ARKIV FÖR MATEMATIK Band 3 nr 52

Communicated 28 May 1958 by Otto Frostman and Lars Gårding

A metric result about the zeros of a complex polynomial ideal

By Christer Lech

Introduction

Let us begin by listing some notations. We shall denote by K the field of complex numbers, by $K[x] = K[x^1, \ldots, x^n]$ a polynomial ring over K in n variables, and by K^n the n-dimensional vector space over K. The complex conjugation in K, and its natural extensions to $K[x]$ and K^n, will be indicated by the superscript $\sim$ over the respective elements. Let $\gamma = (\gamma^1, \ldots, \gamma^n)$ be an element of K^n. It is called real if $\tilde{\gamma} = \gamma$, that is, if $\gamma^1, \ldots, \gamma^n$ are all real. The norm $\|\gamma\|$ of γ is defined as the non-negative number satisfying

$$\|\gamma\|^2 = \sum_{i=1}^{n} \tilde{\gamma}^i \gamma^i.$$

If, in $K[x]$, $f = f(x)$ is an element and $\mathfrak{a}$ an ideal, we denote by $d(\gamma; f)$ and $d(\gamma; \mathfrak{a})$ the distances in the sense of the norm between γ and the sets of complex zeros of f and of $\mathfrak{a}$ respectively. More precisely,

$$d(\gamma; f) = \inf \{ \|\gamma - \gamma'\| \mid \gamma' \in K^n, \ f(\gamma') = 0 \},$$
$$d(\gamma; \mathfrak{a}) = \inf \{ \|\gamma - \gamma'\| \mid \gamma' \in K^n, \ f(\gamma') = 0 \quad \text{for every } f \in \mathfrak{a} \},$$

where the infimum of an empty set is counted as $+\infty$.

Now let $\mathfrak{a} = (f_1, \ldots, f_r)$ be an ideal of $K[x]$. There exists in $\mathfrak{a}$ a polynomial which has no more *real* zeros than the ideal $\mathfrak{a}$ itself, for

$$f = \sum_{\nu=1}^{r} \tilde{f}_\nu f_\nu$$

is clearly such a polynomial. The object of the present note is to prove a refinement of this result in the form of the following

Theorem. *Let $\mathfrak{a}$ be an ideal of $K[x]$. There exist a polynomial $f \in \mathfrak{a}$ and a positive constant c such that for every real $\alpha \in K^n$ we have*

$$d(\alpha; f) \geqslant c\, d(\alpha; \mathfrak{a}).$$

If $\mathfrak{a}$ has no complex zeros, $d(\alpha; \mathfrak{a}) = +\infty$ for every α, and the theorem gives the existence of an $f \in \mathfrak{a}$ without complex zeros, i.e. a non-zero constant polynomial. Thus in this case we have a form of Hilbert's "Nullstellensatz".

The theorem has interesting applications in the theory of partial differential equations (see [2]), and this fact is the principal motivation for presenting it. The origin of this note was a question to the author by Prof. L. Hörmander, and the method, which will be used, is partly inspired by results of his (cf. esp. [1], § 3.3).

In our proof we shall consider polynomials f of the form

$$f=\sum_{\nu=1}^{N}\bar{f}_\nu f_\nu.$$

We shall give certain conditions on the K-*module* generated by $f_1, f_2, \ldots, f_N$ which will assure that f (for some constant c) has the property required by the theorem (see Section 1). Since, moreover, the proof can be reduced to the case where $\mathfrak{a}$ is a prime ideal not generated by a single element, we are led to construct, for every such prime ideal $\mathfrak{p}$ in $K[x]$, a certain finitely generated K-module M contained in $\mathfrak{p}$. Let us outline this construction, with a slight deviation of a purely formal nature. Put $d=$ the dimension of $\mathfrak{p}$. Denote by $\mathfrak{l}$ a $(n-d-1)$-dimensional linear variety in affine n-space, whose direction is determined by a set $\{\tau\}$ of indeterminates over K. There is an irreducible polynomial in $K(\tau)[x]$ whose set of zeros can be obtained as the locus of l when moved with fixed direction through the zeros of $\mathfrak{p}$. This polynomial is determined only up to a factor of $K(\tau)$, which we choose so as to obtain an irreducible polynomial $F(x,\tau)$ of $K[x,\tau]$. Now we can describe the module M. It is the K-module generated by all polynomials $F(x,\bar{\tau})$ that can be derived from $F(x,\tau)$ by substituting systems $\{\bar{\tau}\}$ of values in K for the indeterminates $\{\tau\}$. Each of the special polynomials $F(x,\bar{\tau})\neq 0$ in M inherits from $F(x,\tau)$ the property that its set of zeros can be obtained by moving a $(n-d-1)$-dimensional linear variety through the zeros of $\mathfrak{p}$. This fact will be fundamental in proving that M satisfies the necessary conditions (see Lemma 2 and the "intuitive" outline below the formula (5.6), p. 552).

