Specialization of the Isolated Common Zeros of a System of Polynomial Equations

By

D. G. Northcott, Sheffield

(Received October 19, 1960)

Introduction

For the reader's convenience, we begin by stating the main theorem of this paper leaving the precise definitions of some of the concepts until the later sections.

Let $R \to \bar{R}$ be a homomorphism of an integral domain R into an integral domain $\bar{R}$. We suppose these integral domains to have identity elements, but *it is not supposed that they have the same characteristic.* The quotient fields of the two integral domains will be denoted by F and $\bar{F}$ respectively.

Assume next that we have n polynomials $f_i(X_1, X_2, \ldots, X_n) = f_i(X)$, where $1 \leqslant i \leqslant n$, in n variables whose coefficients belong to R. The equations

$$f_i(X) = 0 \ \ (1 \leqslant i \leqslant n)$$

define an algebraic variety over the algebraic closure of the ground-field F. The components of this variety will, in general, be of assorted dimensions. Those components which reduce to single points are called *isolated common zeros* of the $f_i(X)$, and, if we take each such zero with the appropriate multiplicity, we get a complete set of isolated common zeros of the $f_i(X)$. This notion is given a precise formulation in § 1.

Let us now apply the homomorphism $R \to \bar{R}$. This transforms the polynomials $f_i(X)$ into new polynomials $\bar{f}_i(X)$, with coefficients in R, and these will have their own isolated common zeros. Our object is to prove the following theorem.

Theorem. Let the members of a complete set of isolated common zeros of the polynomials $f_i(X)$ be specialized simultaneously over $R \to R$.

The images of these common zeros can then be separated into two non-overlapping sets, one of which is a complete set of isolated common zeros of the polynomials $\bar{f}_i(X)$.

The notion of a specialization over $R \to \bar{R}$ needs clarification. This is provided in § 2.

1. Isolated zeros

In this section we shall be concerned with fields F and F^*, where F^* is an arbitrary extension of F, and F^* itself is regarded as being embedded in some algebraically closed field. In addition, we focus our attention on n given polynomials $f_i(X_1, \ldots, X_n)$ $(1 \leqslant i \leqslant n)$, in n variables, whose coefficients belong to F.

Let $\xi_1, \xi_2, \ldots, \xi_n$ be elements taken from the field in which F^* is embedded. These determine a prime ideal P in $F[X] = F[X_1, X_2, \ldots, X_n]$; indeed $g(X) \varepsilon P$ if and only if $g(\xi) = 0$. The dimension of P is equal to the transcendence degree of $F(\xi)$ over F and, in particular, P has dimension zero if and only if the ξ_i are algebraic over F. Clearly (ξ) is a common zero of the $f_i(X)$ if and only if P contains the $F[X]$-ideal $(f_1, f_2, \ldots, f_n)$.

Definition. The set (ξ) is called an 'isolated common zero' of the polynomials $f_i(X)$ if (i) *P is zero-dimensional and* (ii) *P is a minimal prime ideal of the ideal generated by $f_1, f_2, \ldots, f_n$ in $F[X]$.*

Suppose now that the elements ξ_i are algebraic over F, then the ideal P is unchanged if we replace (ξ) by one of its conjugates over F. By a *complete set of conjugates of (ξ) over F* one understands a set consisting of the distinct conjugates of (ξ) over F each repeated $[F(\xi):F]_i$ times. (We use $[F(\xi):F]_i$ to denote the degree of inseparability of $F(\xi)$ over F.) Since this complete set is already determined by the prime ideal P, we may use the symbol $\{P\}$ to denote it. As a further extension of this notation, we shall use $m\{P\}$, where $m \geqslant 0$ is an integer, to denote the set consisting of $\{P\}$ repeated m times.

Definition. By a 'complete set of isolated common zeros' of the $f_i(X)$ we understand the set

$$\bigcup_P \operatorname{Lgth}[(f); P]\,\{P\},$$

where P ranges over all zero-dimensional prime ideals of $F[X]$ which are also minimal prime ideals of the ideal $(f_1, f_2, \ldots, f_n)$.

In this definition, $\operatorname{Lgth}[(f); P]$ denotes the length of the P-primary component of the ideal $(f_1, f_2, \ldots, f_n) = (f)$.

After these preliminaries, let us shift our attention to the field F^*. If P is a prime ideal of $F[X_1, \ldots, X_n]$ and P^* a prime ideal of $F^*[X_1, \ldots \ldots, X_n]$, it will be convenient to write P^*/P if P^* contracts to P in $F[X]$. Observe that if P is zero-dimensional and P^*/P, then P^* is also zero-dimensional.

Let $(\xi) = (\xi_1, \xi_2, \ldots, \xi_n)$ be a set of elements all algebraic over F, $(\xi^{(1)})$, $(\xi^{(2)})$, $\ldots$, $(\xi^{(s)})$ a complete set of conjugates of (ξ) over F, and P the prime $F[X]$-ideal associated with (ξ). We introduce an equivalence relation $\sim$ between the $(\xi^{(\mu)})$ by writting $(\xi^{(\mu)}) \sim (\xi^{(\nu)})$ if $(\xi^{(\mu)})$ and $(\xi^{(\nu)})$ are conjugates over F^*; then the equivalence classes correspond to the prime ideals P^* such that P^*/P. Indeed, the $(\xi^{(\mu)})$ belonging to the class attached to P^*, constitute a complete set of conjugates over F^* repeated

$$[F(\xi) : F]_i/[F^*(\xi^{(\mu)}) : F^*]_i = [F[X]/P : F]_i/[F^*[X]/P^* : F^*]_i$$

times, which shows that

$$\{P\} = \bigcup_{P^*/P} j_{P^*} \{P^*\}, \tag{1.1}$$

where

$$j_{P^*} = [F[X]/P : F]_i/[F^*[X]/P^* : F^*]_i. \tag{1.2}$$

Next, still assuming that P is zero-dimensional, let N be a P-primary ideal. If now P^*/P, then P^* is a minimal prime ideal of $NF[X]$. Denote the P^*-primary component of $NF[X]$ by N^*. We shall need the following lemma, a proof of which will be found in the appendix.

