SOME BASIC THEOREMS IN DIFFERENTIAL ALGEBRA (CHARACTERISTIC p, ARBITRARY)

BY

A. SEIDENBERG

J. F. Ritt [6] has established for differential algebra of characteristic 0 a number of theorems very familiar in the abstract theory, among which are the theorems of the primitive element, the chain theorem, and the Hilbert Nullstellensatz. Below we also consider these theorems for characteristic $p \neq 0$, and while the case of characteristic 0 must be a guide, the definitions cannot be taken over verbatim. This usually requires that the two cases be discussed separately, and this has been done below. The subject is treated *ab initio*, and one may consider that the proofs in the case of characteristic 0 are being offered for their simplicity. In the field theory, questions of separability are also considered, and the theorem of S. MacLane on separating transcendency bases [4] is established in the differential situation.

1. Definitions. By a *differentiation* over a ring R is meant a mapping $u \to u'$ from R into itself satisfying the rules $(uv)' = uv' + u'v$ and $(u+v)' = u' + v'$. A *differential ring* is the composite notion of a ring R and a differentiation over R: if the ring R becomes converted into a differential ring by means of a differentiation D, the differential ring will also be designated simply by R, since it will always be clear which differentiation is intended. If R is a differential ring and R is an integral domain or field, we speak of a *differential integral domain* or *differential field* respectively. An ideal A in a differential ring R is called a *differential ideal* if $u \in A$ implies $u' \in A$. The ring $\{u+A\}$ of residue classes of the differential ring R mod a differential ideal A is also a differential ring under the differentiation $(u+A)' = u' + A$.

If F is a differential field, then from $(v \cdot u/v)' = v(u/v)' + v'(u/v)$ we obtain $(u/v)' = (u'v - uv')/v^2$. If R is a differential integral domain, then its quotient field F becomes a differential field on setting $(u/v)' = (u'v - uv')/v^2$: it is this differential field which is intended when we speak of the quotient field of R. From $1' = (1 \cdot 1)' = 1 \cdot 1' + 1' \cdot 1$, it follows that $1' = 0$, whence the differentiation in F coincides with the given differentiation in R.

An element u whose derivative u' is zero will be called a *constant*. It is immediate that all the elements of the primitive field of a differential field are constants.

The modifier "differential" will usually be omitted: if "differential" is *not* intended, we shall refer to the modified object "in the algebraic sense."

Notation. The symbols ( ) and [ ] will be used in their usual senses of field and ring adjunction respectively: the symbols $\langle\ \rangle$ and $\{\ \}$ will be

Presented to the Society, May 3, 1952; received by the editors December 14, 1951.

used in the corresponding differential situations. The symbol ( ) is also used in its usual ideal-theoretic sense, the symbol [ ] taking its place in the differential case: thus, for example, $[p, q]=(p, q, p', q', p'', q'', \cdots)$. The symbol $\{\cdots\}$ is also used in the set-theoretic sense, to indicate the set exhibited, and will also be used to indicate the perfect ideal (definition below) generated by the elements enclosed. Subscripts are used in the usual way, but are also used to indicate derivatives: thus $u, u_1, u_2, \cdots$ may indicate the successive derivatives of u; but also $u_1, u_2, \cdots, u_n$ may indicate several quantities not particularly related, in which case a second subscript is used to indicate the derivative.

2. **Field extensions.** Let K be a differential field and F a subfield of K; i.e., F is understood to be a differential field under a differentiation induced in it by the given differentiation in K. Let $F\{u\}$ designate the smallest differential ring containing F and an element $u\in K$; $F\langle u\rangle$ designates the smallest differential field containing F and u.

Let now K be of characteristic 0. We shall say that the element $u\in K$ is *algebraic over F* if there is a nontrivial polynomial relation $H(u, u', u'', \cdots, u^{(i)})=0$ satisfied by u and its first i derivatives (for some i); that is, if $U, U_1, U_2, \cdots$ is a sequence of indeterminates (in the usual algebraic sense), there should be an element $H(U, U_1, \cdots, U_i)\in F[U, U_1, \cdots]$, $H(U, U_1, \cdots, U_i)\neq 0$, such that $H(u, u', u'', \cdots, u^{(i)})=0$.

In van der Waerden's *Moderne Algebra* [7], the theory of linear as well as algebraic dependence is made to rest on the following axioms:

I. *u_i is dependent on $u_1, \cdots, u_n$.*

II. *If u is dependent on $u_1, \cdots, u_n$, but not on $u_1, \cdots, u_{n-1}$, then u_n is dependent on $u_1, \cdots, u_{n-1}, u$.*

III. *If w is dependent on $v_1, \cdots, v_m$ and each v_j is dependent on $u_1, \cdots, u_n$, then w is dependent on $u_1, \cdots, u_n$.*

If, now, *y dependent on $x_1, \cdots, x_n$* is taken to mean that y is algebraic over $F\langle x_1, \cdots, x_n\rangle$, then the above axioms become true theorems. The first two are trivial, and the third follows at once from the following lemma.

LEMMA. *If u is algebraic over F, then $F\langle u\rangle=F(u, u', u'', \cdots)$ has a finite degree of transcendency over F; in fact $F(u, u', \cdots)$ is even finite over F. On the other hand, if u is not algebraic over F, then $F\langle u\rangle$ has infinite degree of transcendency over F.*

Proof. Let u be algebraic over F; then there is an $r>0$ such that $u=u^{(0)}$, $u^{(1)}, u^{(2)}, \cdots, u^{(r)}$ are algebraically dependent (in the algebraic sense) over F, while $u, u^{(1)}, \cdots, u^{(r-1)}$ are not. Let $G(U, U^{(1)}, \cdots, U^{(r)})$ be a polynomial of least degree in $U^{(r)}$ which is satisfied by $u, u^{(1)}, \cdots, u^{(r)}$ over F. Let $S(U, \cdots, U^{(r)})=\partial G/\partial U^{(r)}$: we see that $S(u, \cdots, u^{(r)})\neq 0$. Now S is the coefficient of $U^{(r+1)}$ in $(G(U, U^{(1)}, \cdots, U^{(r)}))'$, whence we see that $u^{(r+1)}\in F(u, u^{(1)}, \cdots, u^{(r)})$, and likewise $u^{(j)}\in F(u, \cdots, u^{(r)})$ for $j>r+1$:

this proves the first point. The second point is trivial.

Statement III is now immediate; for $F\langle u, v, w\rangle$ has a finite degree of transcendency over $F\langle u, v\rangle$, $F\langle u, v\rangle$ has a finite degree of transcendency over $F\langle u\rangle$, whence $F\langle u, v, w\rangle$ and $F\langle u, w\rangle$ have finite degrees of transcendency over $F\langle u\rangle$.

The whole theory of degree of transcendency in the algebraic case can therefore be carried over to the differential case, and we can speak of the *degree of differential transcendency* (d.d.t.). In particular note that if u and v are algebraic over F, then so are $u \pm v$, $u \cdot v$, and u/v (if $v \neq 0$).

The above results are, of course, well known, and go back to H. W. Raudenbush [5].

For any n it is clear that we can construct a differential ring $F\{U_1, \cdots, U_n\}$ with d.d.t $F\langle U\rangle/F = n$: then $U_1, \cdots, U_n$ will be called *differential indeterminates*, as in the algebraic case.

