SOME PROPERTIES OF IDEALS IN RINGS OF POWER SERIES

BY

CLAUDE CHEVALLEY

The behavior of a prime ideal in a polynomial ring when the basic field is extended to a larger field has been studied extensively by Zariski[1] in the case of a basic field of characteristic 0 and by A. Weil in the general case (his results are not published as yet). Our main purpose is to extend these results to the case of ideals in rings of power series, a case in which essentially new difficulties are encountered. We have nevertheless included in this paper a treatment of the "polynomial" case; several types of arguments appear in their simplest form in this case.

1. **Separably generated extensions.** A finite extension Z/K of a field K is said to be *separably generated* if there exists a transcendence base B of Z with respect to K such that Z is separable over $K(B)$.

MacLane has proved[2] that the following conditions are equivalent when Z/K is a finite extension of a field K of characteristic $p\neq 0$:

I. *The extension Z/K is separably generated*;

II. *The extension Z/K preserves p-independence*;

III. *If $y_1, \cdots, y_m$ are elements of Z and are linearly independent over K, then $y_1^p, \cdots, y_m^p$ are linearly independent over K.*

Conditions II and III remain equivalent if Z/K is an infinite extension, but they are no longer equivalent with I. It seems to me that the "good" notion of separably generated extension is the one which is expressed by II or III. For this reason, the term "separably generated extension" will be taken in this paper as synonymous with "extension preserving p-independence."

We shall often use a trivially equivalent formulation of condition II, which is:

II′. *If L/K is any finite extension of K such that $K\subset L\subset K^{1/p}$, then* $[ZL:Z]=[L:K]$.

PROPOSITION 1. *Assume that the extension Z/K is separably generated. If K'/K is any algebraic extension of K, the extension ZK'/K' is separably generated.*

Presented to the Society, November 27, 1943; received by the editors August 27, 1943.

[1] Cf. O. Zariski, *Algebraic varieties over ground fields of characteristic* 0, Amer. J. Math. vol. 62 (1940) p. 187.

[2] Cf. S. MacLane, *Modular fields.* I. *Separating transcendence bases*, Duke Math. J. vol. 5 (1939) p. 372.

It is clearly sufficient to prove Proposition 1 in the case where the extension Z/K is finite. In that case, there exists a separating transcendence base B of Z with respect to K; B is a transcendence base of ZK'/K' and ZK' is separable over $K'(B)$.

PROPOSITION 2. *Assume that the extension Z/K is separably generated. Let L/K be any finite purely inseparable extension of K. Then $[ZL:Z]=[L:K]$.*

We can find a finite chain $L_0=K\subset L_1\subset \cdots \subset L_h=L$ of subfields of L such that $L_i\subset L_{i-1}^{1/p}$ $(1\leqq i\leqq h)$. Since ZL_{i-1}/L_{i-1} is separably generated, we have $[ZL_i:ZL_{i-1}]=[L_i:L_{i-1}]$ $(1\leqq i\leqq h)$. Proposition 2 follows immediately from this formula.

PROPOSITION 3. *Let $\mathfrak{S}$ be a semi-simple hypercomplex system over the field K, and let Z/K be a separably generated extension of K. Then the hypercomplex system $\mathfrak{S}_Z$ over Z (obtained from $\mathfrak{S}$ by extending the field of coefficients from K to Z) is semi-simple.*

Let $\{u_1, \cdots, u_m\}$ be a base of $\mathfrak{S}/K$. Assume that $a=\sum_{i=1}^m z_iu_i$ $(z_i\in Z, 1\leqq i\leqq m)$ is an element of the radical of $\mathfrak{S}_Z$; then ab is nilpotent for every $b\in\mathfrak{S}_Z$. It follows that a belongs to the radical of $\mathfrak{S}_{Z'}$, where $Z'=K(z_1, \cdots, z_m)$. It is therefore sufficient to prove Proposition 3 in the case where Z is finite over K.

Let then $\{x_1, \cdots, x_r\}$ be a separating transcendence base of Z/K, and set $Z^*=K(x_1, \cdots, x_r)$. Since Z is algebraic and separable over Z^*, it is sufficient to prove that $\mathfrak{S}_{Z^*}$ is semi-simple. Let $\mathfrak{o}$ be the subring $K[x_1, \cdots, x_r, u_1, \cdots, u_m]$ of $\mathfrak{S}_{Z^*}$, and let a be an element of $\mathfrak{o}$ which is contained in the radical of $\mathfrak{S}_{Z^*}$. If $\xi_1, \cdots, \xi_r$ are any r elements of the algebraic closure of K, and if $K'=K(\xi_1, \cdots, \xi_r)$, there exists a homomorphism ϕ_ξ of $\mathfrak{o}$ onto $\mathfrak{S}_{K'}$ such that $\phi\ (x_j)=\xi_j$ $(1\leqq j\leqq r)$ and $\phi_\xi(u_i)=u_i$ $(1\leqq i\leqq m)$. It is clear that $\phi_\xi(a)$ belongs to the radical of $\mathfrak{S}_{K'}$, whence $\phi_\xi(a)=0$ if $\xi_1, \cdots, \xi_r$ are separable over K. Set $a=\sum P_i(x_1, \cdots, x_r)u_i$, where each P_i is a polynomial with coefficients in K. If we had $P_i\neq 0$ for some i, there would exist r elements $\xi_1, \cdots, \xi_r$, separable over K, such that $P_i(\xi_1, \cdots, \xi_r)\neq 0$, which brings a contradiction. It follows that $a=0$. Since every element of $\mathfrak{S}_{Z^*}$ can be brought in $\mathfrak{o}$ by multiplication by an element of Z^*, it follows that $\mathfrak{S}_{Z^*}$ is semi-simple.

PROPOSITION 4. *Let $X_1, \cdots, X_r$ be r letters. If the extension Z/K is separably generated, the extension $Z((X_1, \cdots, X_r))/K((X_1, \cdots, X_r))$ is also separably generated*[3].

Let $L_1/K((X_1, \cdots, X_r))$ be a finite extension of $K((X_1, \cdots, X_r))$ such that $L_1\subset [K((X_1, \cdots, X_r))]^{1/p}$. It is clear that L_1 is contained in some field L of the form $K((X_1, \cdots, X_r))(\phi_1^{1/p}, \cdots, \phi_h^{1/p})$, with $\phi_i\in K[[X_1, \cdots, X_r]]$

[3] We denote by $K[[X_1, \cdots, X_r]]$ the ring of formal power series in $X_1, \cdots, X_r$ with coefficients in K, and by $K((X_1, \cdots, X_r))$ the field of quotients of $K[[X_1, \cdots, X_r]]$.

$(1 \leqq i \leqq h)$, and we may assume without loss of generality that $[L:K((X_1, \cdots, X_r))] = p^h$. In order to prove that $[L_1Z((X_1, \cdots, X_r)):Z((X_1, \cdots, X_r))] = [L_1K((X_1, \cdots, X_r)):K((X_1, \cdots, X_r))]$, it will be sufficient to prove the similar formula with L_1 replaced by L.

We have $Z((X_1, \cdots, X_r))L = Z((X_1, \cdots, X_r))(\phi_1^{1/p}, \cdots, \phi_h^{1/p})$. Assume for a moment that we have a relation of the form

$$\sum_{(e)} \psi_{(e)} \phi_1^{e_1/p} \cdots \phi_h^{e_h/p} = 0,$$

where (e) runs over all the h-tuples $(e_1, \cdots, e_h)$ of integers such that $0 \leqq e_i < p$ $(1 \leqq i \leqq h)$, and where each $\psi_{(e)}$ belongs to $Z((X_1, \cdots, X_r))$. We can find an element $\theta \neq 0$ in $Z[[X_1, \cdots, X_r]]$ such that $\theta\psi_{(e)} \in Z[[X_1, \cdots, X_r]]$ for all (e).