Lemma 1. In the situation just described,

$$\operatorname{Lgth}(N^*) = j_{P^*} \operatorname{Lgth}(N),$$

where j_{P^*} *is defined by* (1.2).

To apply this result, let $P_1, P_2, \ldots, P_m$ be the zero-dimensional prime ideals of $F[X]$ which are also minimal prime ideals of $(f_1, \ldots, f_n)$. If now P^* is a prime ideal of $F^*[X]$, then, in order that P^* should be zero-dimensional and a minimal prime ideal of $(f_1, \ldots, f_n) F^*[X]$, it is necessary and sufficient that P^*/P_i for some i. Assume now that P^*/P, where P occurs among $P_1, P_2, \ldots, P_m$, and let N be the P-primary component of $(f_1, \ldots, f_n)$. Then $(f_1, \ldots, f_n)F^*[X]$ and $NF^*[X]$ have the same P^*-primary component N^* (say), and so, by Lemma 1,

$$\operatorname{Lgth}[(f); P^*] = j_{P^*} \operatorname{Lgth}[(f); P]$$

It follows, from (1.1), that

$$\bigcup_{i=1}^{m} \mathrm{Lgth}[(f); P_i]\{P_i\} = \bigcup_{i=1}^{m} \bigcup_{P^*/P_i} \mathrm{Lgth}[(f); P^*]\{P^*\}$$

Referring back to the last definition we see that we have proved

Proposition 1. Any complete set of isolated common zeros of the n polynomials $f_i(X_1, \ldots, X_n)$, when these are regarded as having coefficients in F, remains such when the polynomials are regarded as having coefficients in the extension field F^*.

Proposition 1 not only helps to justify the terminology but it provides an extremely useful tool in some of the arguments which follow.

2. Specializations

Let $R \to \bar{R}$ be a homomorphism of an integral domain R into an integral domain $\bar{R}$, and let F and $\bar{F}$ be their respective quotient fields. We shall regard each of F and $\bar{F}$ as being embedded in an appropriate *universal domain.* By a universal domain for F, we understand an algebraically closed extension field which has infinite transcendence degree over F.

Let $(\omega) = (\omega_1, \omega_2, \ldots, \omega_m)$ and $(\bar{\omega}) = (\bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_m)$ be two sets, each of m elements, the former taken from the universal domain for F and the latter from the universal domain for $\bar{F}$. We shall say *provisionally* that $(\bar{\omega})$ is a specialization of (ω) over $R \to \bar{R}$, if there is a homomorphism

$$R[\omega_1, \ldots, \omega_m] \to \bar{R}[\bar{\omega}_1, \ldots, \bar{\omega}_m]$$

which extends $R \to \bar{R}$ and in which $\omega_i \to \bar{\omega}_i$.

This definition has now to be broadened so that we can always be sure of the existence of specializations in appropriate circumstances. To this end, we adjoin an 'infinite element' to each of the universal domains and denote them both by ∞. Furthermore, we adopt the convention that $\infty^{-1} = 0$ and $0^{-1} = \infty$.

Suppose now that $(\omega_1, \omega_2, \ldots, \omega_m)$ has the property that, for each i, ω_i is either an element of the universal domain for F or is the infinite element. For brevity, we say that (ω) is a set of *generalized elements* over F. Should $e_i = \pm 1$ for $1 \leqslant i \leqslant m$, then $(\omega_1^{e_1}, \omega_2^{e_2}, \ldots, \omega_m^{e_m})$ is also a set of generalized elements and we say that it has been obtained from (ω) by a *reciprocation.* If, in addition, $(\bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_m)$ is a set of generalized elements over $\bar{F}$, then $(\omega_1^{e_1}, \ldots, \omega_m^{e_m})$ and $(\bar{\omega}_1^{e_1}, \ldots, \bar{\omega}_m^{e_m})$ are said to be obtained from (ω) and $(\bar{\omega})$ by a *common reciprocation.* Finally, when ∞ does not occur among $\omega_1, \omega_2, \ldots, \omega_m$, (ω) is said to be *finite.*

Consider two generalized sets $(\omega_1, \ldots, \omega_m)$ and $(\bar{\omega}_1, \ldots, \bar{\omega}_m)$. It may be possible to turn them into finite sets (ω') and $(\bar{\omega}')$, by means of a common reciprocation, in such a way that there exists a homomorphism $R[\omega'] \to \bar{R}[\bar{\omega}']$, extending $R \to \bar{R}$ and for which $\omega'_i \to \bar{\omega}'_i$. In these circumstances we continue to say that $(\bar{\omega})$ is a specialization of (ω) over $R \to \bar{R}$ and we write $(\omega) \to (\bar{\omega})$ (over $R \to \bar{R}$).

Assuming that $(\omega) \to (\bar{\omega})$ (over $R \to \bar{R}$), this situation will continue to hold if we apply a common reciprocation to (ω) and $(\bar{\omega})$. Should the reciprocation turn them both into *finite* sets (ω^*) and $(\bar{\omega}^*)$, then $(\bar{\omega}^*)$ will be a specialization of (ω^*), over $R \to \bar{R}$, in the original (provisional) sense.