3. **The theorem of the primitive element.** This theorem is entirely parallel to the algebraic theorem. It asserts that if u, v are algebraic over F, then under certain conditions $F\langle u, v\rangle = F\langle\theta\rangle$. The proofs in the algebraic case depend on the fact that if $G(X_1, \cdots, X_n)$ is a polynomial different from 0 and F is an infinite field, then there exist $x_i \in F$, $i = 1, \cdots, n$, such that $G(x_1, \cdots, x_n) \neq 0$. If we consider the differential polynomial X', then it becomes clear that a like fact could obtain over a differential field F only if F contains nonconstant elements. Conversely, if F does contain nonconstants, and $G(X_1, \cdots, X_n) \neq 0$ is a differential polynomial, then there exist $x_i \in F$, $i = 1, \cdots, n$, such that $G(x_1, \cdots, x_n) \neq 0$: we refer to Ritt [6, p. 35] for the proof. Moreover, the theorem of the primitive element could not hold, in general, if all elements of F were constants: for let u, v be two indeterminates in the algebraic sense and convert $F(u, v)$ into a differential field by setting every derivative equal to 0. Then $F\langle u, v\rangle = F(u, v)$, $F\langle\theta\rangle = F(\theta)$, and $F(u, v) = F(\theta)$ is clearly impossible. Subject to these necessary conditions, the theorem holds.

THEOREM 1. *Let F contain nonconstant elements. If u, v are algebraic over F, then there exists a $\lambda \in F$ such that $F\langle u, v\rangle = F\langle u + \lambda v\rangle$. (Note that F is for the present of characteristic* 0.)

Proof. Construct $F\langle u, v\rangle\langle\Lambda\rangle$, where Λ is a differential indeterminate. Since u, v, Λ are algebraic over $F\langle\Lambda\rangle$, we have that $u + \Lambda v$ is algebraic over $F\langle\Lambda\rangle$, and hence we have a nontrivial polynomial relation:

$$G(\Lambda, \Lambda^{(1)}, \cdots, \Lambda^{(t)}, (u + \Lambda v), (u + \Lambda v)^{(1)}, \cdots, (u + \Lambda v)^{(s)}) = 0.$$

Here we are supposing that s is as small as possible and that G is of least possible degree in $(u + \Lambda v)^{(s)}$. Let $u + \Lambda v = w$: note that $\partial w^{(i)}/\partial \Lambda^{(s)} = 0$ if $i < s$, and $= v$ if $i = s$. Taking the partial of the above relation with respect to $\Lambda^{(s)}$ we obtain:

$$\frac{\partial G}{\partial \Lambda^{(s)}} + \frac{\partial G}{\partial w^{(s)}} \cdot v = 0.$$

Because of the minimal conditions placed on G, we have $\partial G/\partial w^{(s)} = S(\Lambda, u+\Lambda v) \neq 0$, whence $v \in F\langle\Lambda\rangle\langle u+\Lambda v\rangle$: we now specialize, appropriately, $\Lambda \to \lambda \in F$; some care has to be exercised, as we cannot suppose (as in the algebraic theorem) that v can be written with a denominator free of w. By the lemma of Ritt mentioned we could specialize Λ to $\lambda \in F\langle u, v\rangle$ so that $S(\lambda, u+\lambda v) \neq 0$: actually, the proof of the lemma shows that if ξ is a nonconstant, then one can specialize Λ to a polynomial in ξ with rational numbers as coefficients (the main point of this proof will have to be considered explicitly below in discussing the case of characteristic $p \neq 0$). Thus we may take $\lambda \in F$, whence $v \in F\langle u+\lambda v\rangle$ and $F\langle u+\lambda v\rangle = F\langle u, v\rangle$. (Or one can apply the lemma directly by writing $1/S(\Lambda, u+\Lambda v)$ in the form $C(\Lambda, u, v)/D(\Lambda, u, v)$, where C, D are polynomials and in D occur only u_i and v_j in some selected transcendency basis of $F\langle u, v\rangle/F$: one would then have only to specialize Λ so that some one coefficient of D does not vanish.)

For a previous treatment of the above theorem, see E. R. Kolchin [2].

4. **The Hilbert Nullstellensatz.** Let $R = F\{U_1, \cdots, U_n\}$ be a polynomial ring in n differential indeterminates. By a *point* one means a system $u_1, \cdots, u_n$ of differential quantities in an extension field of F; by a *zero* of an ideal A one means a point annihilating all the elements of A. By the variety $V(A)$ of an ideal A one means the set of zeros of A. The Hilbert Nullstellensatz says that if $G \in R$ vanishes over $V(A)$, then $G^\rho \in A$ for some ρ. Another possible definition of $V(A)$ restricts $V(A)$ to consist of the 0-dimensional points, i.e., points $(u_1, \cdots, u_n)$ such that d.d.t. $F\langle u_1, \cdots, u_n\rangle/F = 0$. According as one takes the first or second definition one speaks of the weak or strong form of the theorem: initially we are concerned only with the weak form. Another remark must be made: exception can be taken to the above definition of $V(A)$ since no bound has been placed on the cardinal number of $V(A)$. This quite valid objection is easily overcome as it is sufficient to have a field $K \supseteq F$ which contains for every prime P in R the coördinates of a *general point* of P, i.e., a point $u_1, \cdots, u_n$, $u_i \in K$, such that $R/P \cong F\{u_1, \cdots, u_n\}$, and one will then define *point* to have coördinates in K. It would be easy to construct K, but we need not be detained over this matter, since Hilbert's Theorem has an obviously equivalent form stated directly in terms of R, namely, that the set $\{G \mid G^\rho \in A\} = \cap P$ over the prime ideals P in R which contain A.

By a perfect ideal A one means an ideal such that $G^\rho \in A$ implies $G \in A$. One consequence of Hilbert's Theorem is that if A is an ideal, then the *set* $\{G \mid G^\rho \in A\}$ *is an ideal.* Hence it is clear that Hilbert's Theorem cannot hold without some modification if F is of characteristic $p \neq 0$, since, e.g., for $n = 1$, we have $u'^\rho \notin [u^p] = A$, i.e., $\{G \mid G^\rho \in [u^p]\}$ is not an ideal. This possibility

does not arise in the case of ordinary polynomial rings, and in fact it is well known that $\{G \mid G^\rho \in A\}$ is an ideal if A is; neither does it arise in the differential case if the characteristic is 0, since one shows by a simple calculation, which depends upon the characteristic, however, that $(G')^{2\rho-1} \in [G^\rho]$. We may thus say that Hilbert's Theorem consists of two parts, the first says that $\{G \mid G^\rho \in A\}$ is an ideal, in which case it is obviously perfect, and the second says that a perfect ideal is the intersection of prime ideals. This second part is true in general, and deserves the name of Hilbert.

HILBERT'S NULLSTELLENSATZ (WEAK FORM). *A perfect ideal in the polynomial ring* $F\{U_1, \cdots, U_n\}$ *is the intersection of prime ideals* (*F of arbitrary characteristic*).

Proof. Let A be the given perfect ideal, and let $\alpha \in R$, $\alpha \notin A$. We have to show the existence of a prime ideal P containing A but not containing α. Let then S be the set of perfect ideals containing A but not meeting the multiplicatively closed system $\{\alpha^\rho \mid \rho = 1, 2, \cdots\}$. Partially ordering S by inclusion, we see by Zorn's Lemma that there is maximal element P in S, and this we claim is prime. In fact, let $u, v \in R$, $u \notin P$, $v \notin P$, but $uv \in P$. Let $\{P, u\}$, $\{P, v\}$ be the smallest perfect ideals containing $[P, u]$, $[P, v]$ respectively. Some power of α lies in $\{P, u\}$, and some power in $\{P, v\}$, by the maximality of P. In the case of characteristic 0, by the remark that $\{B\} = \{G \mid G^\rho \in [B]\}$, one would even have that a power of α is in $[P, u]$, and a power in $[P, v]$. Now $uv \in P$ implies $(u'v + uv')u'v \in P$, whence $(u'v)^2 \in P$, $u'v \in P$, and more generally $u^{(i)}v^{(j)} \in P$. Hence $[P, u] \cdot [P, v] \subseteq P$, so a power of α is in P, contradiction. In the case of arbitrary characteristic it remains to prove the following lemma. Kolchin [3, §3] has this result, but it is well, for later purposes, to have a proof before our eyes.

LEMMA. *If* uv *is in the perfect ideal* P, *then* $\{P, u\} \cdot \{P, v\} \subseteq P$.

