i$ we can derive a basis for $k(X_1)[X_2, \cdots, X_n] \cdot m \cap \Sigma\, k[X]Z_i$. Thus *we may adjoin an indeterminate to* $k(u)$ *and later remove it.*

Following 10, to get a regularity condition on m we make a transformation $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, where the u_{ij} are indeterminates. After this, to get a regularity condition on n, we make another transformation $X_i'' = v_{i1}X_1' + \cdots + v_{in-1}X_{n-1}'$, $i = 1, \cdots, n-1$, $X_n'' = X_n'$, with the v_{ij} further indeterminates; etc., till we get variables $X_1^{(n-1)}, \cdots, X_n^{(n-1)}$. Let $K = k(u, v, \cdots)$ and $X_1^* = X_1^{(n-1)}$. By the argument in 10, then, we can construct $K(X_1^*)[X_2, \cdots, X_n] \cdot m \cap \Sigma\, K[X]Z_i$; here, if $X_1^* = u_{11}^*X_1 + \cdots + u_{1n}^*X_n$ we have to observe that $u_{11}^* \neq 0$ (see the remark in 10). Let $U, V, \cdots$ be the matrices such that $X' = UX$, $X'' = VX', \cdots$; and let $X^{(n-1)}$ $(= X^*) = U^*X$ and let $U^* = (u^*_{ij})$. Since $U^* = \cdots WVU$, the u^*_{ij} are rational, in fact linear, functions of the u_{ij} with coefficients in $k(v, w, \cdots)$; and vice-versa, so that $k(v, w, \cdots; u) = k(v, w, \cdots; u^*)$, and $k(X, v, w, \cdots; u) = k(X, v, w, \cdots; u^*)$. Hence

$$\mathrm{dt}\; k(X, v, w, \cdots; u^*)/k(X, v, w, \cdots) = n^2;$$

and the u^*_{ij} are algebraically independent over $k(X, v, w, \cdots)$, in particular $u^*_{11} \neq 0$. Let u' abbreviate the $(n-1)n$ quantities u_{ij}, $i > 1$. Since $U^* = \cdots WVU$, we see that $u^*_{1j} = a_j u_{1j} + b_j$ with $a_j, b_j \in k[u', v, w, \cdots]$. Upon specializing $V, W, \cdots$ to the identity matrix, the matrix U^* specializes to U; and u^*_{1j} to u_{1j}, whence $a_j \neq 0$. Hence

$$K = k(u, v, w, \cdots) = k(u^*_{11}, \cdots, u^*_{1n}, u', v, w, \cdots).$$

By the first paragraph of the proof, we can delete $u', v, w, \cdots$ from K, i.e., we can construct

$$k(u^*_{11}, \cdots, u^*_{1n}, X^*_1)[X_2, \cdots, X_n] \cdot m \cap \sum k(u^*_{11}, \cdots, u^*_{1n})[X]Z_i.$$

Since $u^*_{11}, \cdots, u^*_{1n}$ are algebraically independent over $k(X)$, we can just as well write $u_1, \cdots, u_n$ instead of $u^*_{11}, \cdots, u^*_{1n}$, and the proof is complete.

Remark. In [8], we showed that after the transformation $X'_i = u_{i1}X_1 + \cdots + u_{in}X_n$, not only m but also n and all the subsequent modules already have the desired regularity property.

12. Let $R = k[X_1, \cdots, X_n]$ and $m = (l_1, \cdots, l_t)$, a submodule of the free R-module $\Sigma\, RZ_i$. Then one can construct $k(X)m \cap \Sigma\, k[X]Z_i$.

Proof. Let $u_1, \cdots, u_n$ be indeterminates and place $X'_1 = u_1X_1 + \cdots + u_nX_n$. Since $k(u_1, \cdots, u_n, X_1, \cdots, X_n) = k(u_1, \cdots, u_n, X'_1, X_2, \cdots, X_n)$, we have $\mathrm{dt}\; k(u, X'_1)/k = n + 1$, so $k(u, X'_1)$ is explicitly given. We now work over this field and make an induction on n. Hence we can construct

$$k(u, X)m \cap \sum k(u, X'_1)[X_2, \cdots, X_n]Z_i = m_1.$$

From a basis of m_1 we can derive a basis in $\Sigma\, k[X]Z_i$; we omit the simple considerations, of a type already encountered, for proving this. Hence we have a submodule m_2 of $\Sigma\, k[X]Z_i$ such that $m_1 = k(u, X'_1)[X_2, \cdots, X_n]m_2$. By 11, we can construct $m_1 \cap \Sigma\, k(u)[X]Z_i$, so we now have $k(u, X)m \cap \Sigma\, k(u)[X]Z_i$. Now we delete $u_1, \cdots, u_n$ to complete the proof.

13. Let R and m be as in 12. Let $X'_i = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, q$, where $q \leq n$ and the u_{ij} are indeterminates. Then one can construct

$$k(u, X'_1, \cdots, X'_q)[X_{q+1}, \cdots, X_n]m \cap \sum k(u)[X]Z_i.$$

Proof. The case $q = n$ is 12, and for $q < n$, the proof follows precisely the lines of 10 and 11.

14. Let A be a given ideal in $k[X_1, \cdots, X_n]$ and let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, s$, where $s \leq n$ and the u_{ij} are indeterminates. Then one can construct

$$k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n]A \cap k(u)[X].$$

This is just the case $s = 1$ of 13.

15. The ideal $k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n]A \cap k(u)[X]$ of 14 has a basis in $k[X]$ which can be constructed.

Proof. This is rather immediate using the normal decomposition theorem, but we give an alternate proof which will be useful later (cf. 76).

We have a basis of $k(u, X_1', \cdots, X_s')[X]A \cap k(u)[X] = B$ which we may suppose consists of elements in $k[u, X]$. Let $f(u, X)$ be one of the basis elements; it suffices to show that the coefficients of f, regarded as a polynomial in the u_{ij}, are in B. We have an $E = E(u, X_1', \cdots, X_s') \in k[u, X_1', \cdots, X_s'] - 0$ such that $Ef \in k[u, X]A$. Then $\partial(Ef)/\partial u_{ij}$ and $E\partial(Ef)/\partial u_{ij}$ are in $k[u, X]A$, whence $E^2\partial f/\partial u_{ij} \in k[u, X]A$ and $\partial f/\partial u_{ij} \in B$. In the case of ch 0 it follows that the coefficients of f are in B. In the case of ch $p > 0$, one writes f as a polynomial in the u_{ij}^k, $k = 0, 1, \cdots, p-1$, with coefficients in $k[u^p, X]$; and concludes, as before, that these coefficients are in B. Replacing E by E^p, writing v for u^p, and repeating the argument several times, one soon comes to the desired conclusion.

Remark. If R and S are rings with $R \subset S$ and A is an ideal in R such that $S \cdot A \cap R = A$, then we frequently write A for $S \cdot A$ also, as this can usually be done without confusion; in particular, we may do this if $R = k[X_1, \cdots, X_n]$ and $S = k(u)[X_1, \cdots, X_n]$, where u stands for some indeterminates. Then if $A = Q_1 \cap \cdots \cap Q_{t+1} \cap \cdots \cap Q_u$ is a normal decomposition of A (of 14 and 15) into primary ideals and $Q_{t+1}, \cdots, Q_u$ are the primaries of dimension $< s$, then, using familar properties of quotient rings, one sees that the intersection of $k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n]A$ with $k(u)[X]$ is $Q_1 \cap \cdots \cap Q_t$; and the intersection with $k[X]$ is also $Q_1 \cap \cdots \cap Q_t$.

16. Let A be an ideal in $k[X_1, \cdots, X_n]$ of dimension $r > 0$ and assume it has a 0-dimensional prime (something we can decide by computing $k(u, X_1')[X_2, \cdots, X_n]A \cap k(u)[X]$ and comparing this with $k(u)[X]A$). Let $A = Q_1 \cap \cdots \cap Q_s \cap \cdots \cap Q_t$ be a normal decomposition of A and let $Q_{s+1}, \cdots, Q_t$ be the 0-dimensional primaries. Place $B = Q_1 \cap \cdots \cap Q_s$, $n = Q_{s+1} \cap \cdots \cap Q_t$. Then one can compute B and 0-dimensional ideal n' such that $A = B \cap n'$.

Proof. Let $X_1' = u_{11}X_1 + \cdots + u_{1n}X_n$, where the u_{1j} are indeterminates. Then

$$k(u_{11}, \cdots, u_{1n}, X_1')[X_1, X_2, \cdots, X_n]A \cap k(u_{11}, \cdots, u_{1n})[X] = k(u_{11}, \cdots, u_{1n})[X]B.$$

Hence we can find an E_1 in $k[u_{11}, \cdots, u_{1n}, X_1'] - 0$ such that $E_1B \subset A$ so $B \subset A : E_1$ (in $k(u_{11}, \cdots, u_{1n})[X]$). Now also $A : E_1 \subset B$, since if $g \in k(u_{11}, \cdots, u_{1n})[X]$

and $gE_1 \in A$, then obviously $g \in B$. So $A : E_1 = B$. Note also that $B : E_1 = B$, since if $gE_1 \in B$, then $gE_1^2 \in A$ and $g \in B$. Now we say:

$$(1) \qquad (A, E_1) \cap B = A.$$

In fact, the right-hand side is obviously in the left; conversely, let $g \in (A, E_1) \cap B$. Then $g = hE_1 + a$, with $h, a \in k(u_{11}, \cdots, u_{1n})[X]$ and $a \in A$. Since $g \in B$, $gE_1 \in A$, whence $hE_1^2 \in A$. From this $hE_1 \in B$ and $h \in B$. Hence $hE_1 \in A$ and $g \in A$, so equality is proved.

Now extend the base field with further indeterminates $u_{21}, \cdots, u_{2n}$ and repeat the argument. Since B, i.e., the intersection of the primaries of A of positive dimension, is uniquely determined, one sees from (1) that the intersection B_1 of the primaries of (A, E_1) of positive dimension must contain B. Hence we find

$$(A, E_1, E_2) \cap B_1 = (A, E_1) \quad \text{and} \quad (A, E_1, E_2) \cap B = A;$$

here we are working in $k(u_{11}, \cdots, u_{2n})[X]$ and $E_2 = E_2(X_2') \in k[u_{11}, \cdots, u_{2n}, X]$, where $X_2' = u_{21}X_1 + \cdots + u_{2n}X_n$. Repeating the argument several times, we get $(A, E_1, E_2, \cdots, E_n) \cap B = A$, where $E_i = E_i(X_i')$, $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$. Then $n_1 = (A, E_1, E_2, \cdots, E_n)$ is 0-dimensional and the problem is solved over $k(u)$.

Now let $A : B = m$ (in $k[X]$); then m is a 0-dimensional ideal having the same primes as n or n_1. Since $n_1 < n_1 : m < n_1 : m^2 < \cdots$, by 7 one can compute a ρ such that $m^\rho \subset n_1$ (not n!). Now $A \subset B \cap (A, m^\rho) \subset A$, i.e., $A = B \cap (A, m^\rho)$, as desired; this is first obtained in $k(u)[X]$, but since A, B, and m are $k[X]$-ideals, it is also seen to hold in $k[X]$. Then $n' = (A, m^\rho)$ solves the problem over k.

17. Let A be r-dimensional, $r > 0$. Let $A = Q_1 \cap \cdots \cap Q_s \cap \cdots \cap Q_t$ be a normal decomposition of A, and let $Q_1, \cdots, Q_s$ be the r-dimensional primaries. Then one can construct $Q_1 \cap \cdots \cap Q_s$.

Proof. One applies 14 and 15 for $s = r$.

18. Let A be r-dimensional, $r > 0$. We can test whether A is unmixed, by 17, and if it is not we can find the least s for which A still has s-dimensional primes; assume this situation. Let $A = Q_1 \cap \cdots \cap Q_{s_1} \cap \cdots \cap Q_t$ be a normal decomposition, and let $Q_{s_1+1}, \cdots, Q_t$ be the s-dimensional primaries. Place $B = Q_1 \cap \cdots \cap Q_{s_1}$, $n = Q_{s_1+1} \cap \cdots \cap Q_t$. Then one can construct B and an unmixed s-dimensional ideal n' such that $A = B \cap n'$.

Proof. One first computes B, by 14 and 15, then an ideal m in $k[X_1, \cdots, X_n]$ having the same primes as n ($m = A : B$). Now in $k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n]$, for a ρ one can compute, $A = B \cap (A, m^\rho)$. In $k[X]$, (A, m^ρ) is s-dimensional, but may not be unmixed. Let n be the intersection of the s-dimensional primaries of (A, m^ρ). We can compute n. Then

$$k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n]n = k(u, X_1', \cdots, X_s')[X_{s+1}, \cdots, X_n](A, m^\rho)$$

and the contraction is n. Hence $A = B \cap n$.

19. Given an ideal A in $k[X_1, \cdots, X_n]$, one can write it as the intersection of (constructed) unmixed ideals.

This is a corollary of 18.

20. Let A, B be two ideals in $k[X_1, \cdots, X_n]$. Then one can calculate an integer ρ such that $A : B^\rho = A : B^{\rho+1}$.

Proof. Since $A : B^i = A : B^{i+1}$ implies $A : B^{i+1} = A : B^{i+2}$, the chain $A \subset A : B \subset A : B^2 \subset \cdots$ is strictly increasing till we come to equality. By 19 we may assume that A is unmixed, of dimension r, say. Then the ideal $A : B^i = C_i$, if not $= (1)$, is also unmixed r-dimensional. Then the strictly ascending chain $A < C_1 < C_2 \cdots$ remains strictly ascending in $k(u, X_1', \cdots, X_r')[X_{r+1}, \cdots, X_n]$, where $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, r$, and the u_{ij} are indeterminates. In this ring, however, the ideals A, $C_1, \cdots$ are 0-dimensional, so by 7 we get the desired bound ρ.

21. Let $b_1, \cdots, b_t$ be polynomials in $k[X_1, \cdots, X_n]$ of degree at most N, for a given integer N. Then the $(b_1, \cdots, b_t)$, over all possibilities, are in one-to-one correspondence, via the coefficients of the b_i, with the points in an affine space over k; say $(b_1, \cdots, b_t)$ corresponds to $P(b_1, \cdots, b_t)$. Consider a system of equations: $f_{i1}g_1 + \cdots + f_{is}g_s = b_i$, $i = 1, \cdots, t$, as in 4. Then the points $P(b_1, \cdots, b_s)$ for which there is a solution $(g_1, \cdots, g_s)$, $g_i \in k[X]$, fill out a k-linear space, and one can construct a basis for this space. Otherwise said: The conditions that the system have a solution are linear and homogeneous in the coefficients of the b_i, and one can construct a k-basis for the conditions.

Proof. That the $P(b_1, \cdots, b_t)$ fill out a linear space is obvious, and it is merely a question of constructing a basis for this space. If k is finite, we can write down all possibilities for $(b_1, \cdots, b_t)$ and test, by 4, for which ones the corresponding linear system has solutions. If k is infinite, then, following the lines of 4, Proof, one sees how to write down the desired basis (or conditions).