Let $\{\zeta_\alpha\}$ be a linear base of Z/K. We may express every coefficient of any one of the series $\theta\psi_{(e)}$ as a (finite) linear combination of the ζ_α's with coefficients in K; given any $k > 0$, the expressions of the coefficients of the monomials of degrees less than or equal to k will involve only a finite number of the elements ζ_α. We may write

$$\theta\psi_{(e)} = \sum_\alpha \zeta_\alpha \psi_{(e),\alpha}, \qquad \psi_{(e),\alpha} \in K[[X_1, \cdots, X_r]].$$

We have

$$\sum_\alpha \left(\sum_{(e)} \psi_{(e),\alpha}^p \phi_1^{e_1} \cdots \phi_h^{e_h} \right) \zeta_\alpha^p = 0.$$

Let M be any monomial in $X_1, \cdots, X_r$, and let $a_{(e),\alpha}(M)$ be the coefficient of M in $\sum_{(e)} \psi_{(e),\alpha}^p \phi_1^{e_1} \cdots \phi_h^{e_h}$: we have $\sum_\alpha a_{(e),\alpha}(M) \zeta_\alpha^p = 0$. Since the extension Z/K is separably generated, any finite number of the elements ζ_α^p are linearly independent over K, whence $a_{(e),\alpha}(M) = 0$ for all (e), α, M, and

$$\sum_{(e)} \psi_{(e),\alpha}^p \phi_1^{e_1} \cdots \phi_h^{e_h} = 0.$$

Since $[L:K((X_1, \cdots, X_r))] = p^h$, it follows that $\psi_{(e),\alpha} = 0$ for all (e), α whence $\theta\psi_{(e)} = 0$, $\psi_{(e)} = 0$, which proves that $[Z((X_1, \cdots, X_r))L:Z((X_1, \cdots, X_r))] = p^h$ and therefore also that the extension $Z((X_1, \cdots, X_r))/K((X_1, \cdots, X_r))$ is separably generated.

Proposition 4a. *If the extension Z/K is separably generated, the extension $Z(X_1, \cdots, X_r)/K(X_1, \cdots, X_r)$ is also separably generated.*

The proof runs along exactly the same lines as the proof of Proposition 2, and we may therefore omit it.

Lemma 1. *Let K'/K be a finite algebraic extension of K. We have*

$[K'((X_1, \cdots, X_r)):K((X_1, \cdots, X_r))] = [K':K] = [K'(X_1, \cdots, X_r):K(X_1, \cdots, X_r)]$.

Since $[K':K]$ is finite, every element of $K'[[X_1, \cdots, X_r]]$ divides some element of $K[[X_1, \cdots, X_r]]$, whence $K'((X_1, \cdots, X_r))=K' K((X_1, \cdots, X_r))$.

Let $\{\omega_1, \cdots, \omega_m\}$ be a linear base of K'/K. It will be sufficient to prove that $\omega_1, \cdots, \omega_m$ are linearly independent over $K((X_1, \cdots, X_r))$ in $K'((X_1, \cdots, X_r))$. Assume that $\sum_{i=1}^{m}\phi_i\omega_i=0$, $\phi_i\in K((X_1, \cdots, X_r))$ $(1\leqq i\leqq m)$; we can find an element $\theta\neq 0$ in $K[[X_1, \cdots, X_r]]$ such that $\theta\phi_i\in K[[X_1, \cdots, X_r]]$ $(1\leqq i\leqq m)$. If we equate to 0 the coefficient of every monomial in the series $\sum_{i=1}^{m}\theta\phi_i\omega_i$, we see that $\theta\phi_i=0$, whence $\phi_i=0$ $(1\leqq i\leqq m)$, which proves Lemma 1.

PROPOSITION 5. *If K is any field, the extensions $K((X_1, \cdots, X_r))/K$, $K((X_1, \cdots, X_r))/K(X_1, \cdots, X_r)$ are separably generated.*

The first assertion follows immediately from Lemma 1. Let now $L_1/K(X_1, \cdots, X_r)$ be any extension of finite degree of $K(X_1, \cdots, X_r)$ which is obtained by adjunction of a finite number of pth roots of elements of $K(X_1, \cdots, X_r)$. It is clear that $L_1\subset L=K'(X_1^{1/p}, \cdots, X_r^{1/p})$, where K'/K is a suitable finite extension of K contained in $K^{1/p}/K$. In order to prove that $[L_1K((X_1, \cdots, X_r)):K((X_1, \cdots, X_r))]=[L_1:K(X_1 \cdots, X_r)]$, it will be sufficient to prove the same formula with L_1 replaced by L. By Lemma 1, we have $[K'((X_1, \cdots, X_r)):K((X_1, \cdots, X_r))]=[K':K]$. On the other hand, every element of $K'[[X_1, \cdots, X_r]]$ may be written as a linear combination of the elements of a base of K'/K with coefficients in $K[[X_1, \cdots, X_r]]$; it follows that $K'((X_1, \cdots, X_r))\subset K((X_1, \cdots, X_r))L$ and that the latter field is equal to $K'((X_1, \cdots, X_r))(X_1^{1/p}, \cdots, X_r^{1/p})$. The p^r elements $X_1^{e_1/p} \cdots X_r^{e_r/p}$ $(0\leqq e_i<p,\ 1\leqq i\leqq r)$ are clearly linearly independent over $K'((X_1, \cdots, X_r))$, whence $[K((X_1, \cdots, X_r))L:K'((X_1, \cdots, X_r))]=p^r$, $[K((X_1, \cdots, X_r))L:K((X_1, \cdots, X_r))]=p^r\cdot[K':K]$. By entirely similar arguments, we see that we have also $[L:K(X_1, \cdots, X_r)]=p^r[K':K]$, which proves Proposition 5.

2. **Relatively algebraically closed fields.**

DEFINITION 1. *Let K, Z be fields such that K is a subfield of Z. The field K is said to be algebraically closed in Z if every element of Z which is algebraic over K is already contained in K.*

It follows immediately from Lemma 1, §1, that K is always algebraically closed in $K((X_1, \cdots, X_r))$, and, a fortiori, in $K(X_1, \cdots, X_r)$.

PROPOSITION 6. *Assume that K is algebraically closed in Z. Then $K((X_1, \cdots, X_r))$ is algebraically closed in $Z((X_1, \cdots, X_r))$.*

Proposition 6 will follow immediately from the following lemma which holds independently of the assumption that K is algebraically closed in Z.

LEMMA 1. *Let ψ be an element of $Z((X_1, \cdots, X_r))$ which is algebraic over $K((X_1, \cdots, X_r))$. There exists a subfield K' of Z containing K which has the following properties:* (1) *K' is algebraic over K and the largest separable extension of K contained in K'/K is of finite degree*; (2) *we can represent ψ in the form ψ_1/ϕ_0 where $\psi_1 \in K'[[X_1, \cdots, X_r]]$, $\phi_0 \in K[[X_1, \cdots X_r]]$, $\phi_0 \neq 0$.*

Let

$$\phi_0\psi^m + \phi_1\psi^{m-1} + \cdots + \phi_m = 0$$

be an algebraic equation satisfied by ψ with coefficients in $K[[X_1, \cdots, X_r]]$. Then $\psi_1 = \phi_0\psi$ is integral over $K[[X_1, \cdots, X_r]]$, and, a fortiori, over $Z[[X_1, \cdots, X_r]]$. The latter ring being integrally closed, we have $\psi_1 \in Z[[X_1, \cdots, X_r]]$. The field K' will be the field generated over K by the coefficients of ψ_1.

Let Z^* be the algebraic closure of Z, and let σ be any automorphism of Z^*/K; σ may be extended to an automorphism of the ring $Z^*[[X_1, \cdots, X_r]]$ leaving invariant the elements of $K[[X_1, \cdots, X_r]]$. We have

$$\phi_0(\psi^\sigma)^m + \phi_1(\psi^\sigma)^{m-1} + \cdots + \phi_m = 0$$

and therefore there are at most m elements in $Z^*[[X_1, \cdots, X_r]]$ which can be written in the form ψ^σ. It follows that there are at most m distinct isomorphisms of K'/K into Z^*/K. In order to prove that K' is algebraic over K, it will be sufficient to prove that if u is an element of Z which is transcendental over K, and if k is any integer, there always exists an automorphism σ_k of Z^*/K such that $\sigma_k(u) = u^k$. In fact, we can form a transcendence base B of Z^*/K which contains u; let B' be the set obtained by replacing u by u^k in B; B' is also a transcendence base of Z^*/K, and there exists an isomorphism τ of $K(B)$ with $K(B')$ which maps u upon u^k and leaves the elements of K invariant. Since Z^* is the algebraic closure of $K(B)$, τ may be extended to an isomorphism σ_k of Z^* with the algebraic closure of $K(B')$, that is, with Z^*, which proves our assertion.