Proof. Let $A_0 = [P, u]$, let $A_1 =$ the differential ideal *generated by* the elements G such that $G^\rho \in A_0$ for some ρ, and let A_i be defined recursively as the ideal generated by the G such that $G^\rho \in A_{i-1}$ for some ρ; define $B_0 = [P, v]$, $B_1, B_2, \cdots$ similarly. We have $A_0 \subseteq \{P, u\}$, whence also $A_1 \subseteq \{P, u\}$, and now inductively that $A_i \subseteq \{P, u\}$. Hence $\cup A_i \subseteq \{P, u\}$. Conversely, let $G^\rho \in \cup A_i$; then $G^\rho \in A_i$, for some i, so $G \in A_{i+1}$, whence $G \in \cup A_i$, i.e., $\cup A_i$ is a perfect ideal, so $\{P, u\} \subseteq \cup A_i$. Hence $\{P, u\} = \cup A_i$ and similarly $\{P, v\} = \cup B_i$. We have seen already that $A_0 \cdot B_0 \subseteq P$; the proof will be complete upon showing that $A_i \cdot B_i \subseteq P$. We use induction. The ideal A_i is generated by G's such that $G^\rho \in A_{i-1}$; let G be such a generator with $G^\rho \in A_{i-1}$, and let H similarly be a generator of B_i, say $H^\sigma \in B_{i-1}$. Then $(GH)^{\rho\sigma} \in A_{i-1}B_{i-1} \subseteq P$, so $GH \in P$, and also $G^{(i)}H^{(j)}$ by a previous calculation. Hence $A_i \cdot B_i \subseteq P$, and the proof is complete.

The following theorem, taken in conjunction with the above, amounts to

the strong Nullstellensatz. Since dimension has so far been considered only for characteristic 0, the theorem is at this point necessarily subject to that restriction.

HILBERT'S NULLSTELLENSATZ (STRONG FORM). *Let P be an r-dimensional prime ideal in $R=F\{U_1, \cdots, U_n\}$, $r>0$; i.e., d.d.t. $F\langle u_1, \cdots, u_n\rangle/F=r$, where $F\{u_1, \cdots, u_n\}=R/P$. Let $\alpha\in R$, $\alpha\notin P$. Then there exists an $(r-1)$-dimensional prime ideal Q, $P\subset Q$, such that $\alpha\notin Q$.*

Below, in §8, we offer a very brief proof of this theorem. The following proof introduces two points not strictly necessary for a proof. One is the following lemma. In the case $n=1$, if P is a proper prime ideal, then $R/P=F\{u\}$, and $F\langle u\rangle=F(u, u_1, \cdots, u_r)$ is a field of algebraic functions of r variables, $u, u_1, \cdots, u_{r-1}$ algebraically independent over F. The lemma is the converse.

LEMMA. *Let $F(u, u_1, \cdots, u_r)$ be a field of algebraic functions of r variables, with u_r algebraic and separable over $F(u, u_1, \cdots, u_{r-1})$; F, a differential field. Then there is one and only one way to convert $F(u, \cdots, u_r)$ into a differential field so that $u'=u_1$, $u_1'=u_2, \cdots, u_{r-1}'=u_r$.*

This is a well known result; see for example [8, chap. I, Prop. 15, p. 12].

Proof of the theorem. We may suppose that $u_1, \cdots, u_r$ are algebraically independent over F. Since $r>0$, $F\langle u_1, \cdots, u_r\rangle$ contains nonconstant elements, so there exists a w such that $F\langle u_1, \cdots, u_r, w\rangle=F\langle u_1, \cdots, u_n\rangle$. The element w satisfies an equation $G(U_1, \cdots, U_r; W, W_1, \cdots, W_{t+1})=0$, where t is as small as possible and G is irreducible in $F\{U_1, \cdots, U_r\}[W, \cdots, W_{t+1}]$. Note that if $H(U; W)$ is in this last ring and $H(u; w)=0$, then H is divisible by G in that ring. Let $S=\partial G/\partial W_{t+1}$. We have $u_{r+i}=f_i(u_1, \cdots, u_r; w)/d(u_1, \cdots, u_r; w, \cdots, w_t)$, where $f_i, d\in F\{U_1, \cdots, U_r; W\}$. Let $1/S(u; w)=g(u_1, \cdots, u_r; w, \cdots, w_{t+1})/e(u_1, \cdots, u_r; w, \cdots, w_t)$ and let $1/\alpha(u_1, \cdots, u_n)=h(u_1, \cdots, u_r; w)/e_1(u_1, \cdots, u_r; w, \cdots, w_t)$, where $g, h, e, e_1\in F\{U_1, \cdots, U_r; W\}$, and, moreover, we may write $d=e=e_1$; note that $Sg-e$ is divisible by G. We now define a differential field by binding $U_1, \cdots, U_r$, but in such manner that not all the coefficients of $d(U_1, \cdots, U_r; W)$, regarded as a polynomial in $W, \cdots, W_t$, become equal to zero, i.e., we have a field $F\langle \bar{u}_1, \cdots, \bar{u}_r\rangle$, of d.d.t. $r-1$ over F, and such that $d(\bar{u}_1, \cdots, \bar{u}_r; W)\neq 0$; moreover, we can also require, and do, that $G(\bar{u}_1, \cdots, \bar{u}_r; W, \cdots, W_{t+1})$ be of positive degree in W_{t+1}. Then $G(\bar{u}_1, \cdots, \bar{u}_r; W, \cdots, W_{t+1})$ will have an irreducible factor over $F\langle \bar{u}_1, \cdots, \bar{u}_r\rangle$ of positive degree in W_{t+1}, and through it we define, in the canonical manner, a differential field $F\langle \bar{u}_1, \cdots, \bar{u}_r; \bar{w}\rangle$; it will then be so that $\bar{d}=d(\bar{u}_1, \cdots, \bar{u}_r; \bar{w})\neq 0$ and $\bar{S}=S(\bar{u}_1, \cdots, \bar{u}_r; \bar{w})\neq 0$. Define $\bar{u}_{r+i}=f_i(\bar{u}, \bar{w})/d(\bar{u}, \bar{w})$. We now prove that $H(u_1, \cdots, u_n; w)=0$ implies $H(\bar{u}_1, \cdots, \bar{u}_n; \bar{w})=0$; in particular it will therefore be true that

$\alpha(\bar{u}_1, \cdots, \bar{u}_n) \neq 0$. Let $(d(U, W))^{\rho} H(U_1, \cdots, U_n; W) \to H_1(U_1, \cdots, U_r; W)$ under the substitution $U_{r+i} \to f_i(U_1, \cdots, U_r; W)/d$, where ρ is chosen sufficiently high that H_1 be a polynomial. Further, let $(S(U, W))^{\sigma} H_1 \equiv H_2(U_1, \cdots, U_r; W, \cdots, W_{t+1}) \bmod [G]$. It is sufficient to prove $H_2(\bar{u}_1, \cdots, \bar{u}_r; \bar{w}) = 0$, and we have $H_2(u_1, \cdots, u_r; w) = 0$. But $H_2(u; w) = 0$ implies $H_2(U, W) = A(U, W) \cdot G(U, W)$, whence $H_2(\bar{u}, \bar{w}) = A(\bar{u}, \bar{w}) \cdot G(\bar{u}, \bar{w}) = 0$. If $\bar{u}_1, \cdots, \bar{u}_n$ determine Q in $F\{U_1, \cdots, U_n\}$, then Q is a prime ideal of the type sought. Q.E.D.

While Ritt has not explicitly stated, in [6] at any rate, the strong form of Hilbert's Theorem, he does have, in a special case, a theorem much stronger than the weak form. In the case in question, F is the field of functions *meromorphic* throughout a given open set A of the complex plane. A *point* is then defined as the composite notion of an open set B, $B \subseteq A$, and a system of functions $u_1(x), \cdots, u_n(x)$, $u_i(x)$ *analytic* in B. Hilbert's Theorem continues to hold. Applying the strong form of the theorem, one could prove this theorem using a minimum amount of analysis.