The advantage of the above generalization resides in the following result. *If $(\omega_1, \omega_2, \ldots, \omega_m)$ is a set of generalized elements over F, then it is always possible to find generalized elements $\bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_m$ such that $(\omega) \to (\bar{\omega})$ over the homomorphism $R \to \bar{R}$.* This is proved easily by induction with respect to m once the case $m = 1$ has been established. So far as $m = 1$ is concerned, we can use the fact that either $R[\omega_1]$ or $R[\omega_1^{-1}]$ will contain a prime ideal which contracts, in R, to the kernel of the homomorphism $R \to \bar{R}$. A proof of this is to be found in ([2]. Th. 7, p. 260).

3. Reduction of the problem

We shall now use Proposition 1 to reduce our theorem to a special case in which we have a good deal of additional information. First, however, we prove

Lemma 2. Let D be a Noetherian integral domain and Q one of its proper prime ideals. Then there exists a regular one-dimensional local ring (= valuation ring of a discrete, real-valued valuation) A with the following properties:

(i) *A is an extension ring of D and has the same quotient field;*

(ii) *the maximal ideal J of A contracts, in D, to Q.*

Proof. Let D_1 be the ring of fractions of D with respect to Q, then D_1 is a local domain with maximal ideal Q_1 (say) and $Q_1 \cap D = Q$. Let Q_1 be generated by $\alpha_1, \alpha_2, \ldots, \alpha_s$ and let t be an indeterminate. Put* $D_2 = D_1[\alpha_1 t, \alpha_2 t, \ldots, \alpha_s t, t^{-1}]$, then D_2 is a Noetherian integral domain and $D_2 t^{-1} \cap D_1 = Q_1$. Let Q_2 be any minimal prime ideal of

* The device which follows is due to *D. Rees.*

$D_2 t^{-1}$, then rank $Q_2 = 1$ and, since Q_1 is a *maximal* ideal of $D_1, Q_2 \cap D_1 = Q_1$. It follows that $Q_2 \cap D = Q$.

Next let D_3 be the ring of fractions of D_2 with respect to Q_2, then D_3 is a one-dimensional local domain with maximal ideal Q_3 (say) and $Q_3 \cap D = Q$.

Consider the integral closure of D_3 in its quotient field. It is known ([*5*] Th. 7, p. 168) that this is a principal ideal domain with only a finite number of non-trivial prime ideals. Let Λ_1 be the ring of fractions, of the integral closure, with respect to any one of these prime ideals. Λ_1 is a one-dimensional regular local ring with maximal ideal J_1 (say) and $J_1 \cap D_3 = Q_3$. Accordingly $J_1 \cap D = Q$.

Finally, let E be the quotient field of D and put $\Lambda = E \cap \Lambda_1$, $J = E \cap J_1$. Then Λ is a one-dimensional regular local ring and J is its maximal ideal. (This is most easily seen by regarding Λ_1 as arising from a discrete, real-valued valuation, and considering the restriction of the valuation to E.) Since $D \subseteq \Lambda \subseteq E$ and $J \cap D = J_1 \cap D = Q$, the lemma is proved.

It is worthwhile noting that, if Λ is obtained by the above construction, then Λ/J will be of finite transcendence degree over the quotient field of R/Q.

Suppose now that we have an arbitrary specialization $(\omega_1, \ldots, \omega_m) \to (\bar{\omega}_1, \ldots, \bar{\omega}_m)$ over $R \to \bar{R}$ and let us apply a common reciprocation so as to make both sets finite. We then have a homomorphism $R[\omega] \to \bar{R}[\bar{\omega}]$, extending $R \to \bar{R}$, for which $\omega_i \to \bar{\omega}_i$. Denote by R_0 the subring of R generated by the identity element and the coefficients of the n polynomials $f_i(X_1, \ldots, X_n)$ whose zeros we are investigating. Then R_0 is Noetherian. Put

$$D = R_0[\omega],$$

then D is Noetherian, and, by restricting the domain and increasing the range of $R[\omega] \to \bar{R}[\bar{\omega}]$, we obtain a homomorphism

$$D \to \bar{F}(\bar{\omega})$$

in which $\omega_i \to \bar{\omega}_i$.

By Lemma 2, there exists a one-dimensional regular local ring Λ, with maximal ideal J, such that (i) Λ is an extension ring of D having the same quotient field and (ii) $J \cap D$ is the kernel Q (say) of the homomorphism $D \to \bar{F}(\bar{\omega})$. Thus Λ/J is an extension field of the quotient field of D/Q and may be taken as having finite transcendence degree over it. Accordingly, there exists an extension field $\bar{F}'$ of $\bar{F}(\bar{\omega})$, contained in the universal domain for $\bar{F}$, for which $D \to \bar{F}(\bar{\omega})$ can be enlarged to a homomorphism $\Lambda \to \bar{F}'$ with kernel J.

Let F_0 be the quotient field of R_0 and put $L = F_0 \cap \Lambda$, $M = F_0 \cap J$. Then L is a regular one-dimensional local ring and M is its maximal ideal. Note that $R_0 \subseteq L \subseteq L[\omega] \subseteq \Lambda$.