22. Let $A = (f_1, \cdots, f_s)$ be an ideal in $k[X_1, \cdots, X_n]$, $n \geq 1$. If at least one of the f_i is regular in $X_1, \cdots, X_n$, one can construct $A \cap k[X_1, \cdots, X_{n-1}]$.

Proof. We are looking for the $g = g_1f_1 + \cdots + g_sf_s$ with $g_i \in k[X]$ and with $\deg_{X_n} g = 0$. Clearly we may assume $f_s \neq 0$ and that it is regular in $X_1, \cdots, X_{n-1}$. Using the regularity of f_s, we can depress the degree in X_n of $g_1, \cdots, g_{s-1}$, and thus put a bound on the degree in X_n of $g_1, \cdots, g_s$. Writing $g_i = \Sigma\, g_{ij}X_n^j$ and $f_i = \Sigma\, f_{ij}X_n^j$, the condition $\deg_{X_n} g = 0$ can be rewritten as a homogeneous linear system in the g_{ij}. By 1 we can construct a basis for the $(\cdots, g_{ij}, \cdots)$, and the corresponding g give a basis for $(f_1, \cdots, f_s) \cap k[X_1, \cdots, X_{n-1}]$ (cf. [7, Lemma 2]).

23. Let $A = (f_1, \cdots, f_s)$ be a primary ideal in $k[X_1, \cdots, X_n]$. Then one can construct $A \cap k[X_1, \cdots, X_{n-1}]$.

Proof. Let $s = \dim A$. If $s = 0$, one can find an $f \in k[X_n] - 0$ in A. f is regular in $X_1, \cdots, X_n$, so by 22 one can construct $A \cap k[X_1, \cdots, X_{n-1}]$.

For $s > 0$, we make an induction on s. If every X_i, $i = 1, \cdots, n-1$, is algebraic over k mod A, one can find a $g_i(X_i) \in k[X_i] - 0$ in A, $i = 1, \cdots, n-1$. Let $g \in A \cap k[X_1, \cdots, X_{n-1}]$ be an element sought; reducing g mod $(g_1, \cdots, g_{n-1})$, we may suppose $\deg_{X_i} g < \deg_{X_i} g_i = d_i$, $i = 1, \cdots, n-1$. Let $h_1, \cdots, h_M$ be the power products of the X_i with $\deg_{X_i} h_j < \deg_{X_i} g_i$ for every i and j, $i = 1, \cdots, n-1$, $j = 1, \cdots, M$. It is then a matter of finding the $c_1, \cdots, c_M$ such that $c_1h_1 + \cdots + c_Mh_M = f_1g_1 + \cdots + f_sg_s$ has a solution $(g_1, \cdots, g_s)$ with $g_i \in k[X]$. This can be done by 21.

If at least one X_i, $i = 1, \cdots, n-1$, is not algebraic over k mod A, let $X_1' = u_1X_1 + \cdots + u_{n-1}X_{n-1}$, where the u_i are indeterminates. Since A is primary, one notes that $k(u, X_1')[X]A \cap k(u)[X] = A$. Thus it suffices to construct $k(u, X_1')[X]A \cap k[X_1, \cdots, X_{n-1}]$. Since A has dimension $s-1$ over $k(u, X_1')$, we can construct $k(u, X_1')[X_2, \cdots, X_n]A \cap k(u, X_1')[X_2, \cdots, X_{n-1}] = A'$. It remains to construct $A' \cap k[X_1, \cdots, X_{n-1}]$. We have a basis $g_1, \cdots, g_t$ for A' and may suppose $g_i \in k[u, X_1', X_2, \cdots, X_{n-1}] \subset k[u, X_1, \cdots, X_{n-1}]$. When these are written as polynomials in $u_1, \cdots, u_n$ with coefficients in $k[X_1, \cdots, X_{n-1}]$, one sees that the coefficients are in A, hence in A'. Thus one has an ideal A'' in $k[X_1, \cdots, X_{n-1}]$ such that $k(u, X_1')[X_2, \cdots, X_{n-1}]A'' = A'$. By 15 one can construct $k(u, X_1')[X_2, \cdots, X_{n-1}]A'' \cap k[X_1, \cdots, X_{n-1}]$.

Remark. The problem of constructing $A \cap k[X_1, \cdots, X_{n-1}]$ for an arbitrary ideal in $k[X_1, \cdots, X_n]$ was posed in [9]. If k satisfies condition (F), then one can find a decomposition of A into primaries (see 36 below), and the problem can be solved for such fields k. Whether the construction can be done for any explicitly given field k we do not know.[4]

24. **Definition.** A finite integral domain $k[x_1, \cdots, x_n]$ is said to be *given* if one is given (or knows) a finite basis for the ideal of relations satisfied by $x_1, \cdots \cdots, x_n$ over k. The field $k(x_1, \cdots, x_n)$ is then also said to be *given* (relative to k).

A given field $k(x_1, \cdots, x_n)$ is explicitly given, but not vice versa.

By 23, if $\{i_1, \cdots, i_s\}$ is a given subset of $\{1, \cdots, n\}$, with $i_j \neq i_k$ if $j \neq k$, then the field $k(x_{i1}, \cdots, x_{is})$ is given if $k(x_1, \cdots, x_n)$ is.

25. If $k(x_1, \cdots, x_n)$ is given, one can decide whether x_n is algebraic over

[4] Now we see how to do this, but will let what we have written stand, in order not to disturb the structure of the text. Let $m = (f_1, \cdots, f_t)$ be a given ideal; we propose to construct $m \cap k[X_2, \cdots, X_n]$. Let $f_{11}, \cdots, f_{1t_1}$ be the polynomials constructed in footnote 2 (for $r = 1$). Let $g \in m \cap k[X_2, \cdots, X_n]$, i.e., $g \equiv 0$ (m) and $[g]_1 = 0$; and write it as stated: $g = \Sigma g_if_{1i}$ with $[g_if_{1i}]_1 \leq [g]_1$ for every $g_i \neq 0$. Then the f_{1i} with $[f_{1i}]_1 = 0$ will be seen to be a basis for $m \cap k[X_2, \cdots, X_n]$. This part of the argument was communicated to us by Professor Stolzenberg.

$k(x_1, \cdots, x_{n-1})$; and if it is, one can find the defining equation for x_n over $k(x_1, \cdots, x_{n-1})$.

Proof. Let $(f_1, \cdots, f_s)$ be a basis for the $k[X_1, \cdots, X_n]$-ideal P of relations satisfied by $x_1, \cdots, x_n$ over k; and, by 23, let P_0 be the $k[X_1, \cdots, X_{n-1}]$-ideal of relations satisfied by $x_1, \cdots, x_{n-1}$ over k. We also designate by P_0 the extension of P_0 to $k[X_1, \cdots, X_n]$. Then

$$(f_1(x_1, \cdots, x_{n-1}, X_n), \cdots, f_s(x_1, \cdots, x_{n-1}, X_n)) = P/P_0$$

in $k[x_1, \cdots, x_{n-1}, X_n]$. We can decide whether $P/P_0 = (0)$; and x_n is algebraic over $k(x_1, \cdots, x_{n-1})$ if and only if $P/P_0 \neq (0)$; assume this case. Then P/P_0 generates a prime principal ideal in $k(x_1, \cdots, x_{n-1})[X_n]$, and using the Euclidean algorithm we can get a single generator for it. This generator yields the desired defining equation.

It will be convenient to say that $0 = 0$ *is the defining equation for a transcendental element.*

Remark. The argument can be considerably simplified if one assumes condition (F) for k; 23 was brought in in order to avoid (F).

26. Let a sequence of fields $k(x_1)$, $k(x_1, x_2), \cdots, k(x_1, \cdots, x_n)$ be determined by giving, for each i, the defining equation of x_i over $k(x_1, \cdots, x_{i-1})$; here x_i may be transcendental over $k(x_1, \cdots, x_{i-1})$. Then one can construct a basis for the ideal P of relations satisfied by $x_1, \cdots, x_n$ over k.

Proof. By induction we may suppose we have a basis $f_1, \cdots, f_s$ for the ideal P_0 of relations satisfied by $x_1, \cdots, x_{n-1}$ over k; we also designate by P_0 the extension of $(f_1, \cdots, f_s)$ to $k[X_1, \cdots, X_n]$. Let $F(x_1, \cdots, x_{n-1}, X_n) = 0$ be the defining equation of x_n over $k(x_1, \cdots, x_{n-1})$. Here we may suppose $F \in k[X_1, \cdots, X_n]$, $F = D(X_1, \cdots, X_{n-1})X_n^m + D_1(X_1, \cdots, X_{n-1})X_n^{m-1} + \cdots$, and, dismissing the trivial case that x_n is transcendental over $k(x_1, \cdots, x_{n-1})$, that $D(x_1, \cdots, x_{n-1}) \neq 0$. Let $G \in k[X_1, \cdots, X_n]$ with $G(x_1, \cdots, x_n) = 0$. For some ρ we have $D^\rho G = AF + R$, where $A, R \in k[X_1, \cdots, X_n]$ and $\deg_{X_n} R < \deg_{X_n} F$. Moreover, $R(x_1, \cdots, x_{n-1}, X_n)$ vanishes for $X_n = x_n$, whence $R(x_1, \cdots, x_{n-1}, X_n) = 0$ and $R \in P_0$. Thus $G \in (P_0, F):D^\rho$. Conversely, any element in $(P_0, F):D^\rho$, for any ρ, is in P, so $P = \bigcup_\rho ((P_0, F):D^\rho)$ and $P = (P_0, F):D^\rho$ for large ρ. By 20, then, P can be constructed.

Definition. If a field $k(x_1, \cdots, x_n)$ is determined by giving, for each i, the defining equation for x_i over $k(x_1, \cdots, x_{i-1})$, then the field $k(x_1, \cdots, x_n)$ is said to be *canonically given* (relative to k). (Thus by 25 and 26 the field $k(x_1, \cdots, x_n)$ is given if and only if it is canonically given.) In the case that k is a prime field of given characteristic, the canonically given field $k(x_1, \cdots, x_n)$ is said to be *absolutely given.*

27. Let the field $k(x_1, \cdots, x_n)$ be given and let $y_1, \cdots, y_s$ be (given) elements in $k(x_1, \cdots, x_n)$. Then one can construct a basis for the ideal of relations satisfied by $y_1, \cdots, y_s$ over k.

Proof. By 25 we can find the defining equation of x_i over $k(x_1, \cdots, x_{i-1})$. Moreover, if $y_j = a(x_1, \cdots, x_n)/b(x_1, \cdots, x_n)$ with $a, b \in k[X_1, \cdots, X_n]$, then $b(x_1, \cdots, x_n)y_j - a(x_1, \cdots, x_n) = 0$ is the defining equation of y_j over $k(x_1, \cdots, x_n, y_1, \cdots, y_{j-1})$. Hence by 26 we can construct the ideal of relations satisfied by $x_1, \cdots, x_n, y_1, \cdots, y_s$ over k; and then by 25 the ideal of relations satisfied by $y_1, \cdots, y_s$ over k.

28. **Definition.** Let A be an unmixed r-dimensional ideal in $k[X_1, \cdots, X_n]$ with $r < n$, so that if $X'_i = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, r+1$, with the u_{ij} indeterminates, then

$$k(u, X'_1, \cdots, X'_r)[X]A \cap k(u)[X] = A \quad \text{and} \quad k(u, X'_1, \cdots, X'_{r+1})[X]A \cap k(u)[X] = (1).$$

The ideal $k(u)[X]A \cap k(u)[X'_1, \cdots, X'_{r+1}]$ is, as one proves, a principal ideal (F). The generator F may be taken in $k[u, X'_1, \cdots, X'_{r+1}]$ and primitive as a polynomial in $X'_1, \cdots, X'_r$ with coefficients in $k[u]$ (i.e., the coefficients should have 1 as greatest common divisor). Such a polynomial, though still not unique by a factor in k, is called *the ground-form* of A.

In the case A is a prime ideal P, the ground-form F is obviously irreducible. Let $k[X]/P = k(x)$ and let $x'_i = u_{i1}x_1 + \cdots + u_{in}x_n$, $i = 1, \cdots, r+1$. Then $F(u; x'_1, \cdots, x'_{r+1}) = 0$, and since dt $k(u; x'_1, \cdots, x'_{r+1})/k(u) = r$, $F(u; X'_1, \cdots, X'_{r+1})$ is the irreducible polynomial satisfied by $x'_1, \cdots, x'_{r+1}$ over $k(u)$.

29. Let $A \neq (0)$ be an unmixed ideal in $k[X_1, \cdots, X_n]$ (so that $\dim A = r < n$). Then one can construct the ground-form of A.

Proof. We treat separately the case $r = n - 1$ and $r < n - 1$. If $r = n - 1$, then A is principal, $A = (F)$; and when F is written in terms of (generically) transformed variables and normalized, we get the ground-form. Now let $r < n - 1$ and let $X'_i = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, n$, with the u_{ij} indeterminates. Since any element in $A - 0$ becomes regular in $X'_1, \cdots, X'_{n-1}$, by 22 we can construct $A \cap k(u)[X'_1, \cdots, X'_{n-1}]$. If $r = n - 2$, then this intersection is a principal ideal (F), and F, when normalized, gives the ground-form. If $r < n - 2$, we repeat the argument, so that if $X''_i = v_{i1}X'_1 + \cdots + v_{in-1}X'_{n-1}$, $i = 1, \cdots, n - 1$, $X''_n = X'_n$, with the v_{ij} further indeterminates, we can construct $A \cap k(u, v)[X''_1, \cdots, X''_{n-2}]$. Eventually we construct $k(u, v, \cdots)[X_1^{(n-r-1)}, \cdots, X_{r+1}^{(n-r-1)}]$. Write X^* for $X^{(n-r-1)}$. Let $U, V, W, \cdots$ be the matrices of the transformations $X \to X'$, $X' \to X''$, $X'' \to X'''$, $\cdots$; and let $X^* = U^*X$, so that $U^* = \cdots WVU$. Observing that $k(v, w, \cdots; u) = k(v, w, \cdots; u^*)$ and that $v, w, \cdots, u^*$ are algebraically independent over $k(X)$, one sees first that one can construct $A \cap k(v, w, \cdots; u^*)[X^*_1, \cdots, X^*_{r+1}]$, hence $A \cap k(u^*)[X_1^*, \cdots, X_{r+1}^*]$ and $A \cap k(u)[X_1', \cdots, X_{r+1}']$. This soon gives the ground-form.

Basic properties of the ground-form. This section is not constructive in intent, but merely recalls some basic facts.

30. Let $P \neq (0)$ be a separable prime ideal in $k[X_1, \cdots, X_n]$, i.e., if $k[X]/P = k[x]$, we are assuming that $k(x)$ is separable (i.e., separably generated) over k. Let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, r+1$, with the u_{ij} indeterminates, and let $F(u; X_1', \cdots, X_{r+1}')$ be the ground-form of P. Then F is separable in X_{r+1}' (over $k(u, X_1', \cdots, X_r')$). Moreover, if $x_i' = u_{i1}x_1 + \cdots + u_{in}x_n$, then x_{r+1}' is a primitive element of $k(u, x)$ over $k(u, x_1', \cdots, x_r')$.