We have proved that K' is algebraic over K and that there are only a finite number of distinct isomorphisms of K'/K into Z^*/K, which proves that the largest separable extension of K contained in K'/K is of finite degree over K. Lemma 1, and therefore also Proposition 6, are proved.

Remark. It is quite easy to see that it is impossible to require the field K' of Lemma 1 to be of finite degree over K; it can be proved that K' may be selected such that, for a suitable f, K'^{pf} is of finite degree over K. We shall not give here the proof of this assertion, which we shall not use in this paper.

PROPOSITION 6a. *If K is algebraically closed in Z, the field $K(X_1, \cdots, X_r)$ is algebraically closed in $Z(X_1, \cdots, X_r)$.*

This proposition has been proved by Zariski[4]. It can also be derived exactly in the same way as we obtained Proposition 3. For these reasons, we shall omit its proof.

PROPOSITION 7. *If K is algebraically closed in Z, any polynomial in one letter, with coefficients in K, which is irreducible in K remains irreducible in Z*[5].

Let $f(X)$ be such a polynomial. We adjoin to Z an element x which is a root of the equation $f(x)=0$, and we denote by $g(X)$ the irreducible polynomial in Z, with first coefficient 1, which admits x as a zero. Since $g(X)$ divides $f(X)$, the conjugates of x with respect to Z are all zeros of $f(X)$ and are therefore algebraic over K. Taking into account the relations between coefficients and roots of an equation, we see that the coefficients of $g(X)$ are algebraic over K, that is, lie in K, whence $g(X)=af(X)$, $a\in K$, which proves Proposition 7.

COROLLARY. *If K'/K is a simple algebraic extension of K, and if K is algebraically closed in Z, we have $[ZK':Z]=[K':K]$.*

It should be observed that the formula $[ZK':Z]=[K':K]$ may fail to hold if K'/K is an algebraic extension of finite degree but which cannot be obtained by adjunction of a single element to K.

For this reason, it is convenient to introduce the following notion:

DEFINITION 2. *A subfield K of a field Z is said to be strongly algebraically closed in Z if K is algebraically closed in Z and Z is separably generated over K.*

PROPOSITION 8. *If K is strongly algebraically closed in Z, and if K'/K is any algebraic extension of finite degree of K, we have $[ZK':Z]=[K':K]$.*

Let K_0'/K be the largest separable extension of K contained in K'/K: we have already seen that $[ZK_0':Z]=[K_0':K]$. By Proposition 1, §1, we know that the extension ZK_0'/K_0' is separably generated. The extension K'/K_0' being purely inseparable, we have $[ZK':ZK_0']=[K':K_0']$ (cf. Proposition 2, §1). Proposition 8 follows immediately from these formulas.

COROLLARY 1. *If K is strongly algebraically closed in Z and if K'/K is any algebraic extension, K' is strongly algebraically closed in ZK'.*

Let ζ be an element of ZK' which is algebraic over K', and set $[K'(\zeta):K']=d$. We can find a finite algebraic extension K_1'/K, contained in K'/K, such that $[K_1'(\zeta):K_1']=d$ and $\zeta\in ZK_1'$. We have

$$[ZK_1':Z]=[K_1':K], \qquad [ZK_1':Z]=[ZK_1'(\zeta):Z]=[K_1'(\zeta):K],$$

whence $\zeta\in K_1'$, which proves that K' is algebraically closed in ZK'. Since we

[4] Cf. O. Zariski, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, Trans. Amer. Math. Soc. vol. 50 (1941) p. 61, Lemma 2.

[5] Cf. O. Zarski, loc. cit. note [1], p. 147, p. 190, Lemma 1.

also know that the extension ZK'/K' is separably generated, Corollary 1 is proved.

COROLLARY 2. *Let S/K be a finite algebraic extension of K, and assume that K is strongly algebraically closed in a field Z. Then, the hypercomplex system S_Z is a field.*

In fact, the subfield SZ of the algebraic closure of Z is of degree equal to $[S:K]$ over Z. It follows that S_Z coincides with SZ, considered as a hypercomplex system over Z.

3. **Extension of a prime ideal in a polynomial ring.** Let K be a field, and let $\mathfrak{p}$ be a prime ideal in $K[X_1, \cdots, X_n]$. Let Z be an overfield of K and let $\mathfrak{P}$ be the ideal generated by the elements of $\mathfrak{p}$ in $Z[X_1, \cdots, X_n]$. We want to study the structure of $\mathfrak{P}$, and, notably, to find under what condition the ideal $\mathfrak{P}$ is always prime, whatever Z may be.

Let $\{\zeta_\alpha\}$ be a linear base of Z/K; every element of $Z[X_1, \cdots, X_n]$ may be expressed in one and only one way in the form $\sum_\alpha A_\alpha \zeta_\alpha$, with $A_\alpha \in K[X_1, \cdots, X_n]$ and $A_\alpha = 0$ for almost all α. A necessary and sufficient condition for $\sum_\alpha A_\alpha \zeta_\alpha$ to belong to $\mathfrak{P}$ is that $A_\alpha \in \mathfrak{p}$ for every α. The condition is clearly sufficient; conversely, let us assume that $\sum_\alpha A_\alpha \zeta_\alpha = \sum_{i=1}^h B_i V_i$, where $\{V_1, \cdots, V_h\}$ is a set of generators of $\mathfrak{p}$ and $B_i \in Z[X_1, \cdots, X_n]$ $(1 \leqq i \leqq h)$. If we express B_i in the form $\sum_\alpha B_{i,\alpha} \zeta_\alpha$, $B_{i,\alpha} \in K[X_1, \cdots, X_n]$, we have $A_\alpha = \sum_{i=1}^h B_{i,\alpha} V_i \in \mathfrak{p}$ for every α, which proves our assertion.

It follows in particular that $\mathfrak{P} \cap K[X_1, \cdots, X_n] = \mathfrak{p}$, which proves that the ring $\mathfrak{o} = K[X_1, \cdots, X_n]/\mathfrak{p}$ may be identified with a subring of $\mathfrak{O} = Z[X_1, \cdots, X_n]/\mathfrak{P}$. Moreover we see that every element of $\mathfrak{O}$ may be expressed in one and only one way in the form $\sum_\alpha a_\alpha \zeta_\alpha$, with $a_\alpha \in \mathfrak{o}$, $a_\alpha = 0$ for almost all α.

Let S be the field of quotients of $\mathfrak{o}$; we can find r elements $y_1, \cdots, y_r$ of $\mathfrak{o}$ which form a transcendence base of S/K; let also $u_1, \cdots, u_d$ be elements of $\mathfrak{o}$ which form a linear base of $S/K(y_1, \cdots, y_r)$. We see immediately'that $y_1, \cdots, y_r$ are algebraically independent over Z in the ring $\mathfrak{O}$, and that the conditions $\sum_{i=1}^d \phi_i u_i = 0$, $\phi_i \in Z[y_1, \cdots, y_r]$ imply $\phi_i = 0$ $(1 \leqq i \leqq d)$.