5. **The chain theorem.** Let F be a differential field, $U_1, \cdots, U_n$ differential indeterminates. The ascending chain condition does not hold in $S = F\{U_1, \cdots, U_n\}$ for ideals in general, but it does hold for the perfect ideals. We give a new proof, first establishing the following (*for ground-fields of characteristic* 0).

THEOREM 2. (A) *The ascending chain condition holds for prime ideals.*

(B) *Every perfect ideal is a finite intersection of primes.*

We may remark that (A) can be proved very simply using the theory of transcendency, both differential and ordinary. We shall want Theorem 2 in a slightly more general situation, however, as in the following lemma.

LEMMA. *Let R be an integral domain (in the algebraic sense, and of arbitrary characteristic). If the conditions* (A) *and* (B) *hold in R, then they also hold in $R[U]$, where U is a single algebraic indeterminate. If R is a differential domain containing the rational numbers, then the like is true of R and $R\{U\}$, where U is a differential indeterminate.*

Proof. Let $A = \bigcap P_\alpha$ be a perfect ideal in $S = R[U]$. The ideal $A' = R \bigcap A$ contains some prime ideals, for example, (0): let P' be a maximal prime ideal in R contained in A'. Since the ascending chain condition holds for prime ideals in R, we may assume, inductively, that any perfect S-ideal whose contraction to R contains a prime ideal properly containing P' is a finite intersection. Now A' is clearly perfect, so by induction $A' = P_1' \bigcap \cdots \bigcap P_k'$. If $A' \neq P'$, then each $P_i' \supset P'$ properly. Let $A_i = \bigcap P_\alpha$ over those P_α containing P_i'; then each A_i is a finite intersection, whence $A = A_1 \bigcap \cdots \bigcap A_k$ is also. Thus we may assume $A' = P'$. We now consider polynomials $G(U) = \sum c_i U^i \in A$. Let $\bar{G}(U) = \sum \bar{c}_i U^i$, where the $\bar{c}_i$ are the residues of the c_i mod P'. If all

$\overline{G}(U)=0$, one sees easily that A is prime, and is the extension of P' to S. We may suppose, then, that there are $G(U)\in A$ such that $\overline{G}(U)\neq 0$, and of these we choose one, $G(U)$, to be of minimal degree d. For each perfect S-ideal A contracting to P' we have then defined an integer $d=d(A)$, and may assume inductively that any perfect S-ideal contracting to P' and having a degree less than d is a finite intersection. Factor $\overline{G}(U)$ in $\Sigma[U]$, where $\Sigma=$ quotient-field of R/P': $\overline{AG}=\overline{G}_1\cdots\overline{G}_s$, where $\overline{G}_i(U)$ is irreducible in $\Sigma[U]$, and $\overline{A}\in R/P'$ has been so selected that $\overline{G}_i$ has coefficients in R/P'. Let $A_i=\bigcap P_\alpha$ over those P_α containing $G_i(U)$: if $s>1$, then either A_i contracts in R to something containing P' properly or the degree of A_i is less than d; in either case A_i is a finite intersection, and hence so is $A=A_1\cap\cdots\cap A_s$. Thus we may assume that $s=1$, or that $\overline{G}$ is irreducible. Let I be the leading coefficient of G: $I\notin P'$ by the minimal condition placed on G. Let $A_1=\bigcap P_\alpha$ over those P_α containing I, $A_2=\bigcap P_\alpha$ over those P_α not containing I. The ideal A_1 is a finite intersection, so we may suppose $A=A_2$, i.e., that $I\notin P_\alpha$ for *every* α. Hence in particular $I^\rho H\in A$ implies $H\in A$. Under these circumstances, however, A is even prime. In fact, let $H_1(U)H_2(U)\in A$. Reduce the degrees of H_1, H_2: $I^\rho H_1\equiv H_1'(U)$ (G), $I^\sigma H_2\equiv H_2'(U)$ (G), where deg $H_i'(U)<d$, $i=1, 2$. We have $H_1'H_2'\in A$, and from $H_i'\in A$ follows $H_i\in A$. Let $I^\tau H_1'H_2'\equiv R(U)$ (G), where deg $R(U)<d$. Then $\overline{I}^\tau\overline{H}_1'\overline{H}_2'$ is divisible by $\overline{G}$ in $\Sigma[U]$, and this implies $\overline{H}_1'=0$ or $\overline{H}_2'=0$, whence $H_1'\in A$ or $H_2'\in A$. Thus A is prime, and the proof that a perfect ideal is a finite intersection is complete. The proof that the ascending chain condition holds for prime ideals in S follows in quite the same way: in fact, one shows easily that if $S\cdot P'\subset Q_1\subseteq Q_2$, where Q_1, Q_2 are prime ideals contracting to P' and $Q_1\supset S\cdot P'$ properly, then $Q_1=Q_2$.

The proof of the second point is almost the same, and could easily be carried through without the introduction of any further general remark. The following corollary, which will be useful below, may, however, also be used here. Let M be a set of prime ideals in a ring R and define an M-perfect ideal as an intersection of M-prime ideals.

COROLLARY. *If conditions* (A) *and* (B) *hold for the M-prime and M-perfect ideals in an (algebraic) ring R, and $(0)\in M$, then they also hold for any set N of prime ideals in $R[U]$ and their N-perfect ideals, provided that the contraction of an N-prime ideal is an M-prime ideal and that an N-perfect ideal which is prime is an N-prime ideal.*

To apply the corollary to R and $S=R\{U\}$, introduce the rings $S_i=R[U, U_1, \cdots, U_i]$, and let the M_i-prime ideals be those *prime* ideals which are contractions of *prime or perfect* differential ideals in $R\{U\}$; in R, the M-prime ideals are the differential prime ideals. Then one sees that conditions (A) and (B) hold in S_i for the M_i-ideals. Let now $A=\bigcap P_\alpha$ be a perfect ideal in $R\{U\}$: as before we suppose that $A\cap R=P'$ is prime, that the theorem holds for any perfect ideal whose contraction to R contains P'

properly, and that $A \neq R\{U\} \cdot P'$. Let $G(U, U_1, \cdots) \in A$, with coefficients not all in P', and of minimal total degree in $U, U_1, \cdots$; we may, and shall, also suppose that *none* of the coefficients of G is in P'. Let $G = G(U, \cdots, U_r)$ effectively involve U_r, but not U_s, $s > r$, say deg G in U_r is d. The leading coefficient of G, i.e., the coefficient of U_r^d, is not in $R\{U\} \cdot P'$, hence also the leading coefficient of $S = \partial G / \partial U_r$ is not in $R\{U\} \cdot P'$. Hence S is not in A, being of too small degree. Thus S is not in every P_α, and separating off those P_α containing S, we may suppose $S \notin P_\alpha$, every α: in particular, then, $S^\rho H \in A$ implies $H \in A$. We can now further suppose that $A \cap R[U, \cdots, U_r] = P_r'$ is prime. Under these circumstances, A is prime. In fact, let $H_1 H_2 \in A$. Noting that S is the coefficient of U_{r+i} in $G^{(i)}$, we see that for some ρ, σ, $S^\rho H_1 \equiv H_1'$ (A), $S^\sigma H_2 \equiv H_2'$ (A), where $H_1', H_2' \in R[U, \cdots, U_r]$. Since $H_1' H_2' \in A$, also $H_1' H_2' \in P_r'$, H_1' or H_2' is in P_r', hence in A, and H_1 or H_2 is in A. This completes the proof for (A), and (B) follows similarly.