Proof. Introduce further indeterminates and write $x_i' = u_{i1}x_1 + \cdots + u_{in}x_n$, $i = 1, \cdots, n$. Then $k(u, x) = k(u, x')$, $k(u, x')$ is separable over $k(u)$, and some r, hence by symmetry any r, of the $x_1', \cdots, x_n'$ form a separating transcendency basis of $k(u, x')/k(u)$; cf. [13, p. 104, Theorem 30]. Hence x_{r+1}' is separably algebraic over $k(u, x_1', \cdots, x_r')$. Thus the defining polynomial of x_{r+1}' over $k(u, x_1', \cdots, x_r')$ is separable, and as this is $F(u; x_1', \cdots, x_r', X_{r+1}')$, the first assertion follows. Now from $F(u, x_1', \cdots, x_{r+1}') = 0$, taking the partial with respect to $U_{r+1\,i}$, we get $\partial F/\partial u_{r+1\,i} + \partial F/\partial x_{r+1}' \cdot x_i = 0$. Since $\partial F/\partial x_{r+1}' \neq 0$, the second statement follows.

31. Distinct r-dimensional primes $(r < n)$ have distinct ground-forms.

Proof. Let P be an r-dimensional prime, x a generic point over k. We consider first the case that $k(x)/k$ is separable. Let $x_i' = u_{i1}x_1 + \cdots + u_{in}x_n$, $i = 1, \cdots, r+1$, be as in 30, and let F be the ground-form of P. We have seen that $\partial F/\partial u_{r+1\,i} + \partial F/\partial x_{r+1}' \cdot x_i = 0$ (and $\partial F/\partial x_{r+1}' \neq 0$), so we can recover the x_i from $x_1', \cdots, x_{r+1}'$. Now $(x_1', \cdots, x_{r+1}')$ is a generic zero of $F(u, X')/k(u)$. Any other generic zero $(x_1^*, \cdots, x_{r+1}^*)$ of $(F)/k(u)$ is a conjugate of $(x_1', \cdots, x_{r+1}')/k(u)$, and hence

$$\left(-\frac{\partial F/\partial u_{r+1\,1}}{\partial F/\partial X_{r+1}'}, \cdots, -\frac{\partial F/\partial u_{r+1\,n}}{\partial F/\partial X_{r+1}'}\right)_{X'=x^*}$$

conjugate of $(x_1, \cdots, x_n)/k(u)$. We can recover P from $(x_1, \cdots, x_n)$ or equally well from any of its conjugates over $k(u)$. From F we can get a generic point $(x_1^*, \cdots, x_{r+1}^*)$ of $(F)/k(u)$, and from x^* and F we can get a generic point of $P/k(u)$ and P itself. Hence we can recover P from F. Hence if P_1, P_2 are two distinct separable primes, their ground-forms must be distinct.

In the general case, let k^* = perfect closure of k. Let P_1, P_2 be the given primes. Over P_i $(i = 1, 2)$ in $k^*[X_1, \cdots, X_n]$ there lies exactly one prime P_i^*. The ground-form of P_i is a power of that of P_i^*. The primes P_1^*, P_2^* have distinct ground-forms by the case considered. Hence so do P_1, P_2.

32. The ground-form of a primary ideal is a power of the ground-form of its

associated prime; and the ground-form of the intersection of several r-dimensional primary ideals $Q_1, \cdots, Q_s$ having distinct associated primes is the product of the separate ground-forms.

This is immediate.

Constructions holding for a base field k satisfying condition (F).

33. Consider the following problem. Given an $f \in k[X] - 0$, $X = X_1$, to construct the complete factorization of f over k. If this problem has a positive solution for k, we say that *condition* (F), or, also, the *factorization theorem*, holds for k. For example, any prime field of given characteristic satisfies (F).

34. If (F) holds for k, then one can also completely factor any polynomial in $k[X_1, \cdots, X_n] - 0$. Hence if (F) holds for k, then it also holds for a simple transcendental extension of k.

We recall Kronecker's proof:

Kronecker's trick. Let $f = \Sigma\, c_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$, $c_{i_0\cdots i_n} \in k$, be the polynomial to be factored. Let t be an integer greater than any exponent i_j in f. Let X be a new indeterminate, to a power-product $X_1^{i_1} \cdots X_n^{i_n}$ associate

$$X^{i_1+i_2t+\cdots+i_nt^{n-1}},$$

and to $f = \Sigma\, c_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$ associate

$$f' = \sum c_{i_1\cdots i_n} X^{i_1+\cdots+i_nt^{n-1}}.$$

From f' we can recover f. Any factorization of f gives rise to a factorization of f', from which we can recover the factorization of f. Since f' has only a finite number of factorizations, all of which we can write down, we can recover all possible factorizations of f.

35. If (F) holds for k, then it also holds for a simple separably algebraic extension $k(\theta)$ of k.

This is known from [11], but it will be well to recall the proof. Let, then, $F(\theta, Z) \in k(\theta)[Z]$ be the polynomial to be factored; we may suppose F to be monic. Let u be an indeterminate. Form the norm of $F(\theta, Z - u\theta)$ and factor it completely in $k[u, Z]$:

$$N(F(\theta, Z - u\theta)) = F_1(u, Z) \cdots F_t(u, Z).$$

We form GCD $(F(\theta, Z - u\theta), F_i)$, $i = 1, \cdots, t$; if this is not 1 or $F(\theta, Z - u\theta)$, we can factor $F(\theta, Z - u\theta)$ properly, and placing $u = 0$, we get a proper factorization of $F(\theta, Z)$. Hence we may assume GCD $(F(\theta, Z - u\theta), F_i) = 1$ or $F(\theta, Z - u\theta)$ and $F_1(u, Z) \equiv 0 \; (F(\theta, Z - u\theta))$. In this case, $F(\theta, Z)$ is irreducible. In fact, suppose $F(\theta, Z) = g(\theta, Z) h(\theta, Z)$ with $\deg_Z F = n > m = \deg_Z g > 0$. We have

$$NF(\theta, Z - u\theta) = Ng(\theta, Z - u\theta)\, Nh(\theta, Z - u\theta).$$

We may assume $Ng(\theta, Z - u\theta) \equiv 0\ (F_1)$, so that $Ng(\theta, Z - u\theta) \equiv 0\ (F(\theta, Z - u\theta))$. Regarding solely the terms of greatest degree, we get $N(Z - u\theta)^m \equiv 0\ (Z - u\theta)^n$, whence $N(Z - u\theta) \equiv 0\ (Z - u\theta)^2$, a contradiction.

36. Let A be an unmixed r-dimensional ideal in $k[X_1, \cdots, X_n]$, $r < n$. If k satisfies (F), then one can construct the associated primary ideals of A. Hence for any ideal A one can construct a normal decomposition into primary ideals.

Proof. Given $A = Q_1 \cap \cdots \cap Q_t$, unmixed, r-dimensional, we can construct its ground-form F and factor it (over $k(u)$) into a power-product of irreducible polynomials: $F = cF_1^{n_1} \cdots F_t^{n_t}$, $c \in k$. Here $F_1, \cdots, F_t$ must be the ground-forms of the associated primes $P_1, \cdots, P_t$ and $F_1^{r_1}, \cdots, F_t^{r_t}$ those of $Q_1, \cdots, Q_t$. Then $Q_1 = A : F_2^{r_2} \cdots F_t^{r_t}$; and similarly for the other Q_i.

Remark. Let (F′) be the condition on k that one can write any polynomial in $k[X_1, \cdots, X_n]$, effectively, as the product of primary ideals. Then one sees that it is (F′), rather than (F), which is necessary and sufficient for the construction of a primary decomposition. Later (see 54) we shall give an example showing that (F′) really is weaker than (F).

37. Given a primary ideal, we can put a bound on its exponent.

Proof. Reduce to the case of dimension 0 and apply 7. However, we have already dealt with a more general situation in 20.

38. Let A be an ideal in $k[X_1, \cdots, X_n]$. If k satisfies (F), then one can construct $k(X_1)[X_2, \cdots, X_n]A \cap k[X_1, \cdots, X_n]$.

Proof. We can construct a normal decomposition $A = Q_1 \cap \cdots \cap Q_t$ for A. Then we can find which Q_i are such that $k(X_1)[X]Q_i \cap k[X] = (1)$; let these be $Q_{s+1}, \cdots, Q_t$. For the other Q_i, $k(X_1)[X]Q_i \cap k[X] = Q_i$; and $Q_1 \cap \cdots \cap Q_s$ is the desired ideal.

Remark. It would be interesting to know whether this construction can be done for any explicitly given base field k.

Constructions holding for a base field k satisfying conditions (F) and (P).

39. Consider the following problem. Given a finite system of linear homogeneous equations $\sum a_{ij} X_j = 0$ with $a_{ij} \in k$: to decide whether this system has a nontrivial solution in k^p, and if it does to find one. If this problem has a positive solution for k, we say that *condition* (P) *holds for* k; for example, condition (P) holds for any absolutely given finite field (p = characteristic of k).

40. If the condition (P) holds for k, then it also holds for any canonically given extension of k (cf. [5, p. 12]).

Proof. It is sufficient to consider a succession of simple extensions of the following types: (i) a simple transcendental extension, (ii) a simple separably algebraic extension, (iii) extension by a pth root.

First consider type (i). Now the a_{ij} are in $k(u)$ and we seek a solution in

$k^p(u^p)$. There will be one such if and only if there is one such in $k^p[u^p]$. We may also assume

$$a_{ij} \in k[u], \quad a_{ij} = a_{ij0}(u^p) + a_{ij1}(u^p)u + \cdots + a_{ijp-1}(u^p)u^{p-1}.$$

Replace the given system by the equivalent system $\Sigma\, a_{ijk}X_j = 0$. So now we may assume the $a_{ij} \in k[u^p]$. Let $\{\lambda_k\}$ be a maximal k^p-linearly independent subset of the set of coefficients of the a_{ij}, so that we can write $a_{ij} = \Sigma\, a_{ijk}\lambda_k$, $a_{ijk} \in k^p[u^p]$. Then $\Sigma\, a_{ijk}X_j = 0$ is an equivalent system with the coefficients in $k^p[u^p]$. Extracting the pth roots of the left-hand sides, we get a system over $k(u)$ and seek a solution in $k(u)$. This can be resolved.

Now consider case (ii). The coefficients are in $k(\theta)$, the unknowns in $k^p(\theta^p)$. Write $X_i = X_{i0} + X_{i1}\theta^p + \cdots + X_{is-1}\theta^{(s-1)p}$, where $[k(\theta):k] = s$ and the unknowns are in k^p. Rewrite the equations in terms of $1, \theta, \cdots, \theta^{s-1}$ to get an equivalent system over k with solutions to be in k^p.

In case (iii) we have equations over $k(a^{1/p})$ and seek a solution in $k^p(a)$. Here $a \in k$, we can test by the assumption on k whether it is in k^p, and we suppose it is not. Writing the coefficients in the form $c_0 + c_1a^{1/p} + \cdots + c_{p-1}a^{(p-1)/p}$ with $c_i \in k$, we can get an equivalent system with coefficients in k (since $k^p(a) \subset k$). Now we write each X_i as $X_i = X_{i0} + X_{i1}a + \cdots + X_{ip-1}a^{p-1}$ to get a system with coefficients in k and solutions to be in k^p.

41. If conditions (P) and (F) hold for k, then they hold for any canonically given extension of k.

Proof. As in 40, we need consider only extensions of types (i), (ii) and (iii). As noted in 34 and 35, condition (F) carries over to extensions of types (i) and (ii). In case (iii), let $F \in k(a^{1/p})[X]$. Let G be a factor of F, $F = GH$; we may assume F, G, H monic. Then $F^p = G^pH^p$. We can factor F^p over k and so have a finite number of candidates for G^p. Any such must be a polynomial in X^p. Supposing it such, its coefficients must have their pth roots in $k(a^{1/p})$, and this is sufficient. By (P), this can be decided.

42. If conditions (P) and (F) hold for k, then given a primary ideal Q in $k[X_1, \cdots, X_n]$, one can construct its associated prime.

Proof. As the assertion is obvious for $n = 1$, we make an induction on n; and for $n > 1$, an induction on $\dim Q$. If $\dim Q > 0$, adjoin $u_1X_1 + \cdots + u_nX_n$ to the ground-field, reducing the dimension. There remains the case that $\dim Q = 0$. In this case, first get a $g \in k[X_1] - 0$ such that $g \equiv 0$ (Q) and then an irreducible $f \in k[X_1] - 0$ such that $f^\rho \in Q$ for some ρ. Then Q and (Q, f) are both primary with the same associated prime. Now take residues mod f to reduce n.

Alternate method. In the case $\dim Q > 0$, one can find an X_i, say X_1, algebraically independent over k mod Q. Then examine $k(X_1)[X_2, \cdots, X_n]Q$. If P is the associated prime of Q, then by induction on n one can find $k(X_1)[X_2, \cdots, X_n]P$.

Let $(f_1, \cdots, f_s)$ be a basis of this ideal with $f_i \in k[X]$. Then we can find a normal decomposition $(f_1, \cdots, f_s) = P \cap Q_1 \cap \cdots \cap Q_t$ in $k[X]$. We can find the primaries here, one of which is P. Which one? All but P go lost in $k(X_1)[X_2, \cdots, X_n]$.

Remark. Condition (F) is not needed in 42; see 45, below.

43. If k satisfies (P), then elements $z_1, \cdots, z_s$ in k can be checked for p-independence (i.e., one can check whether $[k^p(z_1, \cdots, z_s) : k^p] = p^s$); and if they are p-dependent, then one can construct an equation exhibiting this. Conversely if any $z_1, \cdots, z_s$ in k can be checked for p-independence, and if they are p-dependent, an equation exhibiting this can be constructed, then condition (P) holds for k.

Proof. Elements $z_1, \cdots, z_s$ are p-independent if and only if the power-products $z_1^{i_1} \cdots z_s^{i_s}$, $0 \leq i_j \leq p-1$, are linearly independent over k^p. If (P) holds for k, this can be decided; and in the case of dependence, one can write down a nontrivial relation $\Sigma\, c_{i_1 \cdots i_s} z_1^{i_1} \cdots z_s^{i_s} = 0$, with $0 \leq i_j \leq p-1$ and $c_{i_1 \cdots i_s} \in k^p$. In the latter case, we may also note the following: if $z_1, \cdots, z_{s-1}$ are p-independent, but $z_1, \cdots, z_s$ are not, then we can (constructively) write z_s in the form

$$z_s = \sum c_{i_1 \cdots i_{s-1}} z_1^{i_1} \cdots z_{s-1}^{i_{s-1}}, \quad 0 \leq i_j \leq p-1, \quad c_{i_1 \cdots i_{s-1}} \in k^p.$$

For we already have a polynomial $F(z_1, \cdots, z_{s-1}, Z)$ over k^p of degree $< p$ in Z and satisfied by z_s; also $Z^p - z_s^p$ is satisfied by z_s. Hence we can soon get z_s in the desired form (by taking a GCD, etc.).