We shall employ the following algebraic tools: (i) Noether decomposition of ideals in a polynomial ring over a field (see e.g. [3], Chap. I, or [4], Chap. XII); (ii) elements of field extensions (see [5], Chap. I, §§ 1, 2, 3); (iii) the notion of a specialization and the theorem on extension of specializations ([5], Chap. II, §§ 1, 2, 3).

1. Modules

The aim of this section is to prove Lemma 2 below. The proof will be based on the following

Lemma 1. *Let M be a finitely generated K-module in $K[x]$, and suppose that $\{f_\nu\}_1^N$ and $\{g_\nu\}_1^{N'}$ are two systems of generators of M. Then there is a positive constant c_1 such that for every real $\alpha\in K^n$ we have*

$$d(\alpha;\sum_\nu \bar{f}_\nu f_\nu)\geqslant c_1 \min_\nu d(\alpha;g_\nu).$$

Proof. We shall use a certain approximate expression $d^*(\alpha;f)$ for $d(\alpha;f)$ where f is an arbitrary element of $K[x]$. If r is a natural number, and if $h_1, \ldots, h_r$ are arbitrary elements of $K[x]$, let $|h_1, \ldots, h_r|_\alpha$ denote $\max_\nu |h_\nu(\alpha)|$. Similarly, if $S_1, \ldots, S_r$ are sets of elements of $K[x]$, let $|S_1, \ldots, S_r|_\alpha$ denote $\sup|h(\alpha)|$ where h ranges over $S_1\cup\ldots\cup S_r$. In particular these definitions apply to the case $r=1$. Let t be a new variable and consider, for every $\theta = (\theta^1, \ldots, \theta^n)$ in K^n *of unit norm*, the expansion in powers of t of

$$f(x + t\theta) = f(x^1 + t\theta^1, \ldots, x^n + t\theta^n).$$

Denote by $D^k f$ $(k = 0, 1, 2, \ldots)$ the *set* of coefficients of t^k in these expansions. Then $D^k f \subset k[x]$. We define $d^*(\alpha; f)$ as the supremum of those positive real numbers A for which

$$|f|_\alpha > A^k |D^k f|_\alpha \quad k = 1, 2, 3, \ldots$$

or 0 if there are no such numbers. To elucidate this definition, consider for every θ of unit norm the expansion of $f(\alpha + \bar{t}\theta)$ in powers of $\bar{t}$, where $\bar{t} \in K$. If $|\bar{t}| < d^*(\alpha; f)$, then, in every such expansion, the first term $f(\alpha)$ will exceed in absolute value each of the subsequent terms. Moreover, $d^*(\alpha; f)$ is precisely the largest number with this property, or possibly $+\infty$.

Let us show that there are positive constants C_1 and C_2 depending on the total degree of f but *independent of* α such that, if $d(\alpha; f)$ and $d^*(\alpha; f)$ are not both 0 or both $+\infty$, then

$$C_1 \leqslant \frac{d(\alpha; f)}{d^*(\alpha; f)} \leqslant C_2. \tag{1.1}$$

It is easily checked that, if $d^*(\alpha; f)$ is equal to 0 or $+\infty$, then $d(\alpha; f)$ has the same value. In the remaining cases we can and shall assume that $d^*(\alpha; f) = 1$. For, if necessary, we can make a homothetic transformation with centre α, which changes $d(\alpha; f)$ and $d^*(\alpha; f)$ by the same suitably chosen factor, and of course such a transformation does not alter the degree of f. Thus, under the assumption that

$$0 \neq |f|_\alpha = \max_{k=1,2,3,\ldots} |D^k f|_\alpha, \tag{1.2}$$

we have to find C_1 and C_2 such that

$$C_1 \leqslant d(\alpha; f) \leqslant C_2.$$

If $|\bar{t}| \leqslant \frac{1}{2}$, it follows from (1.2) that, for every θ of unit norm, the first term in the expansion of $f(\alpha + \bar{t}\theta)$ in powers of $\bar{t}$ will have a larger absolute value than the sum of the others, so that $f(\alpha + \bar{t}\theta) \neq 0$. Hence we can take $C_1 = \frac{1}{2}$.