An element $\phi \neq 0$ in $Z[y_1, \cdots, y_r]$ is not a zero divisor in $\mathfrak{O}$. In fact, assume that $\phi\psi = 0$, $\psi \in \mathfrak{O}$. We may express ψ in the form $\sum_\alpha b_\alpha \zeta_\alpha$, $b_\alpha \in \mathfrak{o}$. This sum having only a finite number of terms not equal to 0, we can find an element $c \neq 0$ in $K[y_1, \cdots, y_r]$ such that $cb_\alpha \in \sum_{i=1}^d K[y_1, \cdots, y_r]u_i$ for all α, whence $c\psi = \sum_{i=1}^d \psi_i u_i$, $\psi_i \in Z[y_1, \cdots, y_r]$. We have $\sum_{i=1}^d \phi\psi_i u_i = 0$, whence $\phi\psi_i = 0$ $(1 \leqq i \leqq d)$, and $\psi_i = 0$ $(1 \leqq i \leqq d)$ because $Z[y_1, \cdots, y_r]$ is a domain of integrity. It follows that $c\psi = 0$, whence $cb_\alpha = 0$ for every α, $b_\alpha = 0$ and $\psi = 0$ which proves our assertion.

Let us construct the ring of quotients $\mathfrak{S}$ of $\mathfrak{O}$; it follows from what we have proved that $\mathfrak{S}$ contains the field $Z(y_1, \cdots, y_r)$ and that the elements $u_1, \cdots, u_d$ are linearly independent over this field. It is clear. that $u_1, \cdots, u_d$ form a linear base of $\mathfrak{S}$ over $Z(y_1, \cdots, y_r)$.

The field S may be considered as a hypercomplex system over $K(y_1, \cdots, y_r)$; we see that $\mathfrak{S}$ is the hypercomplex system $S_{Z(y_1,y_2,\cdots,y_r)}$ which is deduced from S by extension of the field of coefficients from $K(y_1, \cdots, y_r)$ to $Z(y_1, \cdots, y_r)$.

Since $\mathfrak{S}$ is a hypercomplex system, the zero ideal in $\mathfrak{S}$ has no imbedded prime divisor; the same holds therefore for the zero ideal in $\mathfrak{O}$. We conclude that the ideal $\mathfrak{B}$ has no imbedded prime divisor. Moreover, if $\mathfrak{W}$ is any prime divisor of $\mathfrak{B}$, the ideal $\mathfrak{W}/\mathfrak{B}$ is a prime divisor of the zero ideal in $\mathfrak{O}$ and therefore has only 0 in common with $Z[y_1, \cdots, y_r]$. It follows that the field of quotients of $Z[X_1, \cdots, X_n]/\mathfrak{W}$ contains $Z(y_1, \cdots, y_r)$, and is therefore of degree of transcendency r over Z. We have therefore obtained the following result:

Proposition 9. *Let $\mathfrak{v}$ be a prime ideal of dimension r in $K[X_1, \cdots, X_n]$ and let Z be any overfield of K. The ideal generated by $\mathfrak{v}$ in $Z[X_1, \cdots, X_n]$ is an intersection of primary ideals whose associated prime ideals are all of dimension r*[6].

If K is strongly algebraically closed in Z, we know that $K(y_1, \cdots, y_r)$ is strongly algebraically closed in $Z(y_1, \cdots, y_r)$ (cf. Propositions 4a, §1, and 6a, §2). By Corollary 2 to Proposition 7, §2, it follows that $\mathfrak{S}$ is in this case a field, that is, that $\mathfrak{B}$ is a prime ideal.

We shall now prove that $\mathfrak{B}$ is always a prime ideal when K is strongly algebraically closed in S. We first show that it is sufficient to prove this statement in the case where the extension Z/K is finite. In fact, if there exist two polynomials in $Z[X_1, \cdots, X_n]$, neither of them belonging to $\mathfrak{B}$, but whose product belongs to $\mathfrak{B}$, let Z' be the field generated by adjunction to K of the coefficients of these polynomials; Z'/K is a finite extension, and the ideal generated by $\mathfrak{v}$ in $Z'[X_1, \cdots, X_n]$ is not prime.

Let us therefore assume that the extension Z/K is finite, and let $\{z_1, \cdots, z_s\}$ be a transcendence base of Z/K; we set $K' = K(z_1, \cdots, z_s)$; the field K is strongly algebraically closed in K' (cf. Lemma 1, §1), and therefore the ideal generated by $\mathfrak{v}$ in $K'[X_1, \cdots, X_n]$ is prime. Since Z/K' is a finite algebraic extension, we see that it will be sufficient to prove our statement in the case where Z/K is a finite algebraic extension. Assuming that such is the case, we observe that every element of $\mathfrak{S}$ may be written in the form $\sum_\alpha a_\alpha \zeta_\alpha$, $a_\alpha \in S$, and that the elements ζ_α are linearly independent over S. It follows that $\mathfrak{S}$ may be identified with the hypercomplex system Z_S obtained by considering Z as a hypercomplex system over K and extending the field of coefficients from K to S. Since K is strongly algebraically closed in S,

[6] Cf. W. Krull, *Der allgemeine Diskriminantensatz. Unverzweigte Ringerweiterungen*, Math. Zeit. vol. 45 (1939), and O. Zariski, loc. cit. note [1], p. 147; p. 193, Theorem 2'.

Z_S is a field by Corollary 2 to Proposition 7, §2, which proves our assertion.

Conversely, let us assume that $\mathfrak{V}$ is a prime ideal whenever Z/K is a finite algebraic extension; we shall then prove that K must be strongly algebraically closed in S. Let S^* be the algebraic closure of S; if Z/K is any algebraic extension of finite degree contained in S^*/K, the hypercomplex system Z_S over S is a field, which proves that $[ZS:S] = [Z:K]$. Taking first Z/K to be purely inseparable, we see that S/K is separably generated. Taking then for Z a subfield of S, we see that K is algebraically closed in S. Therefore we have the following result:

PROPOSITION 10. *Let $\mathfrak{v}$ be a prime ideal in $K[X_1, \cdots, X_n]$, and let S be the field of quotients of the ring $K[X_1, \cdots, X_n]/\mathfrak{v}$. If K is strongly algebraically closed in $\mathfrak{S}$, and if Z/K is any extension of K, the ideal generated by $\mathfrak{v}$ in $Z[X_1, \cdots, X_n]$ is prime. Conversely, if the latter condition is verified whenever Z/K is a finite algebraic extension, then K is strongly algebraically closed in S.*

PROPOSITION 11. *Let K be a field and let $\mathfrak{v}$ be a prime ideal in $K[X_1, \cdots, X_n]$. Assume that K is strongly algebraically closed in the field of quotients of the ring $K[X_1, \cdots, X_n]/\mathfrak{v}$. Let Z be any overfield of K, and let $\mathfrak{V}$ be the ideal generated by $\mathfrak{v}$ in the ring $Z[X_1, \cdots, X_n]$. Then Z is strongly algebraically closed in the field of quotients of the ring $Z[X_1, \cdots, X_n]/\mathfrak{V}$.*

In fact, let Z^* be the algebraic closure of Z. The ideal generated by $\mathfrak{V}$ in $Z^*[X_1, \cdots, X_n]$ is prime; but this ideal is also the ideal generated by $\mathfrak{V}$ in the same ring, which proves our assertion.

We shall now give a proposition which is the base of the theory of products of algebraic varieties. We denote by K a field, and by $(X_1, \cdots, X_m)$, $(Y_1, \cdots, Y_n)$ two series of letters with no letter in common.

PROPOSITION 12. *Let $\mathfrak{u}$ be a prime ideal in $K[X_1, \cdots, X_m]$ and let $\mathfrak{v}$ be a prime ideal in $K[Y_1, \cdots, Y_n]$. Let $\mathfrak{w}$ be the ideal generated by the elements of $\mathfrak{u}$ and of $\mathfrak{v}$ in $K[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$. Let S and T be the fields of quotients of the rings $K[X_1, \cdots, X_m]/\mathfrak{u}$, $K[Y_1, \cdots, Y_n]/\mathfrak{v}$ respectively. If K is strongly algebraically closed in at least one of the fields S, T, the ideal $\mathfrak{w}$ is prime. If K is strongly algebraically closed in both S and T, it is also strongly algebraically closed in the field of quotients of $K[X_1, \cdots, X_m, Y_1, \cdots, Y_n]/\mathfrak{w}$.*

Assume that K is strongly algebraically closed in S. We know that the ideal generated by $\mathfrak{u}$ in $T[X_1, \cdots, X_m]$ is prime. Let $\mathfrak{U}$ be this ideal.