For the converse, let (P′) be the condition like (P) except that it refers to a single equation. Then (P′) and (P) are equivalent. In fact, (P) obviously implies (P′). Conversely, let (P′) hold and let $\Sigma\, a_{ij} X_j = 0$ be a finite system with $a_{ij} \in k$, to be solved nontrivially in k^p. From the a_{ij} one can pick out a maximal k^p-linearly independent subset $\{\lambda_k\}$: this can be done with (P′) alone. Then we can write $a_{ij} = \Sigma\, a_{ijk} \lambda_k$, $a_{ijk} \in k^p$, and our given system is equivalent to $\Sigma\, a_{ijk} X_j = 0$. Extracting the pth roots of the left-hand sides, we get a simple linear system to be resolved. So (P′) and (P) are equivalent. Now let (P″) be the condition that any elements $z_1, \cdots, z_s$ in k can be checked for p-independence, and in the case of p-dependence, one can write down an equation exhibiting this: then (P′) and (P″) are equivalent. In fact, (P′) obviously implies (P″). Conversely, let (P″) hold for k and let $\lambda_1, \cdots, \lambda_t$ be elements in k. By (P″) we can find a p-basis amongst the λ_i for $k^p(\lambda_1, \cdots, \lambda_t)$: say these are $\lambda_1, \cdots, \lambda_s$, so that $k^p(\lambda_1, \cdots, \lambda_t) = k^p(\lambda_1, \cdots, \lambda_s)$ and $[k^p(\lambda_1, \cdots, \lambda_s) : k^p] = p^s$. By the remark in the previous paragraph, we can write $\lambda_{s+1}, \cdots, \lambda_t$ (and $\lambda_1, \cdots, \lambda_s$, too) as k^p-linear combinations of $\lambda_1^{i_1} \cdots \lambda_s^{i_s}$, $0 \leq i_j \leq p-1$. Thus $\lambda_1, \cdots, \lambda_t$ are k^p-linear combinations of elements linearly independent over k^p. The problem is now a linear one over k^p, and the proof is complete.

44. Let $p = \text{ch}\, k > 0$. For any $a_1, \cdots, a_n \in k$, the ideal $(X_1^p - a_1, \cdots, X_n^p - a_n)$ is primary; and it is prime if and only if $a_1, \cdots, a_n$ are p-independent.

We omit the simple proof.

Remark. The ground-form of $(X_1^p - a_1, \cdots, X_n^p - a_n)$ is $X_1'^p - u_1^p a_1 - \cdots - u_n^p a_n$. This is irreducible if $[k^p(a) : k^p] \geq p$. Hence a primary ideal not a prime may very well have an irreducible ground-form. This is not possible, however, for a primary ideal Q whose associated prime P is separable, since if P is separable and A is the ideal generated by the coefficients of its ground-form, then it is known [3, p. 131, Theorem 5] that $A = P \cap Q_1 \cap \cdots \cap Q_s$, with the primes of $Q_1, \cdots, Q_s$ embedded.

45. Consider the problem: Given a primary ideal Q in $k[X_1, \cdots, X_n]$, to construct its associated prime (cf. 42). A necessary and sufficient condition for this problem to have a positive resolution is that k satisfy (P).

Proof. The necessity follows from 44 and 43: to test the p-independence of $a_1, \cdots, a_n$ we merely have to test whether $(X_1^p - a_1, \cdots, X_n^p - a_n)$ is equal to its associated prime; moreover, if $a_1, \cdots, a_{n-1}$ are p-independent but $a_1, \cdots, a_n$ are not, then $X_n^p - a_n$ is a pth power in

$$k[X_1, \cdots, X_n]/(X_1^p - a_1, \cdots, X_{n-1}^p - a_{n-1}) = k(a_1^{1/p}, \cdots, a_{n-1}^{1/p})[X_n],$$

one can construct its pth root, and from this get a desired expression for a_n as an element of $k^p(a_1, \cdots, a_{n-1})$.

As for the sufficiency, the proof is by induction on n. First, for $n = 1$, let (F) be a given primary ideal in $k[X]$, $X = X_1$. We may assume F is monic. We make an induction on $\deg F$. If F is not a polynomial in X^p, then $dF/dX \neq 0$; and $F/\text{GCD}\,(F, dF/dX)$ is the desired polynomial. If F *is* a polynomial in X^p, we first test whether it is a pth power: we have merely to test whether each coefficient is a pth power. If F is a pth power, $F = F_1^p$, then $\deg F_1 < \deg F$, and we achieve a reduction. If F *is not a* pth power, then $F = F_1^r$, where $r \not\equiv 0\ (p)$ and hence F_1 is a polynomial in X^p. Place $X^p = Y$, $F(X) = G(Y)$. Then $(G(Y))$ is primary and we need only study G. Hence again we have a reduction, and the proof for $n = 1$ is complete.

For $n > 1$, we make an induction on $\dim Q$. If $\dim Q > 0$, then (as in 42) we adjoin $u_1 X_1 + \cdots + u_n X_n$, u_i indeterminates, to the base field, to achieve a reduction in $\dim Q$. If $\dim Q = 0$, then by 23 we can find $Q \cap k[X_1] = (g)$; and, by the foregoing, an irreducible $f \in k[X_1]$ such that $g = cf^r$, $c \in k$. Now we complete the proof as in 42 (first proof).

46. Consider the problem: Given an ideal A in $k[X_1, \cdots, X_n]$, to find its associated primes. A necessary and sufficient condition for this problem to have a positive resolution is that k satisfy (F) and (P).

Proof. The necessity of (F) follows immediately from the case $n = 1$; the necessity of (P) follows from (the first part of) 45. The sufficiency follows from 36 and 42.

Remark. Since any prime field of given characteristic satisfies (F) and (P), *all of our constructions hold for an absolutely given base field.*

Independence of the conditions (P) and (F).

47. *Example of an explicitly given field not satisfying* (F). In [10] van der Waerden showed that it is out of the question to establish (F) for an arbitrary explicitly given field. We reproduce his argument as we shall have to use it several times. Let, then, E (= $E(n)$) be a property of positive integers having the following properties: For any positive integer we can decide whether $E(n)$ holds, but *we* do not know how to decide whether there exists an n for which $E(n)$ holds. For example, let $E(n)$ be the assertion that in the decimal expansion of π the nth, $(n+1)$th, $\cdots$, $(n+98)$th digits are all nines. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \cdots$ be the sequence of positive primes and let $x_1, x_2, \cdots$ be a sequence of numbers defined as follows: if $E(n)$ does not hold, we define $x_n = (p_n)^{1/2}$; if $E(n)$ does hold, we define $x_n = (-1)^{1/2}$. If, now, we could establish (F) for $k = Q(x_1, x_2, \cdots)$, where Q is the rational number field, then we could decide whether there is an n for which $E(n)$ holds, for there is such an n if and only if $X^2 + 1$ factors properly in $k[X]$.

From an intuitive point of view, van der Waerden's argument is about as convincing as one could want, short of an actual counterexample. Actually, his argument can be strengthened, from a classical point of view; and one can even, on the basis of a widely accepted definition of *computable*, give an actual counterexample; see [6]. However, partly for simplicity, we here limit ourselves to van der Waerden's argument. From [6] it will be clear how to modify our arguments, if this is desired.

Remark. Scrutinizing van der Waerden's argument, one may wonder what the role of the p_i is: if instead of $(p_n)^{1/2}$ one adjoins 0, one comes to the same conclusion. Thus, as one sees, the distinction is not between finite and infinite extensions of a prime field k_0, but rather between explicitly given and canonically given extensions of k_0.

48. **Lemma.** *Let L/k be separable (i.e., elements in L linearly independent over k remain such over $k^{1/p}$, so that L and $k^{1/p}$ are linearly disjoint over k). If a system of equations $\Sigma\, a_{ij} X_j^p = 0$, $a_{ij} \in k$, has a nontrivial solution in L, then it has a nontrivial solution in k ($p = \text{ch}\, k$).*

For the simple proof, we refer to [5, p. 21].

49. *Example of an explicitly given field satisfying* (P) *but not* (F). In the case of characteristic 0, (P) is vacuous, so 47 gives an example. However, one will want an example in positive characteristic. Let, then, $E = E(n)$ be as in 47.

Let k_0 be a prime field of characteristic $p = 3$ (or any prime p not having -1 as quadratic residue). Define a sequence of fields recursively as follows: $k_i = k_{i-1}$ if $E(i)$ does not hold and $k_i = k_{i-1}((-1)^{1/2})$ if E_i does hold. Clearly $k = \bigcup k_i$ is an explicitly given field. Now given a finite system $\Sigma\, a_{ij} X_j^p = 0$, let k_m contain the a_{ij}. By 40, k_m satisfies (P), so we can decide whether the system has a solution in k_m, and if it does, can find one. By 48, this allows us to decide whether the system has a solution in k, and if it does, to find one. Hence k satisfies (P). On the other hand, as in 48, we cannot decide whether $X^2 + 1$ factors properly over k.

50. **Lemma.** *Let k_0 be a prime field of* ch $p \neq 0$. *Let a, b be indeterminates over k_0 and let $K = k_0(a, b)$. In the polynomial ring $K[X, Y]$, the polynomial $Y^p - a - bX^p$ is (obviously) irreducible. Let (x, y) be a generic zero over K of $(Y^p - a - bX^p)$. Then K is algebraically closed in $K(x, y)$.*

Proof. Let $q \in K(x, y)$ be algebraic over k, write:

$$q = (a_0(x) + a_1(x)y + \cdots + a_{p-1}(x)y^{p-1})/c(x),$$

with $a_i(x)$, $c(x) \in K[x]$. Then q^p is in $K(x)$ and hence in K. Then

$$a_0^p(x) + a_1^p(x)(a + bx^p) + \cdots + a_{p-1}^p(x)(a + bx^p)^{p-1} = u(a, b)c^p(x).$$

Clearing appropriate denominators in $k_0[a, b]$, we may suppose the a_i and c to be in $k_0[a, b, x]$ and, changing q by a factor in $k_0[a, b]$, that $u(a, b)$ is in $k_0[a, b]$. Comparing the coefficients of $a^{rp+(p-1)}$ on both sides, we see that $a_{p-1} \equiv 0$ (c) in $k_0[a, b, x]$. Then comparing the coefficients of $a^{sp+(p-2)}$, we see that $a_{p-2} \equiv 0$ (c); etc., so we may assume $c = 1$. Now comparing the coefficients of $b^{tp+(p-1)}$, we see that $a_{p-1} = 0$; and then successively that $a_{p-2}, \cdots, a_1$ are zero. So $q = a_0(x) \in K(x)$, whence $q \in K$.

51. *Example of an explicitly given field satisfying* (F) *but not* (P). Let $E = E(n)$ be as in 47. Let k_0 be a prime field of given characteristic $p \neq 0$, let a, b be indeterminates, and let $K_0 = k_0(a, b)$. Define a sequence of fields $K_0, K_1, K_2, \cdots$ recursively as follows: $K_i = K_{i-1}(x, (a + bx^p)^{1/p})$ with x transcendental over K_{i-1} if i is the least integer for which $E(i)$ holds; and otherwise $K_i = K_{i-1}$. Let $K = \bigcup K_i$. Each K_i, and also K, is either $= k_0(a, b)$ or $= k_0(a, b, x, (a + bx^p)^{1/p}) = k_0(b, x, (a + bx^p)^{1/p})$, a pure transcendental extension of k_0 with degree of transcendency 3. Hence each K_i satisfies (F). Since, by 50, each K_i is algebraically closed in K_{i+1}, any complete factorization of a polynomial over K_i remains such over K_{i+1}, whence also K satisfies (F). On the other hand, we cannot decide whether $Y^p - aZ^p - bX^p = 0$ has a nontrivial solution in K, for there is such a solution if and only if there exists an i such that $E(i)$ holds. Hence K does not satisfy (P).

52. *Example of an explicitly given field K satisfying* (F) *but containing an a such that $K(a^{1/p})$ does not satisfy* (F) (*cf.* [6]). The field K of 51 also applies here, since $b^{1/p} \in K(a^{1/p})$ if and only if $E(i)$ holds for some i.

53. *Example of a primary ideal Q in a polynomial ring over an explicitly given field K satisfying* (F) *such that its associated prime cannot be constructed.* Let K be the field K of 51, and let $Q = (X^p - a, Y^p - b)$ in $K[X, Y]$. If the associated prime could be constructed, then we could decide whether a, b are p-dependent, but a, b are p-dependent if and only if $E(i)$ holds for some i, and this cannot be decided.

54. *Example of an explicitly given field k satisfying* (F$'$), *of* 36, *but not* (F). Let $k = K(a^{1/p})$, where K, a are as in 51 and 52. Then $k = K(a^{1/p})$ does not satisfy (F), by 52. On the other hand, let $F \in k[X_1, \cdots, X_n] - 0$. Since K satisfies (F), we can construct a complete factorization of F^p in $K[X_1, \cdots, X_n]$, $F^p = cF_1^{r_1} \cdots F_s^{r_s}$; we may assume $F, F_1, \cdots, F_s$ monic, whence $c = 1$; $F_i \neq F_j$ for $i \neq j$. Then $r_i \equiv 0\ (p)$ for every i and $F = F_1^{r_1/p} \cdots F_s^{r_s/p}$ holds in $k[X_1, \cdots, X_n]$. Here (F_i) and $(F_i^{r_i/p})$ are primary, so one gets the desired primary decomposition in $k[X_1, \cdots, X_n]$.

Computation of some bounds.

55. Let $f_{i1}g_1 + \cdots + f_{is}g_s = 0$, $i = 1, \cdots, r$, $f_{ij} \in k[X_1, \cdots, X_n]$, be the system considered in 1, and let $d \geq \max\{\deg f_{ij}\}$. Then there is a $k[X]$-module basis $(g_1^{(i)}, \cdots, g_s^{(i)})$, $g_j^{(i)} \in k[X]$, for the solutions, in fact the basis constructed in 1, such that $n(rd)^{2^{n-1}}$ is a bound on $\deg g_j^{(i)}$. Here the bound is a simple, in fact, primitive recursive function of n, r, d.

Proof. In 1 we wrote down some solutions $(g_{11}, \cdots, g_{1r}; \Delta, 0, \cdots, 0), \cdots, (g_{s1}, \cdots, g_{sr}; 0, \cdots, 0, \Delta)$. One finds here that $\deg_{X_n} g_{ij} \leq rd$ and $\deg \Delta \leq rd$. We then place a bound on the degrees in X_n of the sought $g_1, \cdots, g_s$: one finds that $rd - 1$ is such a bound. Then the g_i are written as polynomials $\Sigma\, g_{ij}X_n^j$ of degree $rd - 1$ in X_n with coefficients in $k[X_1, \cdots, X_{n-1}]$. Each equation $f_{i1}g_1 + \cdots + f_{is}g_s = 0$ then gives rise to rd equations in the g_{ij}; and altogether we get r^2d equations. Let $M(n, r, d)$ be a sought bound. Then one sees that $M(n, r, d) = rd + M(n-1, r^2d, d)$ yields a recursive relation for a possible M. Noting that for $n = 0$, $M(0, r, d) = 0$ is allowable, we find $rd + (rd)^2 + (rd)^4 + \cdots + (rd)^{2^{n-1}}$ as a formula for $M(n, r, d)$. This is $\leq n(rd)^{2^{n-1}}$.