The mapping $\Lambda \to \bar{F}'$ induces a homomorphism $L[\omega] \to \bar{F}'$ which, because it vanishes on M, produces a homomorphism $L \to K$ of L *on to* a field K. $L[\omega]$ is therefore mapped on to $K[\bar{\omega}]$ and we have, in fact, a specialization $(\omega) \to (\bar{\omega})$ (over $L \to K$). It will be recalled that we applied a preliminary reciprocation to (ω) and $(\bar{\omega})$ to make them both finite. If the same reciprocation is applied again, (ω) and $(\bar{\omega})$ will return to their original forms. Thus the *original* specialization $(\omega) \to (\bar{\omega})$ (over $R \to \bar{R}$) has been transformed into a specialization $(\omega) \to (\bar{\omega})$ (over $L \to K$). Observe that the coefficients of the $f_i(X)$ are in L.

Let us apply this by taking $(\omega_1, \omega_2, \ldots, \omega_m)$ to be the set of elements obtained when we write out, in full, the coordinates of a complete set of isolated common zeros of the $f_i(X)$. The given specialization $(\omega \to (\bar{\omega})$ (over $R \to \bar{R}$) then provides an entirely general specialization of these common zeros.

In this situation, the ω_i are algebraic over the quotient field F_1 (say) of L. Denote by L^* the completion of L, as a local ring, and let $F_1{}^*$ be the quotient field of L^*. Notice that the mapping $L \to K$ gives rise to a homomorphism $L^* \to K$.

It is known that $(\omega) \to (\bar{\omega})$ (over $L \to K$) is equivalent to a specialization over $L^* \to K$. To be precise [see (*4*) Th. 1.], there is an isomorphism of $F_1(\omega)$, over F_1 and into the algebraic closure of $F_1{}^*$, such that $(\omega^*) \to (\bar{\omega})$ (over $L^* \to K$), where (ω^*) denotes the image of (ω) under the isomorphism in question. But (ω^*) will consist of the coordinates of a complete set of isolated common zeros of the $f_i(X)$, when these are regarded as polynomials with coefficients in $F_1{}^*$. This enormously simplifies our problem as is shown in the opening paragraph of the next section.

4. Completion of the proof

In this section, we shall use L to denote a complete, one-dimensional, regular local ring, with quotient field F, and we suppose given a homomorphism $L \to K$ of L on to a field K. The kernel of the homomorphism must, of course, be the maximal ideal M of L. We shall be concerned with n polynomials $f_i(X_1, \ldots, X_n)$ in n variables, and with their images $\bar{f}_i(X)$ under the homomorphism $L \rightarrow K$. The discussion, carried out in Section 3, shows that the theorem, described in the introduction, will be proved if we can establish the following special case.

Lemma 3. Let the members of a complete set of isolated common zeros, of the polynomials $f_i(X)$, be specialized simultaneously over $L \rightarrow K$. The images of the common zeros can then be separated into two disjoint sets, one of which is a complete set of isolated common zeros of the $\bar{f}_i(X)$.

Of course, as in the more general situation, each of F and K is regarded as being embedded in a universal domain.

In order to handle this problem, we shall fix our attention on a particular isolated common zero $(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n)$ of the $\bar{f}_i(X)$. This will determine a prime ideal $\bar{P}$ in $K[X]$. Denote by Φ the prime ideal which is the inverse image of $\bar{P}$ under the homomorphism $L[X] \rightarrow K[X]$ induced by $L \rightarrow K$. Further, let t be an element of L which generates its maximal ideal M.

It is clear that Φ contains $t, f_1, \ldots, f_n$ and, indeed, is a minimal prime ideal of the $L[X]$-ideal which they generate. Accordingly, $\operatorname{rank}(\Phi) \leqslant n + 1$. On the other hand, $\operatorname{rank}(tL[X]) = 1$ and $\operatorname{rank}(\Phi/tL[X]) = \operatorname{rank}(\bar{P}) = n$. Consequently $\operatorname{rank}(\Phi) = n + 1$.

Denote by $\operatorname{Mult}[(t, f); \Phi]$ the multiplicity of the Φ-primary component of the ideal $(t, f_1, \ldots, f_n)$, or, what comes to the same thing, the multiplicity of $t, f_1, \ldots, f_n$ regarded as a system of parameters in the ring of fractions of $L[X]$ with respect to Φ. We propose to use the associative law for multiplicities* to compute this in two different ways.

Taking the more difficult computation first, we have

$$\operatorname{Mult}[t, f); \Phi] = \sum_{Q} \operatorname{Mult}[f); Q] \operatorname{Mult}[((t, f) + Q)/Q; \Phi/Q], \tag{4.1}$$

where Q ranges over all the minimal prime ideals of the $L[X]$-ideal $(f_1, \ldots, f_n)$, which satisfy $Q \subseteq \Phi$ and $\operatorname{rank}(Q) + \operatorname{rank}(\Phi/Q) = n + 1$.

Suppose that Q is one of the prime ideals which occurs in the above sum. Then rank (Q) is at most n and rank (Φ/Q) is at most unity; consequently we have

$$\operatorname{rank}(Q) = n, \ \operatorname{rank}(\Phi/Q) = n + 1.$$

In addition $Q \cap L = (0)$. (For otherwise, since $Q \cap L$ is a prime L-ideal, Q would contain all of $t, f_1, \ldots, f_n$ and therefore would coincide with Φ.

* See *C. Lech* ([3], Theorem 1).

This, however, is impossible, because rank $(Q) = n$.) Denote by P the extension of Q in $F[X]$ and observe that $F[X]$ is the ring of fractions of $L[X]$, formed with respect to the non-zero elements of L. This shows that

(a) P is a minimal prime ideal of the $F[X]$-ideal $(f_1, f_2, \ldots, f_n)$;

(b) P has rank n, or, equivalently, dimension zero;

(c) $P \cap L[X] = Q$.