The chain theorem follows readily from (A) and (B), without reference to any special differential concept. For let $A_1 \subseteq A_2 \subseteq \cdots$ be a chain of perfect ideals, and let each A_i be written as an irredundant intersection of a finite number of prime ideals. Let $P_1 \subseteq P_2 \subseteq \cdots$ be a chain of prime ideals, where P_i occurs in A_i. Each such chain involves only a finite number, say n, of prime ideals. Then n must be bounded. For if not, then there is some prime P_1 of A_1 which initiates, for any n, chains of length $\geqq n$. Take chains of length $n \geqq 1, 2, \cdots$ and beginning with P_1. In all these we may have $P_1 = P_2 = \cdots = P_i$, but there is some i such that $P_i \subset P_{i+1}$ for some, and hence every, such chain (because A_{i+1} has been written irredundantly). There are only a finite number of possibilities for P_{i+1}, so what has been said for P_1 also goes for some P_{i+1} containing P_1 properly. In this way we get a proper ascending chain of prime ideals: impossible. So n is bounded. Let there be chains of length N, but none of length greater than N. We make an induction on N. Each P_{i+1} contains some P_i, and if $A_i \subset A_{i+1}$ properly, then either at least one P_{i+1} contains some P_i properly, or A_{i+1} has less primes than A_i: if $N = 1$, then the first possibility is excluded, and the chain $A_1 \subseteq A_2 \subseteq \cdots$ is finite. Suppose now that $P_1 = P_2 = \cdots = P_i \subset P_{i+1} \subseteq \cdots$ is a chain of length $N > 1$: call the *pair* (P_i, i) *an initiator*. If (P_i, i), (P_j, j) are initiators and $i \neq j$, say $j > i$, then also $P_i \neq P_j$, for otherwise $P_j (= P_i)$ would be a prime ideal of A_{i+1}, and that is not so. Each P_i of an initiator is a prime ideal of A_1, so there are at most a finite number of initiators. Let i be maximal over the indices of the initiators. Then the theorem follows by induction on $A_{i+1} \subseteq A_{i+2} \subseteq \cdots$.

6. **The case of characteristic $p \neq 0$.** To extend the results of §2 one must first decide what one shall mean by the element u being algebraic over a differential field. Let π be the prime field of ch. $p \neq 0$, x an indeterminate in the algebraic sense. Convert $F = \pi(x)$ into a differential field by setting each derivative equal to zero. In the polynomial ring $S = F\{U\}$, consider the ideal $P = S \cdot (U^p - x)$, generated in the algebraic sense. One sees that P is a prime

differential ideal, that the residue u of U in S/P is algebraic in the previous sense, but that u' is not algebraic in that sense. Here S/P has infinite degree of transcendence (in the algebraic sense) over F. One ought at least to require of an algebraic quantity u that $F\langle u\rangle$ be of finite degree of transcendence over F, but this is not sufficient, as axiom II would fail.

EXAMPLE. Let π be the prime field of ch. $p\neq 0$. Let $x, x_1, \cdots$ be a sequence of indeterminates in the algebraic sense, and convert $F=\pi(x, x_1, \cdots)$ into a differential field by setting every derivative equal to zero. In the ring $S=F\{V\}$, consider the ideal $P=S\cdot(V^p x_1 - V_1^p x, V_2^p x_3 - V_3^p x_2, \cdots)$ generated in the algebraic sense ($V_1=V'$, $V_2=V''$, $\cdots$). One verifies immediately that P is a prime differential ideal: in fact, if $t, t_2, t_4, \cdots$ is a sequence of indeterminates (in the algebraic sense), then $(t, t(x_1/x)^{1/p}, t_2, t_2(x_3/x_2)^{1/p}, \cdots)$ is a "general point" of P. If $v, v_1, \cdots$ are the residues of $V, V_1, \cdots$ in S/P, one sees that $F\langle v\rangle$ is not of finite degree of transcendence over F. In $T=F\langle v\rangle\{U\}$, let $Q=T\cdot(xU^p - v^p, x_2U_2^p - v_2^p, \cdots)$, generated in the algebraic sense. Here also Q is a differential prime ideal in T, and if u is the residue of U in T/Q, then $F\langle v, u\rangle$ is of infinite degree of transcendence over $F\langle v\rangle$. On the other hand, each v_i is algebraic over $F\langle u\rangle$.

We therefore propose the following definition.

DEFINITION. The element u is said to be algebraic over F if $F\langle u\rangle$ is a finite extension of F.

The results of §2 *then continue to hold.* Axiom I is trivially verified; III follows from the fact that if K, L, M are fields, $K\subseteq L\subseteq M$, and M/K is finite, then so is L/K. As for II, adjoining $u_1, \cdots, u_{n-1}$ to F, and calling the other two elements u, v, we have to see that *if v is algebraic over $F\langle u\rangle$ but not over F, then u is algebraic over $F\langle v\rangle$.* Let, then, $F\langle u, v\rangle = F\langle u\rangle(v, v_1, \cdots, v_r)$. We have $v_{r+1}=P(u, u_1, \cdots, u_t, v, \cdots, v_r)/Q(u, \cdots, u_t, v, \cdots, v_r)$, P, Q polynomials. Let us use this relation to compute $v_{r+2}, v_{r+3}, \cdots$, the denominators being always powers of Q. In computing v_{r+2}, v_{r+1} and u_{t+1} may arise in the numerator: eliminating v_{r+1} by the above relation, we have $v_{r+2}=P_1(u, \cdots, u_t, u_{t+1}, v, \cdots, v_r)/Q^p$, and the degree of P_1 in u_{t+1} is at most 1. Here P_1 may not actually involve u_{t+1}, but at any rate one sees that the order of the highest order derivative of u appearing in the numerator increases by 0 or 1 (or possibly decreases); and the like is true in passing successively to $v_{r+3}, v_{r+4}, \cdots$. Now the order of this highest derivative can not be bounded, as otherwise $F\langle v\rangle$ would be finite over F. And since this order increases by either 0 or 1, one sees that it takes on all the values $t, t+1, t+2, \cdots$. The increase from u_s to u_{s+1} gives a linear relation in u_{s+1}, and so we have that $F\langle v, u\rangle$ is a finite extension of $F\langle v\rangle$, i.e., u is algebraic over $F\langle v\rangle$.

To extend the results of §3 one might think, keeping in mind the abstract algebraic results, that the first thing is to define *separable quantity.* It turns out, however, that the theorem of the primitive element has nothing to do with questions of separability, at least subject to the definition of *algebraic*

quantity given above. In fact, if u and v are each algebraic over F, then $F\langle u, v\rangle/F$ as well as $F\langle\Lambda\rangle\langle u, v\rangle/F\langle\Lambda\rangle$ are finite. Now any subfield of a finite extension is also finite, and from any system of generators, a finite subsystem of generators can be selected. Hence $u+\Lambda v$ is algebraic over $F\langle\Lambda\rangle$ and for some r, $(u+\Lambda v)^{(r)}\in F\langle\Lambda\rangle(u+\Lambda v, (u+\Lambda v)', \cdots, (u+\Lambda v)^{(r-1)})$. As before, taking a partial with respect to $\Lambda^{(r)}$, one obtains $F\langle\Lambda\rangle\langle u+\Lambda v\rangle = F\langle\Lambda\rangle\langle u, v\rangle$.

The results of §3 would now carry over provided we have the theorem on satisfying polynomial inequalities. Here again the theorem depends on the nature of the base field, but it is not sufficient to have a nonconstant element.

EXAMPLE. Let π be the prime field of ch. 2, $\pi(\xi)$ a differential field with $\xi'=1$. Then Λ'' is a nonzero polynomial which vanishes for every $\lambda\in\pi(\xi)$.

If F is a differential field, then the constants in F form a field F_0, *the constant field*. If an element ξ in F is separable over F_0 (in the algebraic sense), then one sees immediately that $\xi\in F_0$. In the case of ch. 0, if ξ is nonconstant, then this shows that ξ is transcendental over F_0, in particular F/F_0 has no finite linear basis. This is the main condition that the theorem on satisfying polynomial inequalities hold.