56. Let $A = (f_1, \cdots, f_r)$, $B = (f_{r+1}, \cdots, f_s)$ be two ideals in $k[X_1, \cdots, X_n]$, and let $d \geq \max\{\deg f_i\}$. Then $A \cap B$ has a basis of elements of degree $\leq nd^{2^{n-1}} + d$ and $A : B$ has a basis of elements of degree $\leq n((d+n)^n d)^{2^{n-1}}$.

Proof. The formula for $A \cap B$ is a direct application of 55. As for $A : B$, if B has a basis of s elements one gets directly that $n(sd)^{2^{n-1}}$ is a desired bound. Now the number of power products of degree $\leq d$ in n letters is $\binom{d+n}{n}$, which is $\leq (d+n)^n$. One may replace s with $(d+n)^n$.

57. Let $f_{i1}g_1 + \cdots + f_{is}g_s = b_i$, $i = 1, \cdots, r$, f_{ij}, $b_i \in k[X_1, \cdots, X_n]$, be the system considered in 4. Then the system has a solution in $K[X]$ only if it has one with $\deg_{X_n} g_i \leq n(rd)^{2^{n-1}}$.

The proof is like that of 55.

58. Let $A = (f_1, \cdots, f_s)$ be an ideal in $k[X_1, \cdots, X_n]$ and let $d \geq \max\{\deg f_{ij}\}$. Then $X_1, \cdots, X_r$ are algebraically dependent over k mod A only if there is an $f \in k[X_1, \cdots, X_r] - 0$ in A with $\deg f \leq r(d(d+1)^{n-r})^{2^{r-1}}$.

Proof. We consider the equation $f_1g_1 + \cdots + f_sg_s + g_{s+1} = 0$ with the g_i sought in $k[X_1, \cdots, X_r]$. This equation can be replaced equivalently by $d+1$ equations with coefficients in $k[X_1, \cdots, X_{n-1}]$, and eventually by $(d+1)^{n-r}$ equations with coefficients in $k[X_1, \cdots, X_r]$; the bound d remains a bound. By 55, $r(d(d+1)^{n-r})^{2^{r-1}}$ is a desired bound.

59. Let $X = X_1$, $R = k[X]$, $S = k(X)$, $RZ_1 + \cdots + RZ_s$, $m = (l_1, \cdots, l_t)$, $l_i = f_{i1}(X)Z_1 + \cdots + f_{is}(X)Z_s$, $m_1 = S_m \cap \Sigma RZ_i$ be as in 8 and let $d \geq \max\{\deg f_{ij}\}$. Then there is a polynomial F with $\deg F \leq td$ such that $Fm_1 \subset m$.

Proof. In the proof of 8, one can take the g_i such that $g_{i+1} \equiv 0$ (g_i) for $i = 1, \cdots, r-1$. Then $F = g_r$ is a desired F.

Remark. To get a bound on F one does not need the additional observation of the proof, but the bound td simplifies some future calculations.

60. Let $R = k[X_1, \cdots, X_n]$, $m = (l_1, \cdots, l_t)$, $l_i = f_{i1}Z_1 + \cdots + f_{is}Z_s$, $X_1' = u_1X_1 + \cdots + u_nX_n$, $m_1 = k(u, X_1')[X_2, \cdots, X_n]m \cap \Sigma RZ_i$ be as in 11, and let $q \geq \max \deg\{f_{ij}\}$. (Here deg stands for the degree in all the variables $X_1, \cdots, X_n$.) Then there is an $F \in k(u)[X_1'] - 0$ of degree $\leq (qt)^{2^{n-1}}$ such that $Fm_1 \subset m$.

Proof. Let u_{ij}, $i, j = 1, \cdots, n$, be indeterminates (with $u_{1j} = u_j$) and call the variables $X_1', \cdots, X_n'$ *the transformed variables*. From 9 we can write $Sm \cap \Sigma RZ_j = m + (S_n n \cap \Sigma R_n\zeta_k)$, where it is understood that one is working with the transformed variables over $k(u)$, so that $S = k(u, X_1')[X_2', \cdots, X_n']$, $R_n' = k(u)[X_1', \cdots, X_{n-1}']$, etc. By 11, Remark, the module $S_n n \cap \Sigma R_n\zeta_k$ is already prepared for an induction. Moreover, an F for $S_n n \cap \Sigma R_n\zeta_k$ is also an F for $Sm \cap \Sigma RZ_i$. Now the first step in constructing F is to replace $l_1, \cdots, l_t$ by $l_1, \cdots, l_t, \cdots, l_1X_n^{tq-1}, \cdots, l_tX_n^{tq-1}$, thus t forms by t^2q forms. The bound q remains a bound. Thus a second step replaces t^2q forms by t^4q^3; and after $n-1$ steps, we get $(tq)^{2^{n-1}}/q$ forms with coefficients in $k(u)[X_1']$. By 59 we get the desired results, at least over $k(u) = k(\cdots, u_{ij}, \cdots)$. One can unload the superfluous variables by the first paragraph of 11.

Remark. Since $m_1 = m : F$, applying 55 one sees that m_1 has a basis $g_1^{(i)}Z_1 + \cdots + g_s^{(i)}Z_s$ with $\deg g_j^{(i)} \leq n(s(qt)^{2^{n-1}})^{2^{n-1}}$.

61. By a *rational step*, or more simply *step* for the constructions not involving conditions (F) or (P), we mean a field operation in the base field k. Later we give a different definition for *step* if (F) or (P) is involved.

62. The number of steps required for the constructions of 55–60 can be bounded by simple, in fact primitive recursive functions of the numerical data (n, r, s, d, q, t).

Proof. This could be established by following the proofs in 1–11, but the counting of the number of steps in 55, for example, can be simplified by noting that once one has a bound on deg g_i, $i = 1, \cdots, s$, the system can be converted into a homogeneous linear system. Similar remarks hold for 56–58. In 59 one will have to place a bound on the number of steps required to put an $r \times s$ matrix with entries from $k[X_1]$ into the desired canonical form. This problem is too straightforward to be taken up here, as is the problem of computing a bound on the number of steps required to write down a basis for a homogeneous linear system of r equations in n unknowns.

Remark. In 60 one will note that something new is afoot, since having a bound on deg F does not linearize the problem of finding m_1. To find m_1, one will have to know F itself.

63. Let $f_{i1}g_1 + \cdots + f_{is}g_s = 0$, $i = 1, \cdots, s$, be the system considered in 1 and 55, so that $n(rd)^{2^{n-1}}$ is a bound on deg $g_j^{(i)}$ of some $k[X]$-module basis for the solutions. Then there is a simple, in fact primitive recursive, function $F(n, s, r, d)$ that bounds the number of steps needed to produce a basis $\{(g_1^{(i)}, \cdots, g_s^{(i)})\}$ and at the same time bounds the number of elements in the basis produced. Let $m_1 = k(u, X_1')[X_2, \cdots, X_n]m \cap \sum RZ_i$ be as in 11 and 60, so that there is an $F = F(X_1')$ of degree $\leq (qt)^{2^{n-1}}$ such that $m_1 = m : F$. Then there is a simple, in fact primitive recursive, function $G(n, s, t, q)$ that bounds the number of steps needed to produce a basis $\{l^{(i)}\}$, $l^{(i)} = g_1^{(i)}Z_1 + \cdots + g_s^{(i)}Z_s$, for m_1 and at the same time bounds the number of elements in the basis produced.

The proofs are immediate.

64. Let $R = k[X_1, \cdots, X_n]$, $m = (l_1, \cdots, l_t)$, $l_i = f_{i1}Z_1 + \cdots + f_{is}Z_s$ be as in 12, and let $d \geq \max\{\deg f_{ij}\}$. Let $G(n, s, t, d)$ be a function given by 63 for bounding the number of steps needed to produce a $k[X]$-module basis for $m_1 = k(u, X_1')[X_2, \cdots, X_n]m \cap \sum RZ_i$ and which also bounds the number of generators produced. Let $B(n, s, t, d)$ be a function defined recursively by

$$B(1, s, t, d) = F(1, s, t, d),$$

$$B(n, s, t, d) = F(n-1, s, B(n-1, s, t, d), 2^{B(n-1,s,t,d)}d).$$

Then $B(n, s, t, d)$ is a bound on the number of steps in a canonical construction for producing a $k[X]$-module basis of $k(X)m \cap \sum RZ_i$ and is also a bound on the number of generators produced. Thus B is primitive recursive.

Proof. Let $B(n, s, t, d)$ be a sought bound for the construction in 12. The proof first extends the base field and finds $m_1 = k(u, X)m \cap \sum k(u, X_1')[X_2, \cdots, X_n]Z_i$.

This takes at most $B(n-1, s, t, d)$ steps and produces at most $B(n-1, s, t, d)$ generators. Next 11 is applied. Let $c_1 = f_1(X_1')/g_1(X_1'), \cdots, c_m = f_m(X_1')/g_m(X_1')$ be a set of elements in $k(u, X_1')$ written as quotients of polynomials. If $d \geq \max\{\deg f_i, \deg g_j\}$, then any rational operation on the set produces another in which $2d$ is a bound. Hence for m, one gets a basis in $\Sigma\, k[X]Z_i$ with $2^{B(n-1,s,t,d)}d$ as a bound on the degrees in question. Now the recursion formulae are obvious.

65. Let $A = (f_1, \cdots, f_t)$ be an ideal in $k[X_1, \cdots, X_n]$. Then there is a primitive recursive function $B(n, d)$ and a normal decomposition $A = Q_1 \cap \cdots \cap Q_s$ such that s and the exponents of the Q_i are $\leq B(n, d)$ and such that the Q_i and their associated primes have $B(n, d)$, or fewer, generators of degree $\leq B(n, d)$.

Proof. A difficulty occurred in 12 because of a change in base field; but after that, through 29, no new impediment intervenes for computing the desired bounds. In 36, which constructs a normal decomposition for an unmixed ideal, one needs to factor the ground-form F; but here we are not making a construction, and only need a bound on the degrees of the factors of F. A similar remark holds for getting the desired information on the associated primes (the homomorphism of 42 causes no difficulty). The number t does not enter because we may suppose $t = \binom{n+d}{d}$.

66. For the constructions involving (F) or (P), in the general case we define a *step* as a field operation in the base field k *or* an application of (F) or (P); in the case of an absolutely given field k, by a *step* we mean an addition, subtraction, or multiplication in Z. In either case one could easily put a bound B on the number of steps required for any of our constructions, but in the latter case B will be a function also of a bound b on the coefficients in the data (also of the data defining k), cf. [6, p. 14].

Specialization arguments. In this section we recall some specialization arguments of Krull [2]. The section does not, for the moment, have a constructive intent, though later we shall modify it for constructive purposes.

67. Let k be an infinite base field, t, a single indeterminate (as with Krull) or several indeterminates. Let $f(t, X) \in k(t)[X_1, \cdots, X_n]$ and $a_i \in k$, where $a = (\cdots, a_i, \cdots)$. If $f(t, X)$ can be written in the form $g(t, X)/d(t)$ with $g \in k[t, X]$, $d \in k[t]$ and $d(a) \neq 0$, we define $f(a, X)$ by substitution. Let $A(t)$ be an ideal in $k(t)[X]$, $A(t) = \{f(t, X)\}$. We define $A(a)$ to be the set of $f(a, X)$ insofar as these are defined; then $A(a)$ is obviously a $k[X]$-ideal. For an ideal $A(t) = \{f(t, X)\}$ in $k[t, X]$ we define $A(a)$ as $\{f(a, X)\}$. Similar definitions can be given for a submodule $m(t)$ of a free $k(t)[X]$-module.

A property $P = P(t)$ is said to hold *almost always* if $P(a)$ holds for at least one a ($a_i \in k$) and if there is a polynomial $h(t) \in k[t] - 0$ such that $P(a)$ holds whenever $h(a) \neq 0$.

68. Let $A(t)$ be an ideal in $k(t)[X_1, \cdots, X_n]$. Then $A(t)$ has a basis $f_1^*(t, X), \cdots, f_m^*(t, X)$ such that for all a $(a_i \in k)$ we have $A(a) = (f_1^*(a, X), \cdots, f_m^*(a, X))$. And for any basis $f_1(t, X), \cdots, f_s(t, X)$ almost always $A(a) = (f_1(a, X), \cdots, f_s(a, X))$.

Proof. We recall Krull's proof. Let $B(t) = A(t) \cap k[t, X]$. One first observes that for all a $(a_i \in k)$, $B(a) = A(a)$, which is obvious. Let $f_1^*(t, X), \cdots, f_m^*(t, X)$ be a basis of $B(t)$. Then obviously $B(a) = (f_1^*(a, X), \cdots, f_m^*(a, X))$, whence the first part of the theorem (Satz 1 of [2]) follows. Now let $f_1, \cdots, f_s$ be any basis of $A(t)$. Then one has equations: $f_i^*(t, X) = \Sigma_{k=1}^s c_{ik}(t, X)f_i(t, X)$, and since $f_i^*(a, X) = \Sigma\, c_{ik}(a, X)f_k(a, X)$ holds almost always, the second part follows.

Remark. We have recalled Krull's proof, as later it makes us abandon the theorem.

69. Let the system $f_{i1}g_1 + \cdots + f_{is}g_s = 0$, $i = 1, \cdots, r$, $f_{ij} \in k(t)[X_1, \cdots, X_n] = k(t)[X]$, have $\{(g_1^{(i)}, \cdots, g_s^{(i)})\}$, $g_j^{(i)} \in k(t)[X]$, as a $k(t)[X]$-basis for its solutions. Then, almost always, $\{(g_1^{(i)}(a, X), \cdots, g_s^{(i)}(a, X))\}$ is a $k[X]$-basis for the specialized system $\{f_{i1}(a, X)g_1 + \cdots + f_i(a, X)g_s = 0\}$. Let $A(t)$, $B(t)$, $C(t)$, $D(t)$ be ideals in $k(t)[X]$ with $A(t) \cap B(t) = C(t)$, $A(t) : B(t) = D(t)$. Then almost always $A(a) \cap B(a) = C(a)$ and $A(a) : B(a) = D(a)$. If $A(t)$ is unmixed r-dimensional with $F(t, X)$ as ground-form, then almost always $A(a)$ is unmixed r-dimensional with $F(a, X)$ as ground-form.