Conversely, suppose that P is a prime of $F[X]$, which satisfies (a) and (b) and has the further property that $P \cap L[X] \subseteq \Phi$. Then $Q = P \cap L[X]$ will be one of the prime ideals occurring on the right hand side of (4.1).

Assume that Q and P are related in the manner just described. Then $\mathrm{Mult}[(f); Q] = \mathrm{Mult}[(f); P]$. But the ring of fractions of $F[X]$ with respect to P, is a regular local ring in which $f_1, f_2, \ldots, f_n$ is a system of parameters; accordingly† $\mathrm{Mult}[(f); P] = \mathrm{Lgth}[(f); P]$ so that

$$\mathrm{Mult}[(f); Q] = \mathrm{Lgth}[(f); P]. \tag{4.2}$$

We have next to evaluate $\mathrm{Mult}[((t, f) + Q)/Q; \Phi/Q]$ for a prime ideal Q of the kind we are considering. Since $L \cap Q = (0)$, $L[X]/Q$ is an extension ring of L. Observe that, because Φ is a minimal prime ideal of $ML[X] + Q$, Φ/Q is a minimal prime ideal of the extension of M in $L[X]/Q$.

Denote by Λ the ring of fractions of $L[X]/Q$ with respect to Φ/Q. Λ is a local ring with maximal ideal M' (say), $M\Lambda$ is M'-primary and

$$[\Lambda/M' : L/M] = [L[X]/\Phi : L/M] = [K[X]/\bar{P} : K] < \infty.$$

But L is complete, consequently** Λ is a finite L-module. It follows that *$L[X]/Q$ is a finite L-module.*

Our results, so far, show that $L' = L[X]/Q$ is a complete, one-dimensional, local domain whose quotient field is $F' = F[X]/P$. Further, $\mathrm{Mult}[((t, f) + Q)/Q; \Phi/Q]$ is just the multiplicity of tL', considered as a primary L'-ideal, and this is the same as its length.

Let v be the valuation associated with L and v' the extension of v to F'. (Each of v and v' is to have the full additive group of integers as its value-group.) Now* the length of tL' is equal to $v'(t)$ multiplied

† See, for example, ([6], Theorem 5, p. 123).

** See *C. Chevalley* ([1], Prop. 4, p. 695).

* See ([5], Prop 5, p. 165).

by the degree of the residue field of v' over the residue field of L'; and this degree is equal to $[K_{v'} : K_v]$ divided by

$$[L[X]/\Phi : L/M] = [K[X]/\bar{P} : K].$$

(Here $K_{v'}$ and K_v denote the residue fields of v' and v respectively.) Accordingly

$$\text{Mult}[((t, f) + Q)/Q : \Phi/Q][K[X]/\bar{P} : K] = v'(t)\,[K_{v'} : K_v].$$

But $v'(t)$ is the ramification index for the extension from v to v'. Consequently, the right hand side of the above expression is just the degree of F' over F, and therefore

$$\text{Mult}[((t, f) + Q)/Q; \Phi/Q][K[X]/\bar{P} : K] = [F[X]/P : F]. \qquad (4.3)$$

Finally, combining (4.1), (4.2) and (4.3) all together, we obtain

Lemma 4. With the previous notation

$$\text{Mult}[(t, f); \Phi][K[X]/\bar{P} : K] = \sum_{P} \text{Lgth}[(f); P]\,[F[X]/P : F], \qquad (4.4)$$

where P ranges over all the zero-dimensional prime ideals of $F[X]$, which are minimal prime ideals of $(f_1, f_2, \ldots, f_n)$ and which satisfy $P \cap L[X] \subseteq \Phi$.

We can also compute $\text{Mult}[(t, f); \Phi]$ by considering the minimal prime ideals of $tL[X]$. Since $tL[X]$ is itself prime and $L[X]/tL[X]$ is just $K[X]$, the associative law for multiplicities shows that $\text{Mult}[t, f); \Phi]$ is equal to the product of $\text{Mult}[tL[X]; tL[X]]$ and

$$\text{Mult}[((t, f) + tL[X])/tL[X]; \Phi/tL[X]] = \text{Mult}[(\bar{f}); \bar{P}] = \text{Lgth}[(\bar{f}); \bar{P}].$$

But clearly $\text{Mult}[tL[X]; tL[X]] = 1$ and therefore we have shown that

$$\text{Mult}[(t, f); \Phi] = \text{Lgth}[(\bar{f}); \bar{P}]. \qquad (4.5)$$

Consider the zero-dimensional prime ideals P of $F[X]$ which are also minimal prime ideals of $(f_1, f_2, \ldots, f_n)$. We divide these into two disjoint sets Σ_1 and Σ_2 by putting into Σ_1 those P for which $P \cap L[X] \subseteq \Phi$ (Σ_2 is to consist of those which are left over.) On this understanding, we can combine (4.4) and (4.5) and thus obtain

$$\sum_{P \varepsilon \Sigma_1} \text{Lgth}[(f); P]\,[F[X]/P : F] = \text{Lgth}[(\bar{f}); \bar{P}]\,[K[X]/\bar{P} : K]. \qquad (4.6)$$