THEOREM 3. *The theorem on satisfying polynomial inequalities over F holds if and only if F has no finite linear basis over its constant field F_0.*

Proof. By a lemma of Ritt [6, p. 34], the proof of which is a simple induction and in no way depends on the characteristic, elements $\eta_1, \cdots, \eta_s\in F$ are linearly dependent over F_0 if and only if

$$\begin{vmatrix} \eta_1 & \cdots & \eta_s \\ \eta_1' & \cdots & \eta_s' \\ \vdots & & \vdots \\ \eta_1^{(s-1)} & \cdots & \eta_s^{(s-1)} \end{vmatrix} = 0.$$

Let F/F_0 be finite, and let $s>[F:F_0]$. Form a polynomial $P(\Lambda)$ by replacing in the above determinant $\Lambda^{(i)}$ for η_i. Then $P(\Lambda)\neq 0$, but $P(\lambda)=0$ for every $\lambda\in F$. Conversely, *let $G(U, \cdots, U_s)\neq 0$ be a given polynomial, and let $\xi_0, \cdots, \xi_s\in F$ be linearly independent over F_0: we propose to show that $G\neq 0$ is satisfied for some $U=c_0\xi_0+\cdots+c_s\xi_s$, the $c_i\in F_0$.* In doing so, we may assume inductively that the theorem holds for any polynomial (involving only $U, \cdots, U_s$) of total degree (in $U, \cdots, U_s$) less than the total degree of G: the theorem being trivial for total degree zero, we shall suppose G to have positive degree. Suppose, then, that G were also a polynomial in $U^p, \cdots, U_s^p$. Let $w_1, w_2, \cdots$ be a (possibly infinite) linear basis of F/F^p. Then $G=G_1w_1+G_2w_2+\cdots$, where $G_i\in F^p[U^p, \cdots, U_s^p]$. Let $G_i(U)\neq 0$ and $U=c_0\xi_0+\cdots+c_s\xi_s$ such that $G_i^{1/p}(c_0\xi_0+\cdots+c_s\xi_s)\neq 0$: such an element exists by induction, and also does not annihilate G. We may suppose, then, that G is

not a polynomial in $U^p, \cdots, U_s^p$, which we can express by saying that some $\partial G/\partial U_i \neq 0$. The proof is now parallel to Ritt's, where he has written $1, \xi, \cdots, \xi^s$ instead of $\xi_0, \cdots, \xi_s$. In fact, suppose $G(c_0\xi_0 + \cdots + c_s\xi_s) = 0$ for all $(c_0, c_1, \cdots, c_s)$, $c_i \in F_0$. Let π be the prime field of F, and $\xi \in F$, $\xi \notin F_0$. Then ξ is not algebraic over π (in the algebraic sense): in fact, suppose for a moment it were, and let $f(X) = 0$ be an equation of least degree satisfied by ξ over π. Then $f(X)$ is separable, since π is perfect, so $f'(\xi) \cdot \xi' = 0$ yields $\xi' = 0$, a contradiction. Hence in particular F_0 contains infinitely many elements, all the elements of $\pi(\xi^p)$ for example. Hence taking the partials of $G(c_0\xi_0 + \cdots + c_s\xi_s) = 0$ with respect to the c_i yields true relations. Thus we get:

$$\begin{aligned}
\frac{\partial G}{\partial U}\xi_0 + \frac{\partial G}{\partial U_1}\xi_0' + \cdots + \frac{\partial G}{\partial U_s}\xi_0^{(s)} &= 0, \\
\frac{\partial G}{\partial U}\xi_1 + \frac{\partial G}{\partial U_1}\xi_1' + \cdots + \frac{\partial G}{\partial U_s}\xi_1^{(s)} &= 0, \\
&\vdots \\
\frac{\partial G}{\partial U}\xi_s + \frac{\partial G}{\partial U_1}\xi_s' + \cdots + \frac{\partial G}{\partial U_s}\xi_s^{(s)} &= 0,
\end{aligned}$$

whence, since $\partial G/\partial U_i \neq 0$ for an appropriate choice of the c_i, we get that the determinant of these equations equals zero, and hence that $\xi_0, \cdots, \xi_s$ are linearly dependent over F_0, by the lemma of Ritt already referred to above: this is a contradiction.

Hence, *the theorem of* §3 *on the primitive element also holds more generally, with a condition on the base field F, but without restriction on the characteristic.*

As for the chain theorem, we must first settle on the definition of prime ideal: the old definition is certainly not sufficient.

EXAMPLE. Let π = the prime field of ch. $p \neq 0$, $x, x_1, \cdots$ a sequence of (algebraic) indeterminates, and $F = \pi(x, x_1, \cdots)$ a differential field in which every derivative is zero. In $S = F\{U\}$, let $P_i = S \cdot (U^p - x, \cdots, U_i^p - x_i)$, generated in the algebraic sense: one sees that also P_i is differential and prime. On the other hand $P \subset P_1 \subset \cdots$ is an infinite ascending chain of prime ideals.

In this example, S/P is of infinite degree of transcendence over F. Even requiring S/P to be finite is not sufficient, however. The chain theorem for *prime ideals* would, indeed, obtain, but the finite intersection property fails.

EXAMPLE. Let S be as above; let $P_i = S \cdot (U^p - x, \cdots, U_{i-1}^p - x_{i-1}, U_i, U_{i+1}, \cdots)$ $(i = 1, 2, \cdots; \omega)$ in the algebraic sense. One verifies immediately that P_i is a differential prime ideal. On the other hand, $A = \bigcap P_i$ is not a finite intersection. In fact, $A = S \cdot [U(U^p - x), U_1(U_1^p - x_1), \cdots]$, generated

in the differential sense, i.e., these generators and their various derivatives generate A in the algebraic sense. The minimal prime ideals of A are just the P_i, so A cannot be a finite intersection.

Thus it becomes fairly clear that at least in $S=F\{U\}$ it should be required of an *allowable* proper prime ideal that $F\langle u\rangle/F$, where u is the residue of U mod P, satisfy some separability condition, in addition to the requirement that it be finite. We take the following definition, which is the current one in the algebraic theory (see [1, p. 68]), and which appears to be suitable for the differential theory as well.

DEFINITION. Let $K\subseteq L$, K, L, be fields (of ch. $p\neq 0$). L/K is said to be separable if elements in L linearly independent over K are still such over $K^{1/p}$.

We define allowable prime ideal accordingly.

DEFINITION. A differential prime ideal P in $S=F\{U_1, \cdots, U_n\}$ will be said to be allowable if $F\langle u_1, \cdots, u_n\rangle/F$ is separable, where $F\{u_1, \cdots, u_n\}=S/P$.

In $S=F\{U_1, \cdots, U_n\}$, we define an *allowable perfect ideal as the intersection of allowable prime ideals*, but it is not immediately clear that an allowable perfect ideal which is prime is an allowable prime ideal. We need an ideal-theoretic or ring-theoretic criterion for an allowable ideal. Let $z_1, z_2, \cdots \in F$ be a p-basis for F/F^p, i.e., every element of F can be written uniquely as a polynomial in the z_i, with no exponent exceeding $p-1$, and with coefficients in F^p. One easily defines differentiations $\partial/\partial z_i$ over F^p such that $\partial z_i/\partial z_i=1$, $\partial z_j/\partial z_i=0$ if $j\neq i$, and $\partial U_j/\partial z_i=0$.

THEOREM 4. *Let P be a prime ideal in $S=F\{U_1, \cdots, U_n\}$. Then P is allowable if and only if $P\cap F[U_1^p, U_1'^p, \cdots, U_n^p, U_n'^p, \cdots]$ is closed under all the differentiations $\partial/\partial z_i$.*

Proof. Let $u_1, \cdots, u_n$ be the residues of $U_1, \cdots, U_n$. $F\langle u_1, \cdots, u_n\rangle/F$ is separable if and only if $F^p(u_1^p, u_1'^p, \cdots, u_n^p, u_n'^p, \cdots)/F^p$ is separable, and this will be the case if and only if $G_1w_1+G_2w_2+\cdots=0$ implies that each $G_i=0$, where $G_i\in F^p(u_1^p, \cdots)$ and $w_1, w_2, \cdots$ is a linear basis of F/F^p. We may suppose that $G_i\in F^p[u_1^p, \cdots]$, and the w_i to be the power products of the z_i with exponents not exceeding $p-1$. The differentiations $\partial/\partial z_i$ are introduced merely as a convenient device for deducing $G_i=0$ from $G_1w_1+G_2w_2+\cdots=0$.