Proof. Let $\{(g_1^{*(i)}, \cdots, g_s^{*(i)})\}$ be the basis for the solutions found by the canonical process of 1. If t is specialized to a in such a way that certain coefficients (in $k(t)$) do not become zero, then the canonical process for the specialized system $f_{i1}(a, X)g_1 + \cdots + f_{is}(a, X)g_s = 0$, $i = 1, \cdots, r$, is parallel to that for the general system and so leads to $\{(g_1^{*(i)}(a, X), \cdots, g_s^{*(i)}(a, X))\}$ as a basis for the solutions of the specialized system. Now let $\{(g_1^{(j)}, \cdots, g_s^{(j)})\}$ be another basis for the solutions of the general system. The elements of this basis can be written in terms of those of the other and vice versa; and these relations continue to hold almost always. Hence $\{(g_1^{(j)}(a, X), \cdots, g_s^{(j)}(a, X))\}$ is almost always a basis for the solutions of the specialized system. This proves the first point and the others are proved similarly.

Remark. The constructions through 29 yield properties that hold almost always; on the other hand, those involving (F) or (P) do not. Thus a primary ideal may fail to remain primary, a normal decomposition to remain a normal decomposition, a prime to remain prime upon specialization. Still, the ground-form can be made a basis for their study, as well as for a study of the behavior of a prime ideal under extension of the base field, cf. [3]. An unmixed r-dimensional ideal A remains unmixed r-dimensional upon extension of the base field, since starting from a given basis of A, the canonical process showing that A is unmixed r-dimensional remains such over the extended field. This proof was missed in context by Krull (cf. [3, Note 7, p. 134]); a different proof was given in [4, p. 37]. Also, the ground-form remains the same upon extension of the base field.

The leading coefficient ideal and subcoefficient ideal of a given ideal. The constructions of this section hold for any explicitly given field k.

70. Let A be an ideal in $k[X_1, \cdots, X_n]$. By the ith *leading coefficient* ideal $L_i(A)$ we mean the set of coefficients of X_n^i in the polynomials f in A with $\deg_{X_n} f = i$, together with 0. The ith leading coefficient ideal is contained in the $(i+1)$th, and their union is *the leading coefficient ideal* $L(A)$ of A. By the ith *subcoefficient ideal* $S_i(A)$ we mean the set of coefficients of X_n^i in the polynomials f in A with $\text{subdegree}_{X_n} f = i$, together with 0.

71. Let $f_1, \cdots, f_s \in k[X_1, \cdots, X_n]$, $n \geq 1$, with one of the f_i regular in $X_1, \cdots, X_n$, and let $d \geq \max\{\deg f_i\}$. Then for every i one can construct $L_i((f_1, \cdots, f_s))$ within a number of steps depending only on n, s, d and i (or, also, only on a bound for these). One may also construct polynomials $h_1^{(i)}, \cdots, h_{t_i}^{(i)}$ in A of degree i in X_n whose leading coefficients will generate $L_i((f_1, \cdots, f_s))$, and one can bound the deg $h_j^{(i)}$ in terms of n, s, d and i (or, also, on a bound for these). Similar assertions hold for $S_i((f_1, \cdots, f_s))$, even without the regularity assumption. All bounds may be taken to be primitive recursive.

The proof is like that of 22. In the case of S_i, one has merely to consider elements of the form $g_1 f_1 + \cdots + g_s f_s$ with $\max\{\deg g_j\} \leq i$, so one needs no regularity assumption to depress the degrees of the g_j.

72. Let $f_1, \cdots, f_s$ be as in 71 and let $A = (f_1, \cdots, f_s)$. Then one can construct $L(A)$ within a number of steps depending only on n, s and d. Correspondingly one has a bound on the least ρ for which $L_\rho(A) = L_{\rho+1}(A) = \cdots$, on the number of elements in some basis of $L(A)$, and on their degrees. All bounds may be taken to be primitive recursive.

Proof. By 20 we can calculate a ρ such that $A : X_n^\rho = A : X_n^{\rho+1}$. Consider the $S_k(A)$, $k \leq \rho$, and polynomials $h_1^{(k)}, \cdots, h_{t_k}^{(k)}$ in A of subdegree k (in X_n) whose coefficients of X_n^k yield a basis of $S_k(A)$; and let d be a bound on their degrees, for $k \leq \rho$. Then $L_d(A) = L(A)$. In fact, let $g \in A$ with $\deg_{X_n} g = d' > d$. Subtracting from g appropriate $k[X_1, \cdots, X_{n-1}]$-linear combinations of the $h_j^{(k)}$, we get a g' in A of the same degree in X_n and with the same leading coefficient; so we may suppose $g \equiv 0 \ (X_n^{\rho+1})$. Then g/X_n is also in A, whence $L_{d'}(A) = L_{d'-1}(A)$, and the assertion $L_d(A) = L(A)$ follows.

Remark. Thus for A we have an integer e, depending only on n and d, which is a bound on the least ρ for which $L_\rho(A) = L_{\rho+1}(A) = \cdots$ and is also a bound on the degrees of some polynomials of degree $\rho, \rho-1, \cdots$ in X_n whose leading coefficients yield bases for $L_\rho(A)$, $L_{\rho-1}(A), \cdots$. (We will then have

$L_e(A) = L(A)$, e will be a bound on the degrees of the elements in some bases of $L_e(A)$, $L_{e-1}(A), \cdots$; and there will be polynomials in A of degree $\leq 2e$ and of degree e, $e-1, \cdots$ in X_n whose leading coefficients yield bases for $L_e(A)$, $L_{e-1}(A), \cdots$.) We may assume $e(n, d)$ is monotone increasing in each of the variables n, d and is primitive recursive.

The theory of polynomial ideals in strictly finite terms. In this section we show how to remove every nonfinite form of reasoning from our constructions. The constructions themselves are, of course, already in finite terms, but the underlying theory is not. The main way a nonfinite form of reasoning enters is through Hilbert's considerations on ascending chains of ideals—this is the only serious difficulty. Now Hilbert used these considerations to show that every ideal in $k[X_1, \cdots, X_n]$ has a finite basis, but this is no difficulty since for us an ideal is always given via a finite basis. However, his considerations also come in tacitly in the structure theorems, for example, in the normal decomposition theorem. Therefore we have to go over our proofs and, for example, remove each use of the normal decomposition theorem. We go over the proofs seriatim.

73. There is no occasion for comment until we come, in 6, to the construction of $\dim A$ for an ideal $A \neq (1)$ in $k[X_1, \cdots, X_n]$. Classically, one defines $\dim A$ by considering the associated primes $P_1, \cdots, P_s$ of A and placing $\dim A = \max\{\dim P_i\}$, where $\dim P_i = \mathrm{dt}\,(k[X]/P_i)/k$. This definition is not available to us. However, classically, $\dim A = \max\{r \mid k(X_{i_1}, \cdots, X_{i_r})[X]A \neq (1)\}$; and we could take this equation as defining $\dim A$. Call this Definition I. Now let u_{ij}, $i, j = 1, \cdots, n$, be indeterminates and let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$ be the "transformed" variables. Then also $\dim A = \max\{r \mid k(u, X_1', \cdots, X_r')[X]A \neq (1)\}$: and we could also take this equation to define $\dim A$. Call this Definition II. Classically it is obvious that the definitions are equivalent, but for us it is not obvious. This may be an interesting problem, but not an essential one. We merely have to pick some definition: we take Definition II, as this one is best adapted to our proofs.

One has: $r(\text{Def I}) \leq r(\text{Def II})$. The proof is a simple specialization argument. If $r(\text{Def I}) = 0$, then equality holds. The proof is a simple linear algebra argument.

74. Let $u_1, \cdots, u_n$ be indeterminates, $u_i' = a_{i1}u_1 + \cdots + a_{in}u_n$, $i = 1, \cdots, n$, $a_{ij} \in k$, $\det(a_{ij}) \neq 0$; write A for (a_{ij}). Let $f \in k[u_1, \cdots, u_n]$. Then: if $f(Au) = 0$, then $f = 0$. Similarly, if $b = (b_1, \cdots, b_n)$, $b_i \in k$, and $f(Au + b) = 0$, then $f = 0$.

Proof. If $f(Au) = 0$, then $f(A A^{-1}u) = 0$, whence the first statement follows; the second is proved similarly.

Remark. This will cover anything we need from the theory of transcendency through 95, though in 82 we get a full theory.

75. To use the method of reduction of dimension by extending the base field we should prove:

If A has dimension r over k and $t \leq r$, then $k(u, X_1', \cdots, X_t')[X]A$ has dimension $r - t$ over $k(u, X_1', \cdots, X_t')$.

Proof. Let V be the matrix of the transformation $X_1'' = X_1', \cdots, X_t'' = X_t'$, $X_i'' = v_{it+1}X_{t+1}' + \cdots + v_{in}X_n'$, $i = t + 1, \cdots, n$, where the v_{ij} are indeterminates, so that $W = VU$ is the matrix of the transformation: $X_i'' = w_{i1}X_1 + \cdots + w_{in}X_n$, $i = 1, \cdots, n$. Note that the w_{ij} are algebraically independent over $k(v, X)$; see 74. We have to prove:

$$k(u, v, X_1', \cdots, X_t', X_{t+1}'', \cdots, X_r'')[X'']A \neq (1)$$

and

$$k(u, v, X_1', \cdots, X_t', X_{t+1}'', \cdots, X_{r+1}'')[X'']A = (1).$$

This follows upon observing that $k(v, u) = k(v, w)$, that $u_{ij} \to w_{ij}$ determine an automorphism of $k(v, X, u)$ over $k(v, X)$, and that A has a basis in $k[X]$.

76. There is now no difficulty through 15, after which we can construct $k(u, X_1', \cdots, X_s')[X]A \cap k(u)[X]$ and $k(u, X_1', \cdots, X_s')[X]A \cap k[X]$.

Classically, one defines the depth of $A \neq (1)$ to be the minimum of the dimensions of the associated primes and one proves:

$$\text{depth } A = \max\{s \mid k(u, X_1', \cdots, X_s')[X]A \cap k[X] = A\}.$$

We now take this equation as the definition of *depth* of A. Clearly: depth $A \leq$ dim A. We say A is *unmixed* if depth A = dim A. If $t \leq s$ = depth A, then the depth of A diminishes by t upon extension of the base field to $k(u, X_1', \cdots, X_t')$; the proof is like that of 75.

77. We come now to the crucial points 16 and 18. In 16, dim $A > 0$, depth $A = 0$ and we wish to write $A = B \cap n$ with dim B = dim A, depth $B > 0$, dim $n = 0$. In 16, the equation $k(u_{11}, \cdots, u_{1n}, X_1')[X]A \cap k[X] = B$ was derived, but now we take it as defining B, so dim B = dim A and depth $B > 0$. As in 16 we get an $E_1 = E_1(X_1')$ such that $(A, E_1) \cap B = A$. Then we repeat the argument to get an $E_2 = E_2(X_2')$ such that $(A, E_1, E_2) \cap B_1 = (A, E_1)$. In 16 we proved $B_1 \supset B$ using a structure theorem; now we prove it as follows. We have

$$k(u_{11}, \cdots, u_{1n}, u_{21}, \cdots, u_{2n}, X_1')[X]A \cap k(u)[X] = B.$$

Applying the automorphism over k that interchanges u_{1j} and u_{2j} for $j = 1, \cdots, n$, we obtain:

$$k(u_{11}, \cdots, u_{1n}, u_{21}, \cdots, u_{2n}, X_2')[X]A \cap k(u)[X] = B$$

since $k(u_{11}, \cdots, u_{1n}, u_{21}, \cdots, u_{2n}, X_2')[X](A, E_1) \cap k(u)[X] = B_1$ by definition; and since $(A, E_1) \supset A$, we get $B_1 \supset B$. Hence we get $(A, E_1, E_2) \cap B = A$, and eventually $(A, E_1, E_2, \cdots, E_n) \cap B = A$, which gives the desired result over $k(u)$. To get it over k, before we used a structure theorem, but now we use a specialization argument.

The specialization theory of Krull as previously outlined in 67–69 is not quite in suitable form since, at least in the absence of condition (F), we do not know how to construct the ideal $B(t) = A(t) \cap k[t, X]$ of 68. However, a slight modification will suffice. First, for an $f \in k(t)[X]$, $f = g(t, X)/d(t)$ with $g \in k[t, X]$ and $d \in k[t]$, we define $f(a, X)$ as $g(a, X)/d(a)$ provided $d(a) \neq 0$ (we need not concern ourselves with rewriting f). For an ideal $A(t)$, we do not attempt to define $A(a)$, but if $A(t) = (f_1(t, X), \cdots, f_s(t, X))$, we can speak of the ideal $(f_1(a, X), \cdots, f_s(a, X))$ almost always. The definition of *almost always* is the same as before except that one should be able to construct the polynomial h; and to construct an $a = (a_1, a_2, \cdots)$, $a_i \in k$, such that $h(a) \neq 0$ (a condition assured by assuming k infinite). Now using our canonical constructions, it is obvious that if

$$(f_1(t, X), \cdots, f_s(t, X)) = (f_{s+1}(t, X), \cdots, f_u(t, X)),$$

then almost always

$$(f_1(a, X), \cdots, f_s(a, X)) = (f_{s+1}(a, X), \cdots, f_u(a, X))$$

and if

$$(f_1(t, X), \cdots, f_s(t, X)) \cap (g_1(t, X), \cdots, g_u(t, X)) = (h_1(t, X), \cdots, h_v(t, X)),$$

then almost always

$$(f_1(a, X), \cdots, f_s(a, X)) \cap (g_1(a, X), \cdots, g_u(a, X)) = (h_1(a, X), \cdots, h_v(a, X)).$$

Hence from $(A, E_1(u, X_1'), \cdots, E_n(u, X_n')) \cap B = A$, we get, specializing u to a $(a_{ij} \in k)$,

$$(A, E_1(a, \bar{X}_1), \cdots, E_n(a, \bar{X}_n)) \cap B = A \tag{1}$$

almost always; here instead of A and B we should have written $(f_1, \cdots, f_s)$ and $(g_1, \cdots, g_u)$ with $f_i, g_j \in k[X]$, but the slight abuse in notation should cause no great confusion. In specializing u to a, we also take care that $\det(a_{ij}) \neq 0$. Then (1) gives the desired result over k, at least if k is infinite.

For k finite, observe that the above proof does not require k to be infinite, but merely that k have "enough" elements; and the proof also tells how much "enough" is. Hence we construct a finite, normal extension field $k(\theta)$ having enough elements; the primitive element θ and its distinct conjugates $\theta_1 = \theta$, θ_2, $\cdots, \theta_s$ are available to us. If an ideal $A(\theta)$ in $k(\theta)[X]$ has a basis in $k[X]$ and if $a(\theta, X) = a_0(X) + a_1(X)\theta + \cdots + a_{s-1}(X)\theta^{s-1}$, $a_i \in k[X]$, is in $A(\theta)$, then so are $a(\theta_i, X)$, whence so are the $a_i(X)$. Thus if $A(\theta) = (\cdots, a_i(\theta, X), \cdots)$ and $a_i = a_{i0} + a_{i1}\theta + \cdots + a_{is-1}\theta^{s-1}$, then $A(\theta)$ has a basis in $k[X]$ if and only if it is the extension of $A' = (\cdots, a_{ij}, \cdots)$; and if so, then A' is the contraction of $A(\theta)$ to $k[X]$. One has a 0-dimensional ideal $n(\theta)$ such that $A = B \cap n(\theta)$. Hence also $A = B \cap n(\theta_i)$ and $A = B \cap (n(\theta_1) \cap \cdots \cap n(\theta_s))$. One proves in the familiar way that $n = n(\theta_1) \cap \cdots \cap n(\theta_s)$ is invariant under every automorphism of $k(\theta)$ over k, and hence that n is the extension of an ideal n' in $k[X]$; $\dim n' = 0$. Then $A = B \cap n'$ as desired.