Let m be the total degree of f. Choose $k > 0$ so that $|f|_\alpha = |D^k f|_\alpha$, and θ so that the supremum involved in $|D^k f|_\alpha$ is attained for this θ. The kth elementary symmetric function of the m roots of the equation in z,

$$z^m f\left(\alpha + \frac{1}{z}\theta\right) = 0,$$

has then the absolute value one. It follows that the roots cannot all have absolute values less than $1/m$, for

$$\binom{m}{k} \frac{1}{m^k} \leqslant 1.$$

The equation in t, $f(\alpha + t\theta) = 0$, has therefore at least one root with an absolute value not exceeding m. Hence we can take $C_2 = m$. The formula (1.1) is thereby established. (The fact that α is real was not used here.)

In view of (1.1) and the definition of $d^*(\alpha; f)$, the statement of Lemma 1 can be formulated as follows: There is a positive constant C_3 independent of α such that, if

$$|g_\nu|_\alpha > A^k |D^k g_\nu|_\alpha \quad \begin{matrix} k = 1, 2, 3, \dots \\ \nu = 1, 2, \dots, N', \end{matrix} \qquad A > 0, \tag{1.3}$$

then, with $f = \sum_\nu \bar{f}_\nu f_\nu$, we have

$$|f|_\alpha > (C_3 A)^k |D^k f|_\alpha \quad k = 1, 2, 3, \dots \tag{1.4}$$

We shall prove the lemma on this new form. From (1.3) we get

$$|g_1, \dots, g_{N'}|_\alpha > A^k | D^k g_1, \dots, D^k g_{N'}|_\alpha \quad k = 1, 2, 3, \dots$$

Since each g_ν is a linear combination of the f_ν and conversely, it follows that

$$C_4 |f_1, \dots, f_N|_\alpha > A^k | D^k f_1, \dots, D^k f_N|_\alpha \quad k = 1, 2, 3, \dots \tag{1.5}$$

with $C_4 \geqslant 1$ independent of α. Now we use the fact that α is real. Evidently,

$$|f|_\alpha \geqslant |f_1, \dots, f_N|_\alpha^{\,2}.$$

Further, $|D^k \bar{f}_\nu|_\alpha = |D^k f_\nu|_\alpha$, and hence, expanding $\bar{f}_\nu(\alpha + t\theta) f_\nu(\alpha + t\theta)$ $(\nu = 1, 2, \dots, N)$ in powers of t,

$$|D^k f|_\alpha \leqslant N(k+1) \max_{i+j=k} |D^i f_1, \dots, D^i f_N|_\alpha \, |D^j f_1, \dots, D^j f_N|_\alpha \quad k = 1, 2, 3, \dots$$

Combining the last two inequalities with (1.5) and observing that $k + 1 \leqslant 2^k$ $(k = 1, 2, 3 \dots)$, we obtain (1.4) with $C_3 = (2NC_4^2)^{-1}$. This completes the proof of Lemma 1.

Lemma 2. *Let* $\mathfrak{a}$ *be an ideal of* $K[x]$. *Suppose that a finitely generated* K*-module* M *contained in* $\mathfrak{a}$ *satisfies the following condition:*

For every sequence $\{\alpha_\mu\}_1^\infty$ *of real elements of* K^n *none of which is a zero of* $\mathfrak{a}$, *there is a generating system* $\{g_\nu\}_1^{N'}$ *of* M *such that*

$$\limsup_{\mu \to \infty} \frac{d(\alpha_\mu; g_\nu)}{d(\alpha_\mu; \mathfrak{a})} > 0 \quad (\nu = 1, 2, \dots, N'), \tag{1.6}$$

where the fraction on the left is counted as 1 *when it has the form* ∞/∞, *and as* 0 *when it has the form* A/∞ *with* $A \neq \infty$.