COROLLARY. *An allowable perfect ideal which is prime is an allowable prime ideal.*

REMARK. The above ought, no doubt, to be the basis of defining an allowable ideal in general. *If we do take this definition in general, then we recover Hilbert's Nullstellensatz (weak form) as a theorem.* In fact, the leading statements in the above proof are still true if [ ] and { } are taken in the (present) narrower sense, but these do require some further substantiation. Let A, P

be as before, except that now they are allowable. Let A_0 be exactly as before, i.e., generated in the (previous) wider sense by P and u; and similarly for B_0. As before we have $A_0 \cdot B_0 \subseteq P$. Let A_0' be generated in the wider sense by A_0 and the partials with respect to the z_i of the elements in $A_0 \cap F[U_1^p, U_2^p, \cdots]$; and similarly for B_0'. Let $C \in A_0 \cap F[U_1^p, U_2^p, \cdots]$, $D \in B_0$. Then $\partial(CD^p)/\partial z_i = D^p \cdot \partial C/\partial z_i \in P$, whence $(D \cdot \partial C/\partial z_i)^p \in P$ and $D \cdot \partial C/\partial z_i \in P$. Using the calculation proving $A_0 \cdot B_0 \subseteq P$, we see that $A_0' \cdot B_0 \subseteq P$; and repeating the argument, that $A_0' \cdot B_0' \subseteq P$. Let A_1 be the ideal generated in the wider sense by the G such that $G^\rho \in A_0'$ for some ρ; and similarly for B_1. As before we get $A_1 \cdot B_1 \subseteq P$. Defining A_i, B_i, A_i', B_i' recursively, and repeating the above argument an infinite number of times, we get $\{P, u\} \cdot \{P, v\} \subseteq P$.

We are now in position to prove the chain theorem.

THEOREM 5. *In the case of* ch. $p \neq 0$, *conditions* (A) and (B) *continue to hold for the allowable prime and perfect ideals.*

Proof. Let $A = \bigcap P_\alpha$ be an allowable perfect ideal in $S = F\{U_1, \cdots, U_n\}$; we may suppose $A \neq (0)$. Let $G \in A$, $G \neq 0$, G of minimal degree in $U_1, \cdots, U_n$ and its derivatives: this degree may, trivially, be supposed positive, and further, we may assume inductively that every allowable perfect ideal containing an element of smaller degree is a finite intersection. Now $G \notin F[U_1^p, U_1'^p, \cdots, U_n^p, U_n'^p, \cdots]$. For if it were, then $G = G_1 w_1 + G_2 w_2 + \cdots$, where $w_1, w_2, \cdots$ is a linear basis of F/F^p, and $G_i \in F^p[U_1^p, \cdots]$. Since A is allowable, all the $G_i \in A$, hence $G_i^{1/p} \in A$ and not all $G_i = 0$; this contradicts the minimum condition on G. So at least one of the variables in G occurs with exponent not divisible by p, say U_{nr}, the rth but no higher derivative of U_n, occurs with such exponent t: U_{ns}, $s > r$, may occur, but with exponent divisible by p. It is convenient, and we may assume, that no such terms U_{ns}, $s > r$, occur; namely, adjoining (for a moment) U_{ns}^p, $s > r$, to the ground-field, we see that the coefficient of $U_{n,r+1}$ in G' is $\partial G/\partial U_{nr}$, in particular then $G' \neq 0$, and $U_{n,r+1}$ occurs with exponent not divisible by p; deg G' = deg G, and we replace G by G'. Replacing G by a still higher derivative if necessary, we may assume that deg $G = 0$ in U_{ns}, $s > r$. The coefficient of U_{nr}^t, being of too small degree, is not in A; it may be in some of the P_α, but separating these off, we may suppose that it is not in any P_α. As in the ch. 0 case, we may suppose the theorem to hold for $n-1$ variables, and even that the contraction of A to $F\{U_1, \cdots, U_{n-1}\}[U_n, \cdots, U_{nr}]$ is prime; here we make use of the corollary to §5 just as in the proof of the second point of the lemma. Under these circumstances, A is prime, and the proof for (A) is complete; (B) follows similarly.

For an allied discussion of the above, see Kolchin [3].

7. **Separable extensions.** According to our definition of an algebraic quantity, it is quite possible for an element u to be nonalgebraic over F and yet each u_i be algebraic (in the algebraic sense) over F.

EXAMPLE. Let $F=\pi(x, x_1, \cdots)$, $\pi=$prime field of ch. $p\neq 0$, $x, x_1, \cdots$ a sequence of (algebraic) indeterminates, and let $\alpha'=0$ for every $\alpha\in F$. In $S=F\{U\}$, let $P=S\cdot(U^p-x, U_1^p-x_1, \cdots)$. Then the residue of U mod P has the desired properties.

This pathological feature does not appear in the case of separable extensions. For explicitness we write out the definition of *separable quantity*.

DEFINITION. The algebraic differential quantity u is said to be separable over F if $F\langle u\rangle/F$ is separable.

THEOREM 6. *If u is transcendental over F and $F\langle u\rangle/F$ is separable, then $u, u_1, u_2, \cdots$ are algebraically independent (in the algebraic sense) over F.*

Proof. Suppose there were a nontrivial relation $G(u_1, \cdots, u_r)=0$; then let $G(U, \cdots, U_r)$ be of minimal total degree. If $G\notin F[U^p, U_1^p, \cdots]$, then one sees that we may assume G to have a term with U_r occurring with exponent not divisible by p (by replacing G by a derivative, as in the proof of Theorem 5). In that event, however, $F\langle u\rangle=F(u, \cdots, u_r, u_{r+1})$. Suppose then that $G\in F[U^p, U_1^p, \cdots]$. Let $w_1, w_2, \cdots$ be a basis of F/F^p. Then $G(U)=G_1(U)w_1+G_2(U)w_2+\cdots=0$, with $G_i\in F^p[U^p, U_1^p, \cdots]$, not all $G_i(U)=0$, whence also not all $G_i(u)=0$. On the other hand, $F^p(u^p, u_1^p, \cdots)/F^p$ is also clearly separable, so $w_1, w_2, \cdots$ are also linearly independent over $F^p(u^p, u_1^p, \cdots)$, a contradiction.

In precisely the same way one can establish the following.

COROLLARY. *If* d.d.t. $F\langle u_1, \cdots, u_n\rangle/F=n$ *and* $F\langle u_1, \cdots, u_n\rangle/F$ *is separable, then the u_{ij} are algebraically independent over F.*

The situation for a separable algebraic quantity parallels the case of characteristic 0.

THEOREM 7. *Let u be separable over F, and let* d.t. $F\langle u\rangle/F=r$. *Then $u, u_1, \cdots, u_{r-1}$ are algebraically independent (in the algebraic sense) over F, u_r is separable over $F(u, \cdots, u_{r-1})$, and $F\langle u\rangle=F(u, u_1, \cdots, u_r)$.*

Proof. Let $u, u_1, \cdots, u_{s-1}$ be algebraically independent, but $u, \cdots, u_s$ algebraically dependent over F. Let $G(U, \cdots, U_s)$, $G\neq 0$, be a polynomial of least degree satisfied by $u, \cdots, u_s$, the coefficients of G being in F. As in the proof of the previous theorem, we may assume U_s occurs with an exponent not divisible by p; i.e., we conclude that $F\langle u\rangle=F(u, \cdots, u_s)$, whence $s=r$, and the proof is complete.

Before proving the theorem of MacLane, we would like to consider two examples which are somewhat related to the point in question.

EXAMPLE. In the polynomial ring $S=F\{U, V\}$, the ideal $P=[U^p-V_1, V^p-U_1]$ is prime. Let $S/P=F\{u, v\}$. Then $F\langle u, v\rangle=F(u, v)$. This field is separable over F, but v is not separable over $F\langle u\rangle$, nor is u separable over $F\langle v\rangle$.