78. In 18 we had an ideal A with $\dim A = r$, depth $A = s$; here $s \leq r$ and (to avoid a trivial case) let us suppose $s < r$. We then wrote $A = B \cap n$, with $\dim B = \dim A$, depth $B >$ depth A, and n unmixed of dimension = depth A. The proof was a simple reduction to dimension zero by extending the base field, but we do not see, from our present point of view, how to duplicate this technique, and will have to find a different way. (We do not see how to get the relation $A = B \cap (A, m^\rho)$ of 16.)

By definition $k(u, X_1', \cdots, X_{s+1}')[X]A \cap k[X] = B$ (so $\dim B = \dim A$, depth $B >$ depth A), from which we find an $E_1 = E_1'(X_1', \cdots, X_{s+1}')$ such that $A : E_1 = B$ and (as in 16) $A = B \cap (A, E_1)$. Now with a new set of indeterminates v and new transformed variables, we repeat the argument and find (as in 16): $A = B \cap (A, E_1, E_2)$. Let us repeat this construction over and over. We say that we can find an M such that $(A, E_1, E_2, \cdots, E_M) = (A, E_1, \cdots, E_{M+1})$; here $M \leq g(n, d)$, where n = number of x_i, d is a bound on the degrees of elements in a given basis of A, and g is multi-recursively defined. We may note that Hilbert's theorem on ascending chains says that an M exists, though it does not tell us how to find one; and anyway, we may not use Hilbert's theorem. We postpone to 79 an explanation of how to find a suitable M.

We have, then, $(A, E_1, \cdots, E_M) = (A, E_1, \cdots, E_{M+1})$. Let $u, v, \cdots, y, z$ be the successively new indeterminates for $E_1, E_2, \cdots, E_M, E_{M+1}$ respectively; and $X_{iu}, X_{jv}, \cdots$, the transformed variables. We now specialize $u, v, \cdots, y$, but not z, to k, assumed infinite, and in such a way as to get

$$(A, \overline{E}_1(X_1^*, \cdots, X_{s+1}^*), \cdots, \overline{E}_M(X_1^{**}, \cdots, X_{s+1}^{**}))$$
$$= (A, \overline{E}_1(X_1^*, \cdots, X_{s+1}^*), \cdots, \overline{E}_M(X_1^{**}, \cdots, X_{s+1}^{**}), \overline{E}_{M+1}(z; X_{1z}, \cdots, X_{s+1z})),$$

$\overline{E}_{M+1} \neq 0$, and $A = B \cap (A, \overline{E}_1, \cdots, \overline{E}_M)$. Since $(A, \overline{E}_1, \cdots, \overline{E}_M)$ has a basis in $k[X]$ and contains the element $\overline{E}_{M+1}(z; X_{1z}, \cdots, X_{s+1z})$, the ideal has dimension $\leq s$. Using an induction on r (and that depth $A = s$), one now easily proves that $(A, \overline{E}_1, \cdots, \overline{E}_M)$ is s-dimensional; and one can construct its s-dimensional part. Subject to 79, the proof is complete for infinite k, and finite k are taken care of as before (cf. 78).

Remark. Since classically it is obvious that $\dim(A, E_1) < \dim A$, one might seek improvements in 78.

79. We come now to a finitist version of Hilbert's theorem on ascending chains. We have proved this theorem in [7] and [8], but it will be well to recall the proof, especially as we already have all the ingredients for the proof, except for one combinatorial argument.

Theorem. *Let $f(i)$ be a nonnegative integer for $i = 0, 1, \cdots$ and consider ascending chains of ideals $A_0 < A_1 < \cdots < A_s$ in $k[X_1, \cdots, X_n]$, where A_i has a basis of elements of degree $\leq f(i)$. Then there is a multi-recursively defined function-functional g depending only on n and f such that the length of any such chain is $\leq g(n, f) = g_n(f)$. (Formulae for defining such a g are given in the proof.)*

Proof. In 72, for an ideal A in $k[X]$, we found a ρ such that $A : X_n^{\rho} = A : X_n^{\rho+1}$, but for the proof referred to 20. However, we can just as well work with the transformed variables $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$ (u_{ij}, indeterminates) and by 79 get a ρ such that $A : X_n'^{\rho} = A : X_n'^{\rho+1}$. We can, then, as in 72 find $L(A)$ and have the function $e(n, d)$ of 72, Remark. Then $e_i = e(n, f(i))$ is a corresponding bound for A_i. We shall occasionally write $e_f(n)$ for $e(n, f)$. Understood that we are working over $k(u)$ with the transformed variables, it will be convenient to write k for $k(u)$ and X_i for X_i'.

If f is not already monotone increasing, we may replace it by a function f' defined as follows: $f'(0) = f(0)$, $f'(i + 1) = f'(i) + f(i + 1) + 1$. Thus we may assume f monotone increasing. We do this. Then $f_j(i) = f(j + i)$ is a function like f for $A_j < A_{j+1} < \cdots$.

For inductive purposes, we generalize our theorem. Instead of just one chain $A_0 < A_1 < \cdots$, we will consider a finite set of (not necessarily strictly) ascending chains of ideals: $A_0^{(t)} \subset A_1^{(t)} \subset \cdots \subset A_s^{(t)}$, $t = 1, \cdots, m$. We say that the *set* is *strictly ascending* if for each i, $i = 0, 1, \cdots, s - 1$, there is at least one t for which $A_i^{(t)} < A_{i+1}^{(t)}$. The length of such a set of chains is by definition $s + 1$. Our theorem is now to be understood as asserted for any strictly ascending set of m chains. The function f gives a bound $f(i)$ for all the $A_i^{(t)}$, $t = 1, \cdots, m$; we may assume f monotone increasing. The bound $g_n(f)$ is to be replaced by a bound $g_n(m, f)$. The function e_f continues to apply to the $A_i^{(t)}$ for $t = 1, \cdots, m$.

The function f may be allowed to involve n, m.

We remark that if A, B are ideals with $A \subset B$, and $L_i(A) = L_i(B)$ for every i, then $A = B$.

For any integer j, we get an ascending chain of ideals $L_j(A_0^{(t)}) \subset L_j(A_1^{(t)}) \subset \cdots \subset L_j(A_s^{(t)})$ and thus, for $t = 1, \cdots, m$, m chains; altogether, for $j \leq e$, we get $(e + 1)m$ ascending chains (e, any integer). We have $L_{ef(0)}(A_0^{(t)}) = L(A_0^{(t)})$ for $t = 1, \cdots, m$; and consider the chains for $j \leq e_f(0)$. Assume for a moment that $L_{ef(0)}(A_i^{(t)}) = L(A_i^{(t)})$ for the $(s + 1)m$ ideals $A_i^{(t)}$. Then clearly the $(e_f(0) + 1)m$ chains $L_j(A_0^{(t)}) \subset \cdots \subset L_j(A_s^{(t)})$, $j \leq e_f(0)$, $t = 1, \cdots, m$, gives a strictly ascending set. By induction we have a bound $g_{n-1}((e_f(0) + 1)m, e_f)$ on $s + 1$; we may assume that $g_{n-1}(i, e_f)$ is monotone increasing in i and, inductively, that $g_{n-1}(i, e') \leq g_{n-1}(i, e'')$ for any monotone increasing functions e', e'' such that $e'(j) \leq e''(j)$ for all nonnegative integers j, otherwise put, we can say that if

$s + 1 > g_{n-1}((e_f(0) + 1)m, e_f)$, then for at least one pair (i, t) with $i \le 1 + g_{n-1}((e_f(0) + 1)m, e_f)$, $L_{e_f(0)}(A_i^{(t)}) < L_{e_f(i)}(A_i^{(t)})$; and also $L_{e_f(0)}(A_0^{(t)}) < L_{e_f(i)}(A_i^{(t)})$. In this way we would get a strictly ascending set

$$L_{e_f(0)}(A_0^{(t)}) \subset L_{e_f(i_1)}(A_{i_1}^{(t)}) \subset \cdots \subset L_{e_f(i_p)}(A_{i_p}^{(t)});$$

we suppose $i_1, i_2, \cdots$ to be taken successively as small as possible. Then $i_1 \le 1 + g_{n-1}((e_f(0) + 1)m, e_f)$; and by the monotonicity of e_f, we have a bound $e_f(1 + g_{n-1}((e_f(0) + 1)n, e_f))$ on the degrees of the elements in some bases of the $L_{e_f(i_1)}(A_{i_1}^{(t)})$. Similarly,

$$i_{j+1} - (i_j + 1) \le 1 + g_{n-1}((e_f(i_j) + 1)m, e_{f_{i_j}}).$$

Define a function $h(j)$ as follows:

$$h(0) = 0, \qquad h(j + 1) = h(j) + g_{n-1}((e_f(h(j)) + 1)m, e_{f_{h(j)}}).$$

Using the monotonicity properties of g_{n-1}, one sees by induction that $i_j \le h(j)$. Hence we have a bound $e_f(h(j))$ on the degrees of the elements in some bases of the $L_{e_f(i_j)}(A_{i_j}^{(t)})$. Hence, too, we have the bound $g_{n-1}(m, e_f(b)) = 1 + b$ on $1 + p$. Bringing the two parts of the argument together, we get

$$h(b) + g_{n-1}((e_f(h(b)) + 1)m, e_{f_{h(b)}}) = h(b + 1) = h(g_{n-1}(m, e_f(b))),$$

which is monotone as required, as a desired bound on $s + 1$.

Having now established 78 (or 18), there is no further difficulty through 22.

80. Classically we have the following theorem: An ideal is primary if and only if it is unmixed and its ground-form is a power of an irreducible polynomial. We now take this theorem as defining *primary*. We retain the classical definition of *prime*. A prime ideal is primary.

Remark. Our definition of primary is adapted to our work with condition (F).

81. Coming to 23, we encounter a difficulty, and, in fact, we abandon 23 for a primary ideal A, though we want it, and retain it, for A prime.(5) The proof now is very much as in 23, except that in 23, in the case $\dim A = s > 0$ (A, prime) and at least one of $X_1, \cdots, X_{n-1}$ is not algebraic over k mod A, we adjoined $X_1' = u_1X_1 + \cdots + u_{n-1}X_{n-1}$ to the base field and said that $\dim A = s - 1$ over $k(u, X_1')$, in order (by induction on s) to say that we can construct $k(u, X_1')[X_2, \cdots, X_n]A \cap k(u, X_1')[X_2, \cdots, X_{n-1}]$. With our present definition of dimension, the assertion on the dimension of A is not clear. However, we first make an induction on n! Then again it is clear that we can construct

(5) As already noted in footnote 4, we can construct $A \cap k[X_1, \cdots, X_{n-1}]$ for any ideal A over any explicitly given field k.

$k(u, X_1')[X_2, \cdots, X_n]A \cap k(u, X_1')[X_2, \cdots, X_{n-1}]$, since here n has been reduced.

Remark. Once we have the equivalence of our definition of primary with the classical definition, which, however, we will not get till we come to condition (P), we can come back to 23 for A primary.

82. There is now no difficulty through 27. Moreover, if $k(x_1, \cdots, x_n)$ is a canonically given extension of k and $y_1, \cdots, y_s$ are in $k(x)$, then one can decide whether $y_1, \cdots, y_s$ are algebraically independent over k. On the basis of this one can build up a full theory of transcendency along the lines of the familiar axiomatic method (cf. [11]).

83. There is no difficulty in 28 and 29, whereby we construct the ground-form of an unmixed ideal. For the moment, we need not discuss 30–32, since our work with primary ideals, with condition (F) but with (P) absent, never mentions prime ideals (though 30–32 do enter unofficially in that they motivate our definition of *primary*). Points 34 and 35 hold as before.

84. Using condition (F) alone, one can decide whether a given ideal is primary. This is obvious from our definition, though not from the classical one.

85. Let $A \neq (1)$ be an ideal in $k[X_1, \cdots, X_n]$. If A is not primary, then one can find $a, b \in k[X]$ with $ab \in A$, $a \notin A$, $b^\rho \notin A$, $\rho = 0, 1, 2, \cdots$.

Proof. There are two cases: (i) A is unmixed, (ii) A is mixed. In the first case, from the ground-form we can obviously get $F, G \in k[u, X] - 0$ such that $FG \in A$ but $F^\rho \notin A$, $G^\rho \notin A$, $\rho = 0, 1, \cdots$. By 20 (cf. 79 end), we can test whether some power of a coefficient of F, or of G, is in A. Let F_1 be the sum of the terms in F a power of each of which is in A, and define G_1 for G similarly; $F \neq F_1$, $G \neq G_1$. Then for a ρ one can compute $(F - F_1)^\rho (G - G_1)^\rho \in A$. We order the power products $\alpha, \beta, \cdots$ of the u_{ij} in such a way that $\alpha < \beta$ and $\gamma < \delta$ imply $\alpha\gamma < \beta\delta$ (say, lexiocographically). Let f, g be the first coefficients of $(F - F_1)^\rho$, $(G - G_1)^\rho$. Then $fg \in A$ but $f^\sigma, g^\sigma \notin A$, $\sigma = 0, 1, \cdots$. Case (ii) is similar, and even simpler.

86. Coming to 36 and the normal decomposition theorem, we cannot expect, in the absence of (P), a normal decomposition in the usual sense, since this involves prime ideals. With (F) alone, however, we can write any ideal A as the intersection of primaries. First, we test whether A is primary, and if not, then starting from a given basis of A, we can by a canonical algorithm find $a, b \in k[X]$ with $ab \in A$, $a \notin A$, $b^\rho \notin A$, $\rho = 0, 1, \cdots$. We can then find a $\rho > 0$ such that $A : b^\rho = A : b^{\rho+1}$, so that by a change of notation we have $ab \in A$, $a \notin A$, $b \notin A$, $A : b = A : b^2$. Then we get $A = (A, b) \cap (A : b)$; cf. 16. Moreover, $A < (A, b)$ and $A < A : b$. If (A, b) or $A : b$ is not primary, we repeat the construction. By the finitist version of Hilbert's theorem on ascending chains, this process must stop.

87. Let k satisfy (F) and let A be an r-dimensional primary ideal in $k[X_1, \cdots, X_n]$. Let $X_i' = u_{i1}X_1 + \cdots + u_{in}X_n$, $i = 1, \cdots, n$, be transformed

variables and let $t \leq r$. Then $k(u, X_1', \cdots, X_t')[X]A$ is also primary.