Then, if $\{f_\nu\}_1^N$ *is an arbitrary finite generating system of* M, *there is a positive constant* c *such that, for every real* $\alpha \in K^n$, *we have*

$$d\left(\alpha; \sum_{\nu=1}^N \bar{f}_\nu f_\nu\right) \geqslant c\, d(\alpha; \mathfrak{a}).$$

Proof. Assume that the condition of the lemma is fulfilled. If $\mathfrak{a}$ has no complex zeros, it follows from (1.6) that the g_ν have no complex zeros either, and hence that $M = K$. In this case, as also when $\mathfrak{a} = (0)$, the result is obvious. Let us assume that we are in neither of these cases. Denote by $\alpha, \alpha_1, \alpha_2, \ldots$ real elements of K^n which are not zeros of $\mathfrak{a}$. (Such elements exist since $\mathfrak{a} \neq (0)$.) Put

$$\inf_{\alpha} \frac{d(\alpha; \sum_\nu \bar{f}_\nu f_\nu)}{d(\alpha; \mathfrak{a})} = c.$$

We then have to prove that c is positive. Take a sequence $\{\alpha_\mu\}_1^\infty$ such that

$$\lim_{\mu \to \infty} \frac{d(\alpha_\mu; \sum_\nu \bar{f}_\nu f_\nu)}{d(\alpha_\mu; \mathfrak{a})} = c.$$

For this sequence $\{\alpha_\mu\}_1^\infty$, choose $\{g_\nu\}_1^{N'}$ in accordance with the condition of the lemma so that (1.6) is valid. There is then an infinite subset I of the natural numbers such that

$$\inf_{\mu \in I} \frac{\min_\nu d(\alpha_\mu; g_\nu)}{d(\alpha_\mu; \mathfrak{a})} > 0.$$

By Lemma 1 we have
$$\inf_{\mu \in I} \frac{d(\alpha_\mu; \sum_\nu \bar{f}_\nu f_\nu)}{\min_\nu d(\alpha_\mu; g_\nu)} > 0.$$

Now
$$c = \lim_{\mu \in I} \frac{d(\alpha_\mu; \sum_\nu \bar{f}_\nu f_\nu)}{d(\alpha_\mu; \mathfrak{a})} \geqslant \left(\inf_{\mu \in I} \frac{d(\alpha_\mu; \sum_\nu \bar{f}_\nu f_\nu)}{\min_\nu d(\alpha_\mu; g_\nu)}\right) \left(\inf_{\mu \in I} \frac{\min_\nu d(\alpha_\mu; g_\nu)}{d(\alpha_\mu; \mathfrak{a})}\right).$$

Hence c is positive, which was to be proved.

2. Reduction of the proof of the theorem to the case where $\mathfrak{a}$ is a non-principal prime ideal

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the minimal prime ideals of $\mathfrak{a}$ (associated with an arbitrary Noetherian decomposition of this ideal). There is an integer N such that

$$(\mathfrak{p}_1 \cdots \mathfrak{p}_m)^N \subset \mathfrak{a}. \tag{2.1}$$

From this inclusion (and the fact that $\mathfrak{a} \subset \mathfrak{p}_\mu (\mu = 1, 2, \ldots, m)$) it is seen that the set of zeros of $\mathfrak{a}$ is the union of the sets of zeros of the $\mathfrak{p}_\mu$. Therefore, if $\gamma \in K^n$,

$$d(\gamma; \mathfrak{a}) = \min_\mu d(\gamma; \mathfrak{p}_\mu). \tag{2.2}$$

Suppose that we have proved the theorem for the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then there are polynomials $f_\mu \in \mathfrak{p}_\mu (\mu = 1, 2, \ldots, m)$ and positive constants c_μ such that, for every real $\alpha \in K^n$,

$$d(\alpha; f_\mu) \geqslant c_\mu d(\alpha; \mathfrak{p}_\mu). \tag{2.3}$$

Put $f = (f_1 \ldots f_m)^N$. Then $f \in \mathfrak{a}$ according to (2.1). Applying (2.2) and (2.3) we get

$$d(\alpha; f) = \min_\mu d(\alpha; f_\mu) \geqslant (\min_\mu c_\mu)(\min_\mu d(\alpha; \mathfrak{p}_\mu)) = (\min_\mu c_\mu) d(\alpha; \mathfrak{a}).$$

This means that f meets the requirements of the theorem for $c = \min_\mu c_\mu$. Hence it suffices to prove the theorem when $\mathfrak{a}$ is prime. If $\mathfrak{a}$ is principal, i.e. generated by a single element, the theorem is clearly valid with f equal to that single element and c equal to one. Thus it suffices to prove the theorem for non-principal prime ideals. In particular, this excludes the ideals (0) and (1).