The ring $K[Y_1, \cdots, Y_n]/\mathfrak{v}$ may be considered as a vector space (in general of infinite dimension) over K; let us take a linear base $\{u_\alpha\}$ of this vector space over K; for each α we select a representative U_α of the class u_α modulo $\mathfrak{v}$ in $K[Y_1, \cdots, Y_n]$; every element of the latter ring is then congruent modulo $\mathfrak{v}$ to a linear combination with coefficients in K of the polynomials U_α.

Let F, G be two elements of $K[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$ such that $FG \in \mathfrak{w}$. If we replace in F and G each letter Y_j by its residue class modulo $\mathfrak{v}$, we obtain two polynomials $\overline{F}$, $\overline{G}$ in $X_1, \cdots, X_m$ with coefficients in T, and we have clearly $\overline{FG} \in \mathfrak{U}$. Therefore at least one of the polynomials $\overline{F}$, $\overline{G}$, say $\overline{F}$, belongs to $\mathfrak{U}$. We may represent $\overline{F}$ in the form of a finite sum $\sum_{\alpha,M} a(M; \alpha) M u_\alpha$ where M runs over the distinct monomials in $X_1, \cdots, X_m$ and where $a(M; \alpha) \in K$. The elements $u_\alpha \in T$, being linearly independent over K, may be included in a linear base of T/K; remembering what we have said at the beginning of this section, we see that $\sum_M a(M; \alpha) M \in \mathfrak{u}$ for every α. It follows that $\sum_{M,\alpha} a(M; \alpha) M U_\alpha \in \mathfrak{w}$. On the other hand, we have clearly $F - \sum_{M,\alpha} a(M; \alpha) M U_\alpha \in \mathfrak{w}$, whence $F \in \mathfrak{w}$, which proves the first part of Proposition 12.

Assume now that K is strongly algebraically closed in both S and T, and let K^* be the algebraic closure of K. The ideals $\mathfrak{u}^*$, $\mathfrak{v}^*$ generated by $\mathfrak{u}$, $\mathfrak{v}$ in $K^*[X_1, \cdots, X_m]$, $K^*[Y_1, \cdots, Y_n]$ respectively are prime by Proposition 10. By the first part of Proposition 12, the ideal $\mathfrak{w}^*$ generated by $\mathfrak{u}^*$ and $\mathfrak{v}^*$ in $K^*[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$ is prime. But $\mathfrak{w}^*$ is also the ideal generated by $\mathfrak{w}$, which proves the second part of Proposition 12 (taking into account the converse part of Proposition 10).

4. **Extension of a prime ideal in a ring of power series.** Let $\mathfrak{v}$ be a prime ideal in $K[[X_1, \cdots, X_n]]$ and let Z be any overfield of K. We shall denote by $\mathfrak{V}$ the ideal generated in $Z[[X_1, \cdots, X_n]]$ by the elements of $\mathfrak{v}$.

A good part of the theory of the ideal $\mathfrak{V}$ may be constructed exactly along the same lines as the theory of the extension of a prime ideal in a ring of polynomials. We observe that, if $\{\zeta_\alpha\}$ is a linear base of Z/K, every element of $Z[[X_1, \cdots, X_n]]$ may be represented in one and only one way in the form $\sum_\alpha A_\alpha \zeta_\alpha$, with $A_\alpha \in K[[X_1, \cdots, X_n]]$. This sum may be infinite if Z is not of finite degree over K, but, given any $k > 0$, almost all the power series A_α begin with terms of total degrees greater than or equal to k. We conclude as before that $\mathfrak{V} \cap K[[X_1, \cdots, X_n]] = \mathfrak{v}$.

Let $\mathfrak{o}$, $\mathfrak{O}$ be the rings $K[[X_1, \cdots, X_n]]/\mathfrak{v}$, $Z[[X_1, \cdots, X_n]]/\mathfrak{V}$ respectively. $\mathfrak{o}$ and $\mathfrak{O}$ are complete local rings(7), and $\mathfrak{o}$ may be identified with a subring of $\mathfrak{O}$. Every element of $\mathfrak{O}$ may be written in one and only one way in the form $\sum_\alpha a_\alpha \zeta_\alpha$, $a_\alpha \in \mathfrak{o}$; such a sum may be infinite, but, if $k > 0$, we have $a_\alpha \in \mathfrak{p}^k$ for almost all α, where $\mathfrak{p}$ is the ideal of non-units of $\mathfrak{o}$.

Let $\{y_1, \cdots, y_r\}$ be a system of parameters in $\mathfrak{o}$. We know that $y_1, \cdots, y_r$ are analytically independent over K and that $\mathfrak{o}$ is a finite module over $K[[y_1, \cdots, y_r]]$. Let S be the field of quotients of $\mathfrak{o}$: S contains the field of quotients $K((y_1, \cdots, y_r))$ of $K[[y_1, \cdots, y_r]]$, and we can find a linear base $\{u_1, \cdots, u_d\}$ of $S/K((y_1, \cdots, y_r))$ which is composed of elements of $\mathfrak{o}$. Since $\mathfrak{o}$ is finite over $K[[y_1, \cdots, y_r]]$, there exists in the latter

[7] For the notions relative to local rings, cf. my paper *On the theory of local rings*, Ann. of Math. (2) vol. 44 (1943) p. 690.

ring an element $c\neq 0$ such that $c\mathfrak{o}\subset\sum_{i=1}^{d}K[[y_1, \cdots, y_r]]u_i$.

The elements $y_1, \cdots, y_r$ belong to the ideal of non-units of $\mathfrak{O}$, and we may therefore construct the ring $Z[[y_1, \cdots, y_r]]$ of the elements of $\mathfrak{O}$ which may be represented as power series in $y_1, \cdots, y_r$ with coefficients in Z. Every element of this ring may be represented in one and only one way in the form $\sum_\alpha a_\alpha\zeta_\alpha$ with $a_\alpha\in K[[y_1, \cdots, y_r]]$, which proves that $y_1, \cdots, y_r$ are analytically independent over Z in $\mathfrak{O}$. Moreover, we see that the conditions $\sum_{i=1}^{d}\phi_i u_i=0$, $\phi_i\in Z[[y_1, \cdots, y_r]]$ imply $\phi_i=0$ $(1\leqq i\leqq d)$.

By the same argument which was used in §3, we may conclude that an element not equal to 0 in $Z[[y_1, \cdots, y_r]]$ is not a zero divisor in $\mathfrak{O}$ (using the same notations as in §3, observe that, if c is the element introduced above, we have $cb_\alpha\in\sum_i K[[y_1, \cdots, y_r]]\cdot u_i$ for all α, which validates our argument even in the case where the sums under consideration are infinite).

We conclude as above that the ring of quotients $\mathfrak{S}$ of $\mathfrak{O}$ is the hypercomplex system $S_{Z((y_1, \cdots, y_r))}$ over $Z((y_1, \cdots, y_r))$, and we have therefore the following result:

Proposition 9a. *Let $\mathfrak{b}$ be a prime ideal of dimension r in $K[[X_1, \cdots, X_n]]$ and let Z be any overfield of K. The ideal generated by $\mathfrak{b}$ in $Z[[X_1, \cdots, X_n]]$ is an intersection of primary ideals whose associated prime ideals are of dimension r.*

Moreover, taking into account Propositions 4, §1, and 6, §2, we see that $\mathfrak{B}$ is always prime when K is strongly algebraically closed in Z.

Following the analogy with the case of an ideal in a ring of polynomials, we might expect that $\mathfrak{B}$ is also always prime when K is strongly algebraically closed in S. This is, however, not the case as can be shown by an example. This means that we have to make some more stringent requirement on the ideal $\mathfrak{b}$ in order to insure its "absolutely prime" character.