EXAMPLE. *The sum of separable quantities is not necessarily separable.* Let π be the prime field of ch. $p>2$, a, b algebraic indeterminates, and let $F=\pi(a, b)$, with $\alpha'=0$ for every $\alpha\in F$, $S=F\{U, V\}$, a polynomial ring. One verifies that $P=[(U+V^2)^p+a(U+2V^2)^p-b,\ U-U_1,\ V-V_1]$ is prime. In the residue class ring $F\{u, v\}(=F[u, v])$, u is transcendental (in the algebraic sense), over F, so is v; u is separable, satisfying $U=U_1$, and v also is separable. Moreover $(v^2)'=2v^2$, whence v^2 is separable; but $w=u+v^2$ is not separable. In fact $(u+v^2)^p+a(u+v^2)^p-b=-av^{2p}$, so w is not algebraic (in the algebraic sense) over F. Now w satisfies the irreducible polynomial $W^p+aW_1^p-b$; so w is not separable over F.

THEOREM OF S. MACLANE. *Let $F\langle u_1, \cdots, u_n\rangle/F$ be separable and of degree of differential transcendency t. Then for some relettering of the u_i, $F\langle u_1, \cdots, u_n\rangle$ is separable over $F\langle u_1, \cdots, u_t\rangle$.*

Proof. If $t=n$, there is nothing to prove. Let $t<n$, so that there exist nontrivial relations of the u_i over F. Let $G(U_1, \cdots, U_n)\neq 0$ be such that $G(u_1, \cdots, u_n)=0$, and let G be of minimum degree in the U_{ij}. Because $F\langle u_1, \cdots, u_n\rangle/F$ is separable and G is of minimal degree, we know that at least one U_{ij} occurs with exponent not divisible by p; say this is U_{nr}. Now drop the minimal condition of the degree of G, but assume that r is minimal; i.e., u_{ns} is separable over $F\langle u_1, \cdots, u_{n-1}\rangle(u_n, \cdots, u_{n,s-1})$ for $s=r$ but this is not the case for $s<r$. If now there are no nontrivial relations between the u_{ij}, $i<n$ or $i=n$, $j<r$, then we are through, since obviously $t=n-1$ and $u_1, \cdots, u_{n-1}$ is the required separating transcendency basis. Suppose, then, that there are such nontrivial relations, or that $t<n-1$. Let $G(u_1, \cdots, u_n)=0$ be such a relation, where $G(U_1, \cdots, U_n)$ is of minimal degree. (Incidentally, a straightforward induction does not seem to work.) Again we know that at least one U_{ij}, $i<n$, occurs with exponent not divisible by p; say this is U_{n-1,r_1}. Now drop the minimal condition on the degree of G but assume that r_1 is minimal; i.e., that $u_{n-1,s}$ is separable over $F\langle u_1, \cdots, u_{n-2}\rangle(u_n, \cdots, u_{n,r-1})(u_{n-1}, \cdots, u_{n-1,s-1})$ for $s=r_1$, but this is not the case for $s<r_1$. If now there are no nontrivial relations between the u_{ij}, $i<n-1$, or $i=n-1$, $j<r_1$, or $i=n$, $j<r$, then we are through, since obviously $t=n-2$ and $u_1, \cdots, u_{n-2}$ is the required separating transcendency basis. If, however, $t<n-2$, then the argument is to be repeated, and the proof will be complete after $n-t$ applications of the argument.

8. **The strong Nullstellensatz for arbitrary characteristic.** The strong Nullstellensatz does not hold for arbitrary prime ideals: in fact, above (§7, first example) we gave an example of a 1-dimensional prime ideal P in $R=F\{U\}$ for which R/P is a field. The theorem holds, however, for separable prime ideals; and in fact, the previous proof also holds here, since what is needed is a separating transcendency basis, and this we have. The following proof, however, may also be of interest.

Proof. Let $R/P=F\{u_1, \cdots, u_n\}$, and let $u_1, \cdots, u_r$ be algebraically independent over F. Since $F\langle u_1, \cdots, u_r\rangle/F$ is separable and of degree of differential transcendency r, one sees that the u_{ij}, $i=1, \cdots, r$, satisfy no nontrivial polynomial relations over F. One can now pick from the u_{ij}, $i>r$, a transcendency basis of $F\langle u_1, \cdots, u_n\rangle/F\langle u_1, \cdots, u_r\rangle$, say $v_1, v_2, \cdots, v_s$, and a linear basis $w_1, \cdots, w_t$ of $F\langle u_1, \cdots, u_n\rangle/F\langle u_1, \cdots, u_r\rangle(v_1, \cdots, v_s)$ from the power products of the u_{ij}, $i>r$. Then there exists a $d\in F\{u_1, \cdots, u_r\}[v_1, \cdots, v_s]$ such that for any $G\in F\{u_1, \cdots, u_n\}$ we can write $d^\rho G$ as a linear combination of the w's with coefficients in $F\{u_1, \cdots, u_r\}[v_1, \cdots, v_s]$. The element d involves a number of derivatives of u_r, say up to u_{rk}. Take $g\geqq k$ and also so large that $u_r^{(g+1)}, u_r^{(g+2)}, \cdots$ be algebraically independent over $S=F\{u_1, \cdots, u_{r-1}\}[v_1, \cdots, v_s, w_1, \cdots, w_t, u_r, \cdots, u_{rg}]$; this will be so if $w_1, \cdots, w_t$ are algebraic (in the algebraic sense) over $F\{u_1, \cdots, u_{r-1}\}[v_1, \cdots, v_s, u_r, \cdots, u_{rg}]$. Let $S^*=\{\alpha/d^\rho \mid \alpha\in S, \rho=1, 2, \cdots\}$. Then $S^*\{u_r^{(g+1)}\}$ is a differential subring of $F\langle u_1, \cdots, u_n\rangle$. Let Q^* be the ideal generated in the algebraic sense in $S^*\{u_r^{(g+1)}\}$ by $(u_r^{(g+1)}, u_r^{(g+2)}, \cdots)$; then Q^* is clearly a proper prime ideal, and moreover is differential. Let $q=Q^*\cap F\{u_1, \cdots, u_n\}$. Then q is a proper prime ideal in $F\{u_1, \cdots, u_n\}$, and it determines a proper prime ideal $Q\supset P$ in $F\{U_1, \cdots, U_n\}$; if g is taken sufficiently large (so that $d^\rho\alpha(u)\in S$), then clearly also $\alpha(U)\notin Q$ ($\alpha(U)\notin P$, given). The residue class ring of Q^* is just (isomorphic, in the abstract sense, to) S^*, and $F\{u_1, \cdots, u_n\}/q$ can be regarded as a subring of S^*; the quotient field of S^* is a subfield of the separable field $F\langle u_1, \cdots, u_n\rangle$, whence it is separable and Q is allowable. This completes the proof.

References

1. C. Chevalley, *Some properties of ideals in rings of power series*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 68–84.

2. E. R. Kolchin, *Extensions of differential fields*. I, Ann. of Math. vol. 43 (1942) pp. 724–729.

3. ———, *On the basis theorem for differential fields*, Trans. Amer. Math. Soc. vol. 52 (1942) pp. 115–127.

4. S. MacLane, *Modular fields*. I. *Separating transcendence bases*, Duke Math. J. vol. 5 (1939) pp. 372–393.

5. H. W. Raudenbush, *Differential fields and ideals of differential forms*, Ann. of Math. vol. 34 (1933) pp. 509–517.

6. J. F. Ritt, *Differential algebra*, Amer. Math. Soc. Colloquium Publications, vol. 33, New York, 1950.

7. B. L. van der Waerden, *Moderne Algebra*, vol. 1, Berlin, 1931.

8. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloquium Publications, vol. 29, New York, 1946.

University of California,
Berkeley, Calif.