3. Construction of the module M

From the two preceding sections it is clear that the theorem will be proved if, for every non-principal prime ideal $\mathfrak{p}$ of $K[x]$, we can find a module $M \subset \mathfrak{p}$ satisfying the condition of Lemma 2. For an arbitrary non-principal prime ideal $\mathfrak{p}$ we shall now construct a module M which subsequently will be shown to have the desired properties.

We adopt from algebraic geometry the convenient idea of a "universal domain" and introduce Ω as an extension field of K of infinite transcendence degree over that field and algebraically closed. Then every finitely generated extension of the field K can be isomorphically embedded as an extension within Ω. The elements of Ω will be called *quantities*. By a *generalized quantity* we shall mean an element of the set $\{\Omega, \infty\}$ where ∞ is a new element occurring as image under specializations ([5], Chap. II. § 2, p. 26).

Let $\mathfrak{p}$ be a non-principal prime ideal of $K[x]$, and let d be its dimension. We have $0 \leqslant d \leqslant n-2$ since otherwise $\mathfrak{p}$ would be principal (as to the case $d = n-1$, see [5], Prop. 10 of Chap. I, p. 7). Let $\xi = (\xi^1, \ldots, \xi^n)$ be a set of n quantities such that ξ determines the ideal $\mathfrak{p}$ over K, in other words, such that there is a natural isomorphism between $K[x]/\mathfrak{p}$ and $K[\xi]$ ([5], Chap. I, § 3, p. 6, and Chap. III, § 2, p. 48). For $j = 1, 2, \ldots, n-d-1$, let λ_j be a quantity and $\tau_j = (\tau_j^1, \ldots, \tau_j^n)$ a set of n quantities such that the set of all the λ_j and all the τ_j^i is a set of independent indeterminates over $K(\xi)$. Finally, define $\zeta = (\zeta^1, \ldots, \zeta^n)$ by

$$\zeta^i = \xi^i + \lambda_1 \tau_1^i + \cdots + \lambda_{n-d-1} \tau_{n-d-1}^i \quad (i = 1, 2, \ldots, n) \tag{3.1}$$

or, in vector notation,

$$\zeta = \xi + \lambda_1 \tau_1 + \cdots + \lambda_{n-d-1} \tau_{n-d-1}.$$

We shall prove that the ideal determined by $\{\zeta, \tau\}$ over K is generated by a single non-constant polynomial, which will be denoted by $F(z,t)$. This polynomial will form a basis for our definition of M (cf. the introduction).

In order to avoid repeating the same argument at different places, we first prove a lemma which collects some results about the specializations of $\{\xi, \lambda, \zeta, \tau\}$ over K.

By $\{\xi,\lambda,\zeta,\tau\}$ we mean the set of all the quantities ξ^i, λ_j, ζ^i, τ_j^i. The sets $\{\xi,\lambda\}$, $\{\zeta,\tau\}$ etc. are defined similarly. A set of generalized quantities is called *finite* if none of its elements is ∞, otherwise it is called *infinite*.

Lemma 3. *Let* $\{\bar\xi,\bar\lambda,\bar\zeta,\bar\tau\}$ *be a specialization of* $\{\xi,\lambda,\zeta,\tau\}$ *over* K *with* $\{\bar\zeta,\bar\tau\}$ *finite. The following five implications are true:*

(A) $\quad \{\bar\xi,\bar\lambda\}$ finite $\rightarrow \left[\begin{array}{l}\{\bar\zeta\} \text{ is not a set of independent} \\ \text{indeterminates over } K(\bar\tau).\end{array}\right.$

(B) $\quad \left.\begin{array}{l}\{\bar\xi,\bar\lambda\} \text{ finite,} \\ \bar\lambda_1, \ldots, \bar\lambda_{n-d-1} \text{ not all zero}\end{array}\right] \rightarrow \left[\begin{array}{l}\{\bar\tau\} \text{ is not a set of independent} \\ \text{indeterminates over } K(\bar\zeta).\end{array}\right.$

(C) $\quad \{\bar\xi,\bar\lambda\}$ infinite $\rightarrow \left[\begin{array}{l}\{\bar\tau\} \text{ is not a set of independent} \\ \text{intermediates over } K.\end{array}\right.$