Proof. From 75 and 76 we already know that $k(u, X_1', \cdots, X_t')[X]A$ is unmixed, $(r - t)$-dimensional. Let $E = F^\rho$ be the ground-form of A, with F irreducible. Here

$$F = F(u_1, \cdots, u_{r+1}; X_1', \cdots, X_{r+1}') \in k[u_1, \cdots, u_{r+1}, X_1', \cdots, X_{r+1}'],.$$

where $u_i = (u_{i1}, \cdots, u_{in})$. Using the notation of 75, one can see that

$E(u_1, \cdots, u_t, w_{t+1}, \cdots, w_{r+1}; X_1', \cdots, X_t', X_{t+1}'', \cdots, X_n'')$ is in $k(u, v, X_1', \cdots, X_t')[X]A$.

Because of the automorphism $u_{ij} \to w_{ij}$,

$$F(u_1, \cdots, u_t, w_{t+1}, \cdots, w_{r+1}, X_1', \cdots, X_t', X_{t+1}'', \cdots, X_{r+1}'')$$

is irreducible, and remains irreducible as a polynomial in $X_{t+1}'', \cdots, X_{r+1}''$ over $k(u, v, X_1', \cdots, X_t')$. This is enough to show that $k(u, X_1', \cdots, X_t')[X]A$ is primary. Actually, $E(u_1, \cdots, u_t, w_{t+1}, \cdots, w_{r+1}, X_1', \cdots, X_t', X_{t+1}'', \cdots, X_n'')$ is the ground-form; to prove this, it is still necessary to check a primitivity condition. As this is a secondary issue, we may omit the details.

88. As long as we work with condition (F) alone, we do not attempt the constructions involving the associated prime of a primary, hence we do not try to duplicate 37, which places a bound on the exponent of a primary ideal A. Let, however, A be an r-dimensional primary ideal: then one can place a bound on the length of chains $A < A_1 < A_2 < \cdots$, where A_i is unmixed r-dimensional (hence primary). In fact, for $r = 0$ this follows from 7, and for $r > 0$ one makes a reduction to the case $r = 0$ by 87.

89. We abandon 38 for the moment, as before 23 (cf. 81).

90. Points 39–41 require no comment, so we come to 42, which asks (with (F) and (P)) to construct the associated prime of a given primary (a term which, from our present view, still has to be defined). First let Q be 0-dimensional. We relax the condition that Q be primary and consider any 0-dimensional ideal A in $k[X_1, \cdots, X_n]$. One can then construct a maximal (hence prime) ideal containing A. In fact, we first find an $f \in k[X_1] - 0$ such that $f \in A$. Let $f = f_1 f_2 \cdots f_s$ be the complete factorization of f. One checks easily that $(A, f_i) \neq (1)$ for at least one i; and for such an i, we may replace A by (A, f_i). Changing notation, we may assume $f \in A$ is irreducible. Taking residues mod f, we complete the proof by an induction on n.

In particular, for a 0-dimensional primary Q, one can construct a maximal ideal P containing Q.

91. Let Q be a 0-dimensional primary ideal in $k[X_1, \cdots, X_n]$ and let P_1, P_2 be maximal (hence prime) ideals containing Q. Then $P_1 = P_2 = P$ and one can find a ρ such that $P^\rho \subset Q$. If $ab \in Q$, $a \notin Q$, then for this ρ, $b^\rho \in Q$. The ideal P is called the *associated prime* of Q.

Proof. Let F^r be the ground-form of Q, where $F = F(u, X_1')$ is irreducible. We have $F \in P_1$ and $F \in P_2$. Consider first the case that F is separable (in X_1'). Then by the argument of 31 (though one does not first have to prove that P_1, P_2 are separable), one sees that $P_1 = P_2 = P$.

Now let $F(u, X_1') = G(u, X)$ and let A be the $k[X]$-ideal generated by the coefficients of G considered as a polynomial in the u_{ij}. We say that $A = P$: we postpone the proof to 92 and 93. It remains, then, to prove that some power of each coefficient of G is in Q. We order the power products $\alpha, \beta, \cdots$ of the u_{ij} in such a way that $\alpha < \beta$ and $\gamma \leq \delta$ imply $\alpha\gamma < \beta\delta$ (say, lexicographically). Since $G^r \in Q$, one sees that the first coefficient, f_1, has a power of it in Q. Then $(G - \text{first term of } G)^s \in Q$ for an s we can find. Repeating this argument for $H = G - \text{first term of } G$, we see that the second coefficient of G has a power of it in Q; etc. So we have a ρ with $P^\rho \subset Q$. Now let $ab \in Q$, $a \notin Q$. Then $Q \subset Q : a$, and since $Q : a \neq (1)$, we have $Q : a \subset P$. Hence $b \in P$ and $b^\rho \in Q$. This takes care of the case that $F = F(u, X_1')$ is separable.

If F is inseparable and is a polynomial in X'^{p^e} but not a polynomial in $X'^{p^{e+1}}$, hence a separable polynomial in X'^{p^e}, then one sees that F is also a polynomial in u^{p^e}. Thus after adjoining a finite number of p^eth roots to k to get k', F becomes the p^eth power of an irreducible separable polynomial. Write $k'[X]Q = Q'$, $k'[X]P_1 = P_1'$, $k'[X]P_2 = P_2'$. These all have a power of F^{1/p^e} as ground-form. Let P'' be the prime in $k'[X]$ having F^{1/p^e} as ground-form. Then by the part already proved, a power of P_1' is in P_2' and vice versa. Hence also (as one easily sees) in $k[X]$ a power of P_1 is in P_2 and vice versa. Hence $P_1 = P_2$. The rest of the proof of 91 is as in the separable case.

92. To complete the proof of 91 we first need a lemma.

Lemma. *Let* $f_i(X_i) \in k[X_i] - 0$ *be a polynomial prime to its derivative* $(i = 1, \cdots, n)$. *Then* $(f_1(X_1), \cdots, f_n(X_n))$ *is a finite intersection of maximal ideals*; *and so is any larger ideal* $(f_1, \cdots, f_n, \cdots) \neq (1)$.

Proof. If $f_1(X_1)$ is irreducible, then we take residues mod $f_1(X_1)$ and complete the proof by induction on n. Otherwise, let $f_1 = g_1 g_2 \cdots g_s$ be the complete factorization of f_1; g_i, g_j are not associates if $i \neq j$. Then $(g_i, f_2, \cdots, f_n, \cdots) = \bigcap_j P_{ij}$ for each i. Then $(f_1, f_2, \cdots, f_n, \cdots) = \bigcap_{i,j} P_{ij}$. In fact, the left-hand side is obviously contained in the right. Now let $a \in \bigcap_{i,j} P_{ij}$. Then $a \equiv bg_1 \bmod (f_2, \cdots, f_n, \cdots)$, so $ag_2 \cdots g_s \in (f_1, f_2, \cdots, f_n, \cdots)$. Similarly, $a(f_1/g_i) \in (f_1, f_2, \cdots, f_n, \cdots)$ for each i, whence $a \in (f_1, f_2, \cdots, f_n, \cdots)$.

93. Let P be a 0-dimensional prime ideal in $k[X_1, \cdots, X_n]$ and let $F(u_1, X_1') = G(u_1, X)$ be the ground-form of P; here $u_1 = (u_{11}, \cdots, u_{1n})$. Let A (which we call the *Chow ideal* of P) be the ideal generated (in $k[X]$) by the coefficients of G regarded as a polynomial in the u_{1j}. Then: if $F(u_1, X_1')$ is separable (in X_1'), then $A = P$.

Proof. Clearly, the coefficients of $F(u_i, X'_i)$ also generate A. Hence $(F(u_1, X'_1), \cdots, F(u_n, X'_n)) \subset A$. Hence (by 92) A is the intersection of 0-dimensional prime ideals: $A = P_1 \cap \cdots \cap P_s$; here we are in $k(u)[X]$. Moreover, A, P_1, $\cdots$, P_s and P all clearly have the same ground-form. Hence (by 91 first part) $P_1 = \cdots = P_s = P$ and $A = P$.

94. Let Q be an r-dimensional primary ideal in $k[X_1, \cdots, X_n]$, so that (by 75 and 87) $k(u, X'_1, \cdots, X'_r)[X'_{r+1}, \cdots, X'_n]Q = Q'$ is 0-dimensional and primary, and let P' be the associated prime of Q'. Then P' has a basis in $k[X]$, so that (by 76) one can construct $P' \cap k[X] = P$. Then P is the unique maximal unmixed r-dimensional (hence primary) ideal in $k[X]$ containing Q; and $Q = P$ if and only if $Q' = P'$. If $P'^{\rho} \subset Q'$, then $P^{\rho} \subset Q$; and if $ab \in Q$, $a \notin Q$, a, $b \in k[X]$, then for this ρ, $b^{\rho} \in Q$.

Proof. Let $G \in P'$. Multiplying G by an element in $k(u, X'_1, \cdots, X'_r) - 0$, we may suppose $G \in k[u, X'_1, \cdots, X'_n] \subset k[u, X_1, \cdots, X_n]$. Let us write $G = G(u, X)$: we wish to show that the coefficients of G regarded as a polynomial in the u_{ij} are in P'. We order the power-products of the u_{ij} as in 85, Proof. Since $G^{\rho} \in Q'$ and Q' has a basis in $k[X]$ one sees that a power of the first coefficient of G is in Q', hence the first coefficient is in P'. Repeating the argument for $H = G -$ first term of G, we get that the second coefficient is in P'; etc. Now we have $P' \cap k[X] = P$. If $P'^{\rho} \subset Q'$, then obviously $P^{\rho} \subset Q$. Hence P is at most r-dimensional, and since it is the contraction of its extension P', it is an r-dimensional prime ideal. If $ab \in Q$, $a \notin Q$, a, $b \in k[X]$, then $b^{\rho} \in Q'$ and hence $b^{\rho} \in Q$. The rest of 94 is immediate.

P is called the *associated prime* of Q. Thus we are through 42.

Remark. To decide whether a given ideal A is prime, first check to see whether it is primary; and if it is, then check to see whether it is its associated prime.

95. Point 43 requires no comment. As for 44, we first observe that if condition (F) holds for k, then an ideal $(F) \neq (1)$ in $k[X]$, $X = X_1$, is primary if and only if $ab \in (F)$, $a \notin (F) \Rightarrow b^{\deg F} \in (F)$. We now take this as defining *primary* in $k[X]$: this changes nothing as far as our results above, where (F) was assumed, are concerned, but allows us to proceed a bit with primary ideals also over an arbitrary explicitly given field. Thus for an arbitrary explicitly given field k, $X^p - a$ is always primary: for if $fg \in (X^p - a)$ and $g^p \notin (X^p - a)$, then $g^p \equiv c(X^p - a)$, $c \in k - 0$, and $f \in (X^p - a)$.

Now let $A = (X_1^p - a_1, \cdots, X_n^p - a_n)$ be an ideal in $k[X_1, \cdots, X_n]$, $p = \operatorname{ch} k$. Then $A \cap k[X_1, \cdots, X_{n-1}] = (X_1^p - a_1, \cdots, X_{n-1}^p - a_{n-1})$. In fact, if

$$f(X_1, \cdots, X_{n-1}) = g_1(X_1, \cdots, X_n)(X_1^p - a_1) + \cdots + g_{n-1}(X_1, \cdots, X_n)(X_{n-1}^p - a_{n-1})$$
$$+ g_n(X_1, \cdots, X_n)(X_n^p - a_n),$$

we may first suppose $\deg_{X_n} g_i < p$ for $i = 1, \cdots, n-1$; in which case $g_n = 0$. Then placing $X_n = 0$, we get the desired result.

Now we say that $X_1'^p - u_{11}^p a_1 - \cdots - u_{1n}^p a_n$, which is obviously in A, is the ground-form of A. For A obviously equals $(X_1'^p - u_{11}^p a_1 - \cdots - u_{1n}^p a_n, \cdots, X_n'^p - u_{n1}^p a_1 - \cdots - u_{nn}^p a_n)$, whence the assertion follows from the last paragraph. Hence A is primary.

As before, we omit the proof that A is prime if and only if $a_1, \cdots, a_n$ are p-independent.

Remark. We will not attempt a discussion of 45, as our considerations for the associated primes of primaries are too tied up with (F) and (P). We also do not attempt the necessity in 46, though we still want to prove that the associated primes in an irredundant decomposition of an ideal A into primaries are uniquely determined.

96. Let A be a given ideal in $k[X_1, \cdots, X_n]$ and let k satisfy (F) and (P). Then one can write A as an intersection of primaries with distinct primes: $A = Q_1 \cap \cdots \cap Q_s$; let $P_1, \cdots, P_s$ be the associated primes. If $A = Q_1' \cap \cdots \cap Q_t'$ is another such decomposition, with $P_1', \cdots, P_t'$ as associated primes, then $\{P_1, \cdots, P_s\} = \{P_1', \cdots, P_t'\}$. Moreover, $\dim A = \max\{\dim P_i\}$ and depth $A = \min\{\dim P_i\}$; and $\dim P_i =$ degree of transcendency of $k[X]/P_i$ over k.

The proof of this now proceeds along familiar lines.

Once we have the equivalence of our definitions of primary, dimension, and depth with the classical definitions and have the normal decomposition theorem of 96, we may safely claim to have the whole theory of polynomial ideals over a field k in strictly finite terms.

Added in proof. In a recent work, *Constructive aspects of Noetherian rings*, Proc. Amer. Math. Soc. 44 (1974), 436–441, F. Richman has solved some basic construction problems for a wide class of rings, including the rings $Z[X_1, \cdots, X_n]$, where $Z =$ ring of integers.

REFERENCES

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

2. W. Krull, *Parameterspezialisierung in Polynomringen*, Arch. Math. 1 (1948), 56–64. MR 10, 178.

3. ———, *Parameterspezialisierung in Polynomringen*. II. *Das Grundpolynom*, Arch. Math. 1 (1948), 129–137. MR 11, 310.

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

5. ———, *Construction of the integral closure of a finite integral domain*, Rend. Sem. Mat. Fis. Milano 40 (1970), 100–120. (Italian) MR 45 #3396.

6. ———, *On the impossibility of some constructions in polynomial rings*, Atti del Convegno Intemazionale di Geometria, Accademia Nazionale dei Lincei, 1973, pp. 77–85.

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

8. ———, *Constructive proof of Hilbert's theorem on ascending chains*, Trans. Amer. Math. Soc. 174 (1972), 305–312.

9. G. Stolzenberg, *Constructive normalization of an algebraic variety*, Bull. Amer. Math. Soc. 74 (1968), 595–599. MR 37 #201.

10. B. L. van der Waerden, *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*, Math. Ann. 102 (1930), 738–739.

11. ———, *Moderne algebra*. Vol. I, 2nd rev. ed., Springer, Berlin, 1937; English transl., Ungar, New York, 1949. MR 10, 587.

12. ———, *Moderne algebra*. Vol. II, Springer, Berlin, 1931; English transl., Ungar, New York, 1950.

13. O. Zariski and P. Samuel, *Commutative algebra*. Vol. I, University Series in Higher Math., Van Nostrand, Princeton, N. J., 1960. MR 22 #11006.

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