Let $(\xi) = (\xi_1, \ldots, \xi_n)$ be an isolated common zero of the $f_i(X)$ and P the corresponding prime ideal of $F[X]$. Then P belongs to $\Sigma_1 \cup \Sigma_2$. Suppose first that $P \varepsilon \Sigma_1$ and put $Q = P \cap L[X]$ so that $Q \subseteq \Phi$. The combined mapping

$$L[X] \to K[X] \to K[\bar{\xi}],$$

in which $X_i \rightarrow \bar{\xi}_i$, has kernel Φ and so there is induced a homomorphism $L[X]/Q \rightarrow K[\bar{\xi}]$. But $L[X]/Q$ is isomorphic to $L[\xi]$ ad nnow we see that $(\xi) \rightarrow (\bar{\xi})$ (over $L \rightarrow K$). But we can say more. For we saw earlier that $L[X]/Q$, or equivalently $L[\xi]$, is a finite L-module and therefore a complete local domain. We see from this that there is only one prime ideal of $L[\xi]$ which contracts, in L, to M. Accordingly, *if $P \varepsilon \Sigma_1$ then $(\xi) \rightarrow (\bar{\xi})$ (over $L \rightarrow K$) and the only other specializations of (ξ) over $L \rightarrow K$ are the conjugates of $(\bar{\xi})$ over K.*

Instead of assuming that $P \varepsilon \Sigma_1$, let us suppose instead that $(\xi) \rightarrow (\bar{\xi})$ (over $L \rightarrow K$). Then the combined mapping

$$L[X] \rightarrow L[\xi] \rightarrow K[\bar{\xi}]$$

has kernel Φ whereas $L[X] \rightarrow L[\xi]$ has kernel $P \cap L[X]$. Accordingly $P \varepsilon \Sigma_1$.

The remarks of the last two paragraphs show that $P \varepsilon \Sigma_1$ *if and only if* $(\xi) \rightarrow (\bar{\xi})$ (over $L \rightarrow K$). Put

$$\{A\} = \bigcup_{P \varepsilon \Sigma_1} \text{Lgth}[(f); P]\{P\} \tag{4.7}$$

and

$$\{B\} = \bigcup_{P \varepsilon \Sigma_2} \text{Lgth}[(f); P]\{P\} \tag{4.8}$$

Then $\{A\}$ and $\{B\}$ together make up a complete set of isolated common zeros of the $f_i(X)$. Further, if we specialize $\{A\}$ over $L \rightarrow K$, the result will be composed entirely of conjugates of $(\bar{\xi})$ over K. On the other hand, if we specialize $\{B\}$ over $L \rightarrow K$, no conjugate of $(\bar{\xi})$ will occur.

Let $P \varepsilon \Sigma_1$, let $u_1, u_2, \ldots, u_n, z$ be indeterminates, suppose that $(\xi) \varepsilon \{P\}$ and write

$$u * \xi = u_1 \xi_1 + u_2 \xi_2 + \cdots + u_n \xi_n. \tag{4.9}$$

If now (ξ') also belongs to $\{P\}$, then $u * \xi$ and $u * \xi'$ are conjugate over $F(u)$ and, as (ξ') varies, we get all the distinct conjugates of $u * \xi$ over $F(u)$ each repeated $[F(\xi) : F]_i$ times. Now

$$\begin{aligned}[F(\xi) : F]_i &= [F(u, \xi) : F(u)]_i \\ &= [F(u, \xi) : F(u * \xi)]_i \, [F(u * \xi) : F(u)]_i\end{aligned}$$

which shows that the $u * \xi'$ form a complete set of conjugates of $u * \xi$, over $F(u)$, repeated $[F(u, \xi) : F(u * \xi)]_i$ times. Accordingly, if $\phi(z)$ is the irreducible polynomial for $u * \xi$ over $F(u)$ and $e = [F(u, \xi) : F * (u\xi)]_i$, then

$$\prod_{(\xi') \varepsilon \{P\}} (z - u * \xi') \equiv \phi^e(z).$$

Now in view of the fact that $P \varepsilon \Sigma_1$, we know that $L[\xi]$ is a finite L-module and therefore each ξ_i is integral with respect to L. This shows that $u*\xi$ is integral with respect to $L[u]$. But L, being a complete, one-dimensional regular local ring, is integrally closed in F, and therefore $L[u]$ is integrally closed in $F(u)$. We see from this that $\phi(z)$, regarded as a polynomial in z, has its coefficients in $L[u]$. Accordingly

$$\prod_{(\xi') \varepsilon \{P\}} (z - u*\xi') \text{ and therefore also } \prod_{(\eta) \varepsilon \{A\}} (z - u*\eta) \tag{4.10}$$

belong to $L[u, z]$.

Let $\{A\} = \{\ldots (\eta) \ldots\}$ be specialized over $L \rightarrow K$ and let the result be $\{\bar{A}\} = \{\ldots (\bar{\eta}) \ldots\}$. As already observed, each of the $(\bar{\eta})$ occurring in $\{\bar{A}\}$ is a conjugate of $(\bar{\xi})$ over K and, in particular, is finite. Thus we have a homomorphism

$$L[\ldots, \eta_1, \ldots, \eta_n, \ldots] \rightarrow K[\ldots, \bar{\eta}_1, \ldots, \bar{\eta}_n, \ldots]$$

and this can be extended to a homomorphism

$$L[\ldots, \eta, \ldots, u, z] \rightarrow K[\ldots, \bar{\eta}, \ldots, u, z]$$

in which all of $u_1, u_2, \ldots, u_n, z$ are left fixed. Applying this to (4.10) we find that

$$\prod_{(\bar{n}) \varepsilon \{\bar{A}\}} (z - u*\bar{\eta})$$

is an element of $K[u, z]$. But if $(\bar{\eta}) \varepsilon \{\bar{A}\}$, then $u*\bar{\eta}$ is a conjugate of $u*\bar{\xi}$ over $K(u)$. Denote by $\bar{\psi}(z)$ the irreducible polynomial for $u*\bar{\xi}$ over $K(u)$. Then, since