(D) $\quad \left.\begin{array}{l}\{\bar\xi,\bar\lambda\} \text{ finite,} \\ \bar\lambda_1 = \cdots = \bar\lambda_{n-d-1} = 0\end{array}\right] \rightarrow \left[\begin{array}{l}\{\bar\xi,\bar\lambda,\bar\zeta,\bar{\bar\tau}\} \text{ is a specialization of} \\ \{\xi,\lambda,\zeta,\tau\} \text{ over } K \text{ for every finite } \{\bar{\bar\tau}\}.\end{array}\right.$

(E) $\quad \{\bar\xi,\bar\lambda\}$ infinite $\rightarrow \left[\begin{array}{l}\{\bar\xi,\bar\lambda,\bar{\bar\zeta},\bar\tau\} \text{ is a specialization of} \\ \{\xi,\lambda,\zeta,\tau\} \text{ over } K \text{ for every finite } \{\bar{\bar\zeta}\}.\end{array}\right.$

Proof. We begin with (A). Substituting $\{\bar\xi,\bar\lambda,\bar\zeta,\bar\tau\}$ for $\{\xi,\lambda,\zeta,\tau\}$ in (3.1), we see that $K(\bar\zeta,\bar\tau)\subset K(\bar\xi,\bar\lambda,\bar\tau)$. It follows that the transcendence degree of $K(\bar\zeta,\bar\tau)$ over $K(\bar\tau)$ cannot exceed that of $K(\bar\xi,\bar\lambda)$ over K, which in its turn cannot exceed that of $K(\xi,\lambda)$ over K, i.e. $n-1$. Hence the result. The proof of (B) is similar: if, say, $\bar\lambda_1 \neq 0$, the transcendence degree of $K(\bar\zeta,\bar\tau)$ over $K(\bar\zeta,\bar\tau_2,\ldots,\bar\tau_{n-d-1})$ cannot be larger than $n-1$. Also (C) is proved in essentially the same way. In this case we first extend the specialization so that it applies to all the quotients between any two non-zero elements of the set $\{\xi,\lambda\}$, and choose $\varkappa\in\{\xi,\lambda\}$ such that the quotients with this element as denominator are specialized into finite values ([5], Prop. 10 of Chap. II, p. 34). Dividing by $\varkappa$ in (3.1) and specializing, we obtain n (non-homogeneous) linear equations satisfied by the $\bar\tau_j^i$ with coefficients that are images of elements in $K(\xi,\lambda)$. None of these linear equations can vanish identically since this would mean that they all did, which is clearly impossible. The argument can therefore be continued as in the preceding cases.

The proofs of (D) and (E) depend on the obvious fact that, for each i, any $n-d-1$ of the $n-d$ elements $\zeta^i,\tau_1^i,\ldots,\tau_{n-d-1}^i$ are independent indeterminates over $K(\xi,\lambda)$, and that therefore any such $n-d-1$ elements can be specialized into arbitrary values in compatibility with any specialization of $\{\xi,\lambda\}$ over K ([5], part (a) of the proof of Theorem 6 of Chap. II, p. 30). Thus in (D) the given $\{\bar\xi,\bar\lambda\}$ together with an arbitrary finite $\{\bar{\bar\tau}\}$ forms a specialization $\{\bar\xi,\bar\lambda,\bar{\bar\tau}\}$ of $\{\xi,\lambda,\tau\}$ over K. In view of (3.1) there is only one possibility of extending that specialization of $\{\xi,\lambda,\tau\}$ to ζ, namely to specialize ζ into the same value $(=\bar\xi)$ as in the given specialization $\{\bar\xi,\bar\lambda,\bar\zeta,\bar\tau\}$. This gives the result. The proof of (E) is similar to that of (D), and the actual differences are quite analogous to those between the proof of (C) and that of (A). This finishes the proof of Lemma 3.