Before being able to formulate this additional requirement, we need the following notion. Let $\mathfrak{o}$ be a complete local ring which contains a field K, and let $(u_n)_{n=1,2,\cdots}$ be a sequence of elements of $\mathfrak{o}$ which converges to 0 in $\mathfrak{o}$; if $a_n\in K$ $(n=1, 2, \cdots)$, the series $\sum_n a_n u_n$ is always convergent in $\mathfrak{o}$. We shall say that the elements u_n $(n=1, 2, \cdots)$ are *strongly linearly independent* over K if the conditions $\sum_n a_n u_n=0$, $a_n\in K$, imply $a_n=0$ $(n=1, 2, \cdots)$. The elements of a finite sequence are said to be strongly linearly independent when they are linearly independent.

Definition 3. *A complete local ring $\mathfrak{o}$ containing a field K of characteristic $p\neq 0$ is said to be separably generated over K when the following condition is satisfied: if (v_n) is any finite or infinite sequence of elements of $\mathfrak{o}$ which are strongly linearly independent over K, the elements v_n^p are strongly linearly independent over K. If a complete local domain of integrity $\mathfrak{o}$ is separably generated over K and if moreover K is algebraically closed in the field of quotients of $\mathfrak{o}$, we shall say that K is strongly algebraically closed in $\mathfrak{o}$.*

We observe that this definition coincides with our previous definition of "separably generated" in the case where $\mathfrak{o}$ is a field Z, the ideal of non-units of $\mathfrak{o}$ being then the zero ideal of Z.

On the other hand, we see immediately that, if a complete local domain of integrity is separably generated over K, its field of quotients is also separably generated over K.

PROPOSITION 10a. *Let $\mathfrak{p}$ be a prime ideal in $K[[X_1, \cdots, X_n]]$ and let Z be an overfield of K. Assume that K is strongly algebraically closed in the ring $\mathfrak{o} = K[[X_1, \cdots, X_n]]/\mathfrak{p}$. Then the ideal generated by $\mathfrak{p}$ in $Z[[X_1, \cdots, X_n]]$ is prime.*

Using only the assumption that K is algebraically closed in the field of quotients S of $\mathfrak{o}$, we first prove that $\mathfrak{S} = S_{Z((y_1, \cdots, y_r))}$ does not contain any proper idempotent element. In fact, assume that $\epsilon = \sum_{i=1}^{d} \phi_i u_i$ is an idempotent in $\mathfrak{S}$ with $\phi_i \in Z\ ((y_1, \cdots\ y_r))$ $(1 \leqq i \leqq d)$; if $u_i u_j = \sum_{k=1}^{d} c_{ijk} u_k$ $(1 \leqq i, j \leqq d)$, we have

$$\sum_{i=1, j=1}^{d,d} \phi_i \phi_j c_{ijk} = \phi_k \qquad (1 \leqq k \leqq d).$$

We consider now the system of algebraic equations

$$\sum_{ij} \phi_i \phi_j c_{ijk} = \phi_k \qquad (1 \leqq k \leqq d) \tag{1}$$

in the letters $\phi_1, \cdots, \phi_d$ with coefficients in $K((y_1, \cdots, y_r))$. If Y^* is the algebraic closure of $Z((y_1, \cdots, y_r))$, the solutions of (1) in elements of Y^* are in a one-to-one correspondence with the idempotents of the hypercomplex system S_{Y^*} over Y^*. But a commutative hypercomplex system with a unit element has only a finite number of distinct idempotent elements, from which it follows that the system (1) has only a finite number of solutions in Y^*, and therefore that every such solution is algebraic over $K((y_1, \cdots, y_r))$. It follows that the elements $\phi_1, \cdots, \phi_d$ of $Z((y_1, \cdots, y_r))$ are algebraic over $K((y_1, \cdots, y_r))$. We shall see that they are separable over this field. In fact, if K is of characteristic $p \neq 0$, we have $\epsilon = \epsilon^p$, whence $\sum_i \phi_i^p u_i^p = \sum_i \phi_i u_i$; but we have $u_i^p = \sum_{j=1}^{d} a_{ij} u_j$, $a_{ij} \in K((y_1, \cdots, y_r))$, whence $\phi_j = \sum_{i=1}^{d} \phi_i^p a_{ij}$ and

$$\phi_i \in K((y_1, \cdots, y_r))(\phi_1^p, \cdots, \phi_d^p) \qquad (1 \leqq i \leqq d)$$

which proves our assertion.

It follows then immediately from Lemma 1, §2, that ϵ already belongs to $S_{K'((y_1, \cdots, y_r))}$, where K'/K is a finite algebraic separable extension of K contained in Z/K. Using the same argument as in the proof of Proposition 10, §3, we observe that

$$S_{K'((y_1, \cdots, y_r))} = K'_S.$$

Since K'/K is separable and K is algebraically closed in S, we have $[K'S:S]$

$=[K':K]$ (where K' and S are considered as subfields of the algebraic closure of S for instance; cf. the corollary to Proposition 7, §2); it follows that K'_S is a field, whence $\epsilon=0$ or $\epsilon=1$.

We now proceed to prove Proposition 10a. We may assume without loss of generality that Z is algebraically closed. We observe that, if K'/K is any extension of K, we shall be assured that $S_{K'((y_1,\cdots,y_r))}$ is a field as soon as we know that this hypercomplex system is semi-simple. We shall first prove that this is the case when $K'=K^{p^{-f}}$, where p is the characteristic of K, which is assumed to be not equal to 0 (observe that Proposition 10a would already be proved if K were of characteristic 0). It is sufficient to prove that the conditions $\phi=\sum_{i=1}^{d}\phi_i u_i$, $\phi_i\in K^{p^{-f}}((y_1,\cdots,y_r))$, $\phi^2=0$ imply $\phi=0$. We have $\phi_i^{p^f}\in K((y_1^{p^f},\cdots,y_r^{p^f}))$; we can find an element $\theta\neq 0$ in $K[[y_1^{p^f},\cdots,y_r^{p^f}]]$ such that $\phi_i^{p^f}\theta\in K[[y_1^{p^f},\cdots,y_r^{p^f}]]$. Let us arrange in a simple sequence (μ_k) the elements of $\mathfrak{o}$ which can be written as monomials in $y_1,\cdots,y_r$; we have $\lim_{k\to\infty}\mu_k=0$ and $\theta\phi_i^{p^f}=\sum_k a_{ik}\mu_k^{p^f}$, $a_{ik}\in K$. Since $\phi^2=0$, we have $\sum_i\phi_i^{p} u_i^{p^f}=0$, whence

$$\sum_{ik} a_{ik}(\mu_k u_i)^{p^f} = 0.$$

Since $u_1,\cdots,u_d$ are linearly independent over $K((y_1,\cdots,y_r))$, the elements $\mu_k u_i$ $(1\leqq k<\infty,\ 1\leqq i\leqq d)$ are strongly linearly independent over K; since $\mathfrak{o}$ is separably generated over K, the same holds for the elements $(\mu_k u_i)^{p^f}$, whence $a_{ik}=0$ for all (i,k) and $\phi_i=0$ $(1\leqq i\leqq d)$, which proves our assertion.

We set $K_\infty=\bigcup_{f=1}^{\infty}K^{p^{-f}}$, $Y_0=\bigcup_{f=1}^{\infty}K^{p^{-f}}((y_1,\cdots,y_r))$. We have seen that S_{Y_0} is a field. In order to prove that $S_{K_\infty((y_1,\cdots,y_r))}$ is a field, it will be sufficient to show that $K_\infty((y_1,\cdots,y_r))$ is separably generated over Y_0. If L_1 is any field such that $Y_0\subset L_1\subset Y_0^{1/p}$, we see immediately that $L_1\subset L=Y_0(y_1^{1/p},\cdots,y_r^{1/p})$. We have $[K_\infty((y_1,\cdots,y_r))L:K_\infty((y_1,\cdots,y_r))]=p^r=[L:Y_0]$, whence also $[K_\infty((y_1,\cdots,y_r))L_1:K_\infty((y_1,\cdots,y_r))]=[L_1:Y_0]$, which proves our assertion.

It follows that $S_{K_\infty((y_1,\cdots,y_r))}$ is a field. Since K_∞ is a perfect field, the extension Z/K_∞ is obviously separably generated; therefore the same holds for the extension $Z((y_1,\cdots,y_r))/K_\infty((y_1,\cdots,y_r))$ (by Proposition 4, §1), which completes the proof of Proposition 10a.

Proposition 10b. *Let $\mathfrak{b}$ be a prime ideal in $K[[X_1,\cdots,X_n]]$ and let K^* be the algebraic closure of K. If the ideal generated by $\mathfrak{b}$ in $K^*[[X_1,\cdots,X_n]]$ is prime, K is strongly algebraically closed in the ring $\mathfrak{o}=K[[X_1,\cdots,X_n]]/\mathfrak{b}$.*

The statement to the effect that K is algebraically closed in the field of quotients S of $\mathfrak{o}$ is proved exactly in the same way as the corresponding statement in Proposition 10, §3. In order to prove that $\mathfrak{o}$ is separably generated over K, we return for a moment to the consideration of an arbitrary extension Z/K of K and we observe that, if (v_n) is a sequence of elements of $\mathfrak{o}$ such that $\lim v_n = 0$, the strong linear independence of the elements v_n in $\mathfrak{o}$ over K implies their strong linear independence over Z in the ring denoted above by $\mathfrak{O}$. In fact, assume that $\sum_n b_n v_n = 0$, $b_n \in Z$; we may write b_n in the form $\sum_\alpha b_{n,\alpha}\zeta_\alpha$, $b_{n,\alpha} \in K$; for every n we have $b_{n,\alpha} = 0$ for almost all α; it follows immediately that, k being any integer greater than 0 and $\mathfrak{p}$ being the ideal of non-units in $\mathfrak{o}$, there are only a finite number of pairs (n, α) for which $b_{n,\alpha}v_n \notin \mathfrak{p}^k$; we may therefore write $\sum_n b_n v_n = \sum_\alpha \zeta_\alpha(\sum_n b_{n,\alpha}v_n)$. It follows that $\sum_n b_{n,\alpha} v_n = 0$ for every α, whence $b_{n,\alpha} = 0$ for every (n, α) and $b_n = 0$ for every n. This being said, assume now that $Z = K^*$ and that $\sum_n a_n v_n = 0$, $a_n \in K$. We have $a_n^{1/p} \in K^*$ and $(\sum_n a_n^{1/p} v^p)^p = 0$ in $\mathfrak{O}$. If the ideal generated by $\mathfrak{b}$ in $K^*[[X_1, \cdots, X_n]]$ is prime, $\mathfrak{O}$ is a domain of integrity, whence $\sum_n a_n^{1/p} v_n = 0$, $a_n^{1/p} = 0$ for all n, which proves that $\mathfrak{o}$ is separably generated over K.

PROPOSITION 11a. *Let K be a field and let $\mathfrak{b}$ be a prime ideal in $K[[X_1, \cdots, X_n]]$. Assume that K is strongly algebraically closed in the ring $K[[X_1, \cdots, X_n]]/\mathfrak{b}$. Let Z be any overfield of K, and let $\mathfrak{B}$ be the ideal generated by $\mathfrak{b}$ in the ring $Z[[X_1, \cdots, X_n]]$. Then Z is strongly algebraically closed in the ring $Z[[X_1, \cdots, X_n]]/\mathfrak{B}$.*

The proof is entirely similar to the proof of Proposition 11, §3.

Proposition 12 however cannot be extended so easily to the case of ideals in rings of power series. We need here a supplementary notion (strong linear base of a complete local ring) which we shall establish at the beginning of the next section.

5. The field of definition of an ideal.

PROPOSITION 13. *Let $\mathfrak{b}$ be an ideal in $K[[X_1, \cdots, X_n]]$. We can find a set $\boldsymbol{M}$ of monomials in $X_1, \cdots, X_n$ which has the following property: if F is any element of $K[[X_1, \cdots, X_n]]$, there exists one and only one power series F' of the form $\sum_{M \in \boldsymbol{M}} a(M)M$, $a(M) \in K$, such that $F \equiv F'$* (mod $\mathfrak{b}$).

To every power series $V \neq 0$ in $\mathfrak{b}$ let us assign its "initial form" V^*, which is the sum of the terms of lowest degree which appear in V. Let $\mathfrak{b}^*$ be the ideal generated in $K[X_1, \cdots, X_n]$ by the initial forms of the elements of V. If k is any integer greater than or equal to 0, we denote by $\boldsymbol{F}_k$ the linear space over K formed by the forms of degree k and by $\mathfrak{b}_k^*$ the set $\mathfrak{b}^* \cap \boldsymbol{F}_k$. We can find a finite set $\boldsymbol{M}_k$ of monomials of degree k such that every $F^* \in \boldsymbol{F}_k$ may be represented in one and only one way in the form $\sum_{M \in \boldsymbol{M}_k} a(M)M + W^*$, $a(m) \in K$, $W^* \in \mathfrak{b}_k^*$. We set $\boldsymbol{M} = \cup_{k=0}^\infty \boldsymbol{M}_k$.

If a power series V of the form $\sum_{M \in \boldsymbol{M}} a(M)M$ belongs to $\mathfrak{b}$, we have $a(M) = 0$ for every M. In fact, if we had $V \neq 0$, V would have an initial form V^* of degree say k, and V^* would be of the form $\sum_{M \in \boldsymbol{M}_k} a(M)M$, with some $a(M) \neq 0$, which is impossible since $V^* \in \mathfrak{b}_k^*$.

Let now F be any element of $K[[X_1, \cdots, X_n]]$. We shall construct by induction on k a polynomial F_k' of degree less than or equal to k which is a linear combination of the monomials $M \in \boldsymbol{M}$ and is such that $F - F_k' \in \mathfrak{v} + \mathfrak{x}^{k+1}$, where $\mathfrak{x}$ is the ideal generated by $X_1, \cdots, X_n$. We observe first that every form $W^* \neq 0$ in $\mathfrak{v}_k^*$ is the initial form of some element of $\mathfrak{v}$; in fact, we can write $W^* = \sum_i A_i V_i^*$ where each V_i^* is the initial form of an element $V_i \in \mathfrak{v}$ and where A_i is a form of degree equal to $k - d^0(V_i^*)$; it follows immediately that W^* is the initial form of the element $\sum_i A_i V_i \in \mathfrak{v}$. This being said, if $1 \in \mathfrak{v}$, we set $F_k' = 0$ for every k; if not, we have necessarily $1 \in \boldsymbol{M}$ and we set $F_0' = F(0, \cdots, 0)$. Assume that F_k' has already been determined; we can find an element $V_k \in \mathfrak{v}$ such that $F - F_k' - V_k \in \mathfrak{x}^{k+1}$; if this element belongs to $\mathfrak{x}^{k+2}$, we set $F_{k+1}' = F_k'$; if not, the initial form of $F - F_k' - V_k$ is of degree $k+1$ and may be expressed in the form $\sum_{M \in \boldsymbol{M}_{k+1}} a(M)M + W_{k+1}^*$, where $W_{k+1}^* \in \mathfrak{v}_{k+1}^*$; therefore W_{k+1}^* is the initial form of an element of $\mathfrak{v}$ (or is 0); we then set

$$F_{k+1}' = F_k' + \sum_{M \in \boldsymbol{M}_{k+1}} a(M)M$$

and we have $F - F_{k+1}' \in \mathfrak{v} + \mathfrak{x}^{k+2}$.

Moreover our construction shows that $F' = F_0' + \sum_{k=0}^{\infty}(F_{k+1}' - F_k')$ is a power series of the form $\sum_{M \in \boldsymbol{M}} a(M)M$, and that $F - F' \in \mathfrak{v} + \mathfrak{x}^k$ for every k. Since $\mathfrak{v}$ is closed in $K[[X_1, \cdots, X_n]]$, it follows that $F - F' \in \mathfrak{v}$, which proves Proposition 12.

We can arrange the set of the residue classes modulo $\mathfrak{v}$ of the elements $M \in \boldsymbol{M}$ into a simple sequence (μ_k). The elements of this sequence are strongly linearly independent over $\mathfrak{v}$, and every element of the ring $\mathfrak{o} = K[[X_1, \cdots, X_n]]/\mathfrak{v}$ is expressible in one and only one way in the form of an infinite sum of the form $\sum_k a_k \mu_k$, $a_k \in K$. Such a sequence is called a *strong linear base* of $\mathfrak{o}$ over K.

Having proved the existence of a strong linear base, we may proceed to generalize Proposition 12, §3:

PROPOSITION 12a. *Let $\mathfrak{u}$ be a prime ideal in $K[[X_1, \cdots, X_m]]$ and let $\mathfrak{v}$ be a prime ideal in $K[[Y_1, \cdots, Y_n]]$. Let $\mathfrak{w}$ be the ideal generated by the elements of $\mathfrak{u}$ and of $\mathfrak{v}$ in $K[[X_1, \cdots, X_m, Y_1, \cdots, Y_n]]$. Let $\mathfrak{s}$ and $\mathfrak{t}$ be the rings $K[[X_1, \cdots, X_m]]/\mathfrak{u}$ and $K[[Y_1, \cdots, Y_n]]/\mathfrak{v}$ respectively. If K is strongly algebraically closed in at least one of the rings $\mathfrak{s}$, $\mathfrak{t}$, the ideal $\mathfrak{w}$ is prime. If K is strongly algebraically closed in both, it is strongly algebraically closed in the ring $K[[X_1, \cdots, X_m, Y_1, \cdots, Y_n]]/\mathfrak{w}$.*

Assume that K is strongly algebraically closed in $\mathfrak{s}$. Let T be the field of quotients of $\mathfrak{t}$; the ideal $\mathfrak{U}$ generated by the elements of $\mathfrak{u}$ in $T[[X_1, \cdots, X_m]]$ is prime by Proposition 10a. We take a strong linear base $\{u_\alpha\}$ of the ring $\mathfrak{t}$ over K, and we select for each u_α a representative $U_\alpha \in K[[Y_1, \cdots, Y_n]]$ of the residue class u_α modulo $\mathfrak{v}$. This being done, we can follow step by step the proof of Proposition 12, the finite sums which occur there being here replaced by infinite sums which are convergent.

Another application of the notion of strong linear base is given by the theory of the field of definition of an ideal in a ring of power series[8]. Let $\mathfrak{d}$ be an ideal in $K[[X_1, \cdots, X_n]]$; we shall say that $\mathfrak{d}$ is *"definable"* in a subfield K' of K when there exists a system of generators of $\mathfrak{d}$ which is composed of elements of $K'[[X_1, \cdots, X_n]]$.

PROPOSITION 14. *Among all the subfields of K in which an ideal $\mathfrak{d}$ in $K[[X_1, \cdots, X_n]]$ is definable, there exists a smallest one, which is contained in every other.*

We construct a set $\boldsymbol{M}$ of monomials with the property described in Proposition 13, and we denote by $\boldsymbol{N}$ the set of the monomials which do not belong to $\boldsymbol{M}$. If $N\in\boldsymbol{N}$, we can find a power series G_N of the form $\sum_{M\in\boldsymbol{M}}a(M;N)M$ such that $N\equiv G_N \pmod{\mathfrak{d}}$. If F is any power series, we may write $F=\sum_{M\in\boldsymbol{M}}b(M)M+\sum_{N\in\boldsymbol{N}}b(N)N$, and we have

$$F \equiv \sum_{M\in\boldsymbol{M}}\left(b(M) + \sum_{N\in\boldsymbol{N}} b(N)a(M;N)\right)M \qquad \pmod{\mathfrak{d}}.$$

(Observe that the sum $\sum_{N\in\boldsymbol{N}}b(N)a(M;N)$ contains only a finite number of terms not equal to 0 because $a(M;N)=0$ as soon as N is of degree greater than M.) If we have $F\in\mathfrak{d}$, we have $b(M)+\sum_{N\in\boldsymbol{N}}b(N)a(M;N)=0$ for all M, whence $F=\sum_{N\in\boldsymbol{N}}b(N)(N-G_N)$.

The ideal $\mathfrak{d}'$ generated by the elements $N-G_N$ coincides with $\mathfrak{d}$; in fact, we have clearly $\mathfrak{d}'\subset\mathfrak{d}$; on the other hand, since $\mathfrak{d}'$ is a closed set, every convergent infinite linear combination of elements of $\mathfrak{d}'$ belongs to $\mathfrak{d}'$, whence $F\in\mathfrak{d}'$ if $F\in\mathfrak{d}$.

It follows that $\mathfrak{d}$ is definable in the field $K_{\mathfrak{d}}$ obtained by adjunction to the primitive field contained in K of all elements $a(M;N)$, for $M\in\boldsymbol{M}$, $N\in\boldsymbol{N}$.

Let conversely K' be any subfield of K in which $\mathfrak{d}$ is definable. Since $K'[[X_1, \cdots, X_n]]$ is Noetherian, it contains a finite set $\{V_1, \cdots, V_h\}$ of generators of $\mathfrak{d}$. We may therefore write $N-G_N=\sum_{i=1}^{h}A_{i,N}V_i$, where each $A_{i,N}$ is a power series with coefficients in K. Let us now associate with every monomial P in $X_1, \cdots, X_n$ and to every i $(1\leqq i\leqq h)$ an indeterminate $u_{P,i}$; we set $U_i=\sum_P u_{P,i}P$; if N' is any monomial of the set $\boldsymbol{N}$, we denote by $\lambda_{N'}$ the coefficient of N' in the power series $\sum_{i=1}^{h}U_iV_i$; $\lambda_{N'}$ is a linear form in a finite number of the indeterminates $u_{P,i}$ with coefficients in K'. Consider now the system of linear equations

$$\lambda_N(u_{P,i}) = 1;\ \lambda_{N'}(u_{P,i}) = 0 \text{ for all } N' \neq N \text{ in } \boldsymbol{N}.$$

The coefficients of this system belong to K'; on the other hand, the system

[8] The corresponding theory for ideals in polynomial rings has been developed by André Weil (cf. *Arithmetique et géometrie sur les variétes algebriques*, Hermann, Paris, 1935).

has a solution in K, given by the coefficients of the power series $A_{i,N}$; therefore, it has also a solution in K', which proves the existence of power series $A'_{i,N}$ with coefficients in K' such that

$$\sum_{i=1}^{h} A'_{i,N} V_i = N - \sum_{M \in \boldsymbol{M}} a'(M;N)M \qquad (a'(M,N) \in K).$$

We have clearly $a'(M; N) \in K'$. On the other hand we have

$$\sum_{M \in \boldsymbol{M}} (a'(M;N) - a(M;N))M = \sum_{i=1}^{h} (A'_{i,N} - A_{i,N})V_i \in \mathfrak{d},$$

whence $a'(M; N) = a(M; N)$ for all (M, N), which proves that $a(M; N) \in K'$, whence $K_{\mathfrak{d}} \subset K'$. Proposition 14 is thereby proved.

Similarly, if $\mathfrak{d}$ is an ideal in $K[X_1, \cdots, X_n]$, we shall say that $\mathfrak{d}$ is definable in a subfield K' of K if it has a set of generators composed of elements of $K'[X_1, \cdots, X_n]$.

PROPOSITION 14a. *Among all the subfields of K in which an ideal $\mathfrak{d}$ in $K[X_1, \cdots, X_n]$ is definable there exists a smallest one, which is contained in every other.*

The proof of Proposition 14a is entirely similar to the proof of Proposition 14. The set $\boldsymbol{M}$ is replaced by a set of monomials whose residue classes form a linear base of the ring $K[X_1, \cdots, X_n]/\mathfrak{d}$ over K (the existence of such a set follows from Zorn's lemma); the infinite sums which occurred in the proof of Proposition 13 are replaced by finite sums.

The smallest field in which an ideal $\mathfrak{d}$ in either $K[X_1, \cdots, X_n]$ or $K[[X_1, \cdots, X_n]]$ is definable is called the *field of definition* of the ideal $\mathfrak{d}$.

PRINCETON UNIVERSITY,
PRINCETON, N. J.