$$\prod_{(\bar{\eta}) \varepsilon \{\bar{A}\}} (z - u*\bar{\eta})$$

is a polynomial in z with coefficients in $K(u)$, each of whose roots is a conjugate of $u*\bar{\xi}$ over $K(u)$,

$$\prod_{(\bar{\eta}) \varepsilon \{\bar{A}\}} (z - u*\bar{\eta}) = \bar{\psi}^m(z) \tag{4.11}$$

for a certain integer m. For convenience write

$$\{\bar{C}\} = \text{Lgth}[(\bar{f}); \bar{P}]\{\bar{P}\},$$

then

$$\prod_{(\bar{\xi}') \varepsilon \{\bar{C}\}} (z - u*\bar{\xi}') = \bar{\psi}^h(z), \tag{4.12}$$

where h is an integer. We now contend that $\bar{\psi}^m(z) = \bar{\psi}^h(z)$ and for this we need only show that they have the same degree. But the degree of the former is equal to the number of sets (η) which make up $\{A\}$ or

$$\sum_{P \varepsilon \Sigma_1} \mathrm{Lgth}[(f); P]\, [F[X]/P : F];$$

while that of the latter is $\mathrm{Lgth}[(\bar{f}); \bar{P}]\, [K[X]/\bar{P} : K]$. The equality of these two follows from (4.6).

Having proved that $\bar{\psi}^m(z)$ and $\bar{\psi}^h(z)$ are the same polynomial, we can compare the left hand sides of (4.11) and (4.12). This shows that the set generated by $u * \bar{\eta}$ as $(\bar{\eta})$ varies in $\{\bar{A}\}$, is the same as that generated by $u * \bar{\xi}'$ as $(\bar{\xi}')$ varies in $\{\bar{C}\}$. But this implies that $\{\bar{A}\} = \{\bar{C}\}$ or

$$\{\bar{A}\} = \mathrm{Lgth}[(\bar{f}); \bar{P}]\, \{\bar{P}\} \tag{4.13}$$

Proof of Lemma 3. It is now an easy matter to establish Lemma 3. Suppose that a complete set of isolated common zeros of the $f_i(X)$ is specialized over $L \to K$. By expressing the complete set in the form $\{A\} \cup \{B\}$ (see (4.7) and (4.8)), we find that the result of the specialization is made up of $\{\bar{A}\}$ and $\{\bar{B}\}$ (say), which do not overlap, and where $\{\bar{A}\} = \mathrm{Lgth}[(\bar{f}); \bar{P}]\, \{\bar{P}\}$. Furthermore, there is such a decomposition for every zero-dimensional prime ideal of $K[X]$ which is also a minimal prime ideal of $(\bar{f}_1, \ldots, \bar{f}_n)$. Lemma 3 merely combines these facts.

Appendix

The author was unable to find a reference for a proof of Lemma 1, though this result must be known. For the reader's convenience, the main outlines of a proof are sketched here.

Let P be a zero-dimensional prime ideal of $F[X_1, \ldots, X_n]$, F^* an extension field of F, and P^* a prime ideal of $F^*[X_1, \ldots, X_n]$ such that P^*/P. We begin by showing that

$$\mathrm{Lgth}[PF^*[X]; P^*] = [F[X]/P : F]_i / [F^*[X]/P^* : F^*]_i \tag{A}$$

which is Lemma 1 for the special case $N = P$.

Observe first that

$$F^*[X]/PF^*[X] \approx F^* \otimes_F (F[X]/P),$$

where, in this context, $\approx$ denotes a ring-isomorphism. Put $E = F[X]/P$, then E is an extension field of F and

$$F^*[X]/PF^*[X] \approx F^* \otimes_F E. \tag{B}$$

Let us use S to denote the field, between F and E, which consists of all the elements of E that are separable over F. We can then obtain a new expression for $F^* \otimes_F E$ by employing the isomorphisms

$$F^* \otimes_F E \approx F^* \otimes_F (S \otimes_S E) \approx (F^* \otimes_F S) \otimes_S E. \tag{C}$$

Now S is a separable extension of F of finite degree, consequently $F^* \otimes_F S$ is a direct sum of fields, say

$$F^* \otimes_F S = \Lambda_1 + \Lambda_2 + \dots + \Lambda_m, \quad \text{(direct sum)}$$

where each of $\Lambda_1, \Lambda_2, \dots, \Lambda_m$ contains both S and F^* as subfields and is their composition. From (B) and (C) we now obtain the ring-isomorphism

$$F^*[X]/PF^*[X] \approx (\Lambda_1 \otimes_S E) + \dots + (\Lambda_m \otimes_S E), \tag{D}$$

where it is to be understood that, on the right hand side, we have a direct sum of rings.

Let p denote the characteristic of F, then, since E is purely inseparable over S, there exists an integer σ with the following property: *if $y \varepsilon \Lambda_r \otimes_S E$, then y^{p^σ} belongs to Λ_r considered as a subfield of $\Lambda_r \otimes_S E$.* It follows that $\Lambda_r \otimes_S E$ possesses only a single prime ideal I_r (say) which is necessarily maximal. Accordingly

$$(\Lambda_1 \otimes_S E) + \dots + (\Lambda_{r-1} \otimes_S E) + I_r + (\Lambda_{r+1} \otimes_S E) + \dots + (\Lambda_m \otimes_S E)$$

is a maximal ideal of the right hand side of (D) and, by varying r, we get all its maximal ideals. We shall suppose that r is chosen so that

$$(\Lambda_1 \otimes_S E) + \dots + (\Lambda_{r-1} \otimes_S E) + I_r + (\Lambda_{r+1} \otimes_S E) + \dots + (\Lambda_m \otimes_S E)$$

corresponds to $P^*/PF^*[X]$, and then, if N^* denotes the P^*-primary component of $PF^*[X]$, $N^*/PF^*[X]$ corresponds to

$$(\Lambda_1 \otimes_S E) + \dots + (\Lambda_{r-1} \otimes_S E) + 0 + (\Lambda_{r+1} \otimes_S E) + \dots + (\Lambda_m \otimes_S E).$$

We conclude from this that Lgth$[PF[X]; P^*]$ is equal to the length of the zero ideal of $\Lambda_r \otimes_S E$, considered as a primary ideal belonging to I_r.