Let $K[z,t]$ be a polynomial ring over K where $\{z\}$ and $\{t\}$ are independent sets of variables indexed in the same way as $\{\zeta\}$ and $\{\tau\}$ respectively. We assert that the ideal in $K[z,t]$ determined by $\{\zeta,\tau\}$ is a principal ideal different from (0) and (1). This is equivalent to saying that the transcendence degree of $K(\zeta,\tau)$ over K is precisely one less than the number of elements in the set $\{\zeta,\tau\}$, i.e. $n(n-d)-1$ ([5], Prop. 10 of Chap. I, p. 7). It follows directly from our successive introduction of ξ, $\{\lambda\}$, $\{\tau\}$, ζ that the transcendence degree of $K(\xi,\lambda,\zeta,\tau)$ over K is just $n(n-d)-1$. We therefore have to prove that the set $\{\xi,\lambda\}$ is algebraic over $K(\zeta,\tau)$. Suppose the contrary! Then there is an infinite specialization of $\{\xi,\lambda\}$ over $K(\zeta,\tau)$ ([5], part (a) of the proof of Theorem 6 of Chap. II, p. 30). But since $\{\tau\}$ is a set of independent indeterminates over K, this contradicts (C) of Lemma 3, and our assertion follows. Let $F(z,t)$ be a generator of the ideal in $K[z,t]$ determined by $\{\zeta,\tau\}$. A set of quantities $\{\zeta',\tau'\}$ is then a specialization of $\{\zeta,\tau\}$ over K if and only if $F(\zeta',\tau')=0$.

The polynomial $F(z,t)$ can be written

$$F(z,t)=\sum_{\nu=1}^{N} f_\nu(z)\,\varphi_\nu(t), \tag{3.2}$$

where $f_\nu(z)\in K[z]$, $\varphi_\nu(t)\in K[t]$ ($\nu=1,2,\ldots,N$), and where each of the two sets of polynomials, $\{f_\nu(z)\}_1^N$ and $\{\varphi_\nu(t)\}_1^N$, are linearly independent over K. Let us fix such a decomposition of $F(z,t)$. We then define M as the module generated by the set $\{f_\nu(x)\}_1^N$. It is easy to see that M is uniquely determined by $\mathfrak{p}$, but we shall not use this fact.

4. Auxiliary results about $F(z,t)$ and M

Lemma 4. *The common zeros of $f_\nu(x)$ ($\nu=1,2,\ldots,N$) are precisely the finite specializations of ξ over K. The common zeros of $\varphi_\nu(t)$ ($\nu=1,2,\ldots,N$) are precisely those sets $\{\bar\tau\}$ which occur in some specialization $\{\bar\xi,\bar\lambda,\bar\zeta,\bar\tau\}$ of $\{\xi,\lambda,\zeta,\tau\}$ over K with $\{\bar\xi,\bar\lambda\}$ infinite, $\{\bar\zeta,\bar\tau\}$ finite.*

Proof. Let $\bar\zeta=(\bar\zeta^1,\ldots,\bar\zeta^n)$ be a set of quantities. We shall prove the first part of the lemma by showing successively that the following four statements are equivalent:

(i) $f_\nu(\bar\zeta)=0$ ($\nu=1,2,\ldots,N$);

(ii) $\bar\zeta$ occurs in a specialization $\{\bar\zeta,\bar\tau\}$ of $\{\zeta,\tau\}$ over K where $\{\bar\tau\}$ is a set of independent indeterminates over $K(\bar\zeta)$;

(iii) $\bar\zeta$ occurs in a finite specialization $\{\bar\xi,\bar\lambda,\bar\zeta,\bar\tau\}$ of $\{\xi,\lambda,\zeta,\tau\}$ over K with $\bar\lambda_1=\cdots=\bar\lambda_{n-d-1}=0$;

(iv) there is a specialization $\bar\xi$ of ξ over K such that $\bar\zeta=\bar\xi$.

The condition for $\{\bar\zeta,\bar\tau\}$ to be a specialization of $\{\zeta,\tau\}$ over K is $F(\bar\zeta,\bar\tau)=0$. It therefore follows directly from (3.2) that (i) implies (ii). To obtain the reverse implication we have just to observe that, as formal polynomials, the $\varphi_\nu(t)$ are linearly independent over any extension field of K, in particular over $K(\bar\zeta)$; this can be seen for instance from the fact that their independence over K means the non-vanishing of some determinant. The equivalence of (ii) and (iii) follows from (B), (C), and (D) of Lemma 3 and the extension theorem for specializations. The equivalence of (iii) and (iv) is a consequence of (3.1) and the fact that $\{\lambda,\tau\}$ is a set of independent indeterminates over $K(\xi)$.

The second part of the lemma is proved quite similarly. We assume that $\{\bar\tau\}$ is a set of quantities indexed in the same way as $\{\tau\}$, and prove the equivalence, this