To simplify the notation, let us write Λ and I for Λ_r and I_r respectively. Consider a composition series of $(\Lambda \otimes_S E)$-ideals extending from the ring itself to the zero ideal. Each composition factor is isomorphic to $(\Lambda \otimes_S E)/I$ and the number of composition factors is equal to Lgth$[PF^*[X]; P^*]$. It follows that the dimension of $\Lambda \otimes_S E$, considered as a vector space over Λ, is equal to the product of Lgth$[PF^*[X]; P^*]$ and $[(\Lambda \otimes_S E)/\mathrm{I} : \Lambda]$. But the dimension of $\Lambda \otimes_S E$ over Λ is $[E : S] = [E : F]_i$ and so we obtain

$$[E : F]_i = \text{Lgth}[PF^*[X]; P^*][(\Lambda \otimes_S E)/\mathrm{I} : \Lambda]$$

Thus, to establish (A), we have only to prove that

$$[(\Lambda \otimes_S E)/I : \Lambda] = [F^*[X]/P^* : F^*]_i$$

Consider $(\Lambda \otimes_S E)/I$. This can be identified with $F^*[X]/P^*$. On the other hand, it contains $\varLambda$ as a subfield and is inseparable over it. But, as was noted earlier, $\varLambda$ is a compositum of F^* and S. Since S is a separable extension of F, $\varLambda$ is separable over F^* and now we see that $\varLambda$ is the separable closure of F^* in $(\varLambda\otimes_S E)/I$. Accordingly

$$\begin{aligned}[(\varLambda\otimes_S E)/I:\varLambda] &= [(\varLambda\otimes_S E)/I:F^*]_i\\ &= [F^*[X]/P^*:F^*]_i\end{aligned}$$

as required.

We turn now to the consideration of Lemma 1 itself. Let N be a P-primary ideal and

$$N = N_h \subset N_{h-1} \subset \ldots \subset N_1 \subset N_0 = F[X]$$

a composition series of $F[X]$-ideals. Then, for each integer r in the range $0 \leqslant r \leqslant h-1$, we have a non-canonical $F[X]$-isomorphism

$$N_r/N_{r+1} \approx F[X]/P.$$

This will give rise to an isomorphism

$$F^*\otimes_F(N_r/N_{r+1}) \approx F^*\otimes_F(F[X]/P) \tag{E}$$

in which the two sides are to be considered as modules with respect to the ring $F^*\otimes_F F[X]$.

Observe next that if A is an $F[X]$-module, then $F^*\otimes_F A$ is an exact functor of A. Accordingly

$$F^*\otimes_F(N_r/N_{r+1}) \approx (F^*\otimes_F N_r)/(F^*\otimes_F N_{r+1}).$$

Furthermore, the inclusion mapping $N_r \to F[X]$ induces a monomorphism $F^*\otimes_F N_r \to F^*\otimes_F F[X]$ and therefore $F^*\otimes_F N_r$ can be regarded as a submodule of $F^*\otimes_F F[X]$. But $F^*\otimes_F F[X]$ can be identified with $F^*[X]$ and, if this is done, $F^*\otimes_F N_r$ becomes identified with $N_rF^*[X]$. In this way we arrive at an isomorphism

$$F^* \otimes_F(N_r/N_{r+1}) \approx N_rF^*[X]/N_{r+1}F^*[X]$$

and, by similar arguments, we obtain

$$F^* \otimes_F(F[X]/P) \approx F^*[X]/PF^*[X].$$

Returning to (E) we may conclude from this that $N_rF^*[X]/N_{r+1}F^*[X]$ and $F^*[X]/PF^*[X]$ are isomorphic as $F^*[X]$-modules.

It is now a simple matter to deduce that

$$\begin{aligned}&\mathrm{Lgth}[N_{r+1}F^*[X];\,P^*] - \mathrm{Lgth}[N_rF^*[X];\,P^*]\\ &= \mathrm{Lgth}[PF^*[X];\,P^*]\\ &= [F[X]/P:\,F]_i/[F^*[X]/P^*:F^*]_i\end{aligned}$$

by virtue of (A). Lemma 1 itself follows if we sum for $r = 0, \ldots, h-1$.

References

[1] *Chevalley C.*, "On the theory of local rings", Ann. Math. Princeton, **44** (1943), 690–708.

[2] *Cohen l. S.* and *A. Seidenberg*, "Prime ideals and integral dependence", Bull. Amer. Math. Soc. **52** (1946), 252–261.

[3] *Lech C.*, "On the associativity formula for multiplicities", Arkiv för Mathematik **3** (1956), 301–314.

[4] *Northcott D. G.*, "Specializations over a local domain", Proc. London Math. Soc. (3) **1** (1951), 129–137.

[5] *Northcott D. G.*, "A general theory of one-dimensional local rings", Proc. Glasgow Math. Assoc. **2** (1956), 159–169.

[6] *Northcott D. G.*, "Semi-regular local rings", Mathematika **3** (1956), 117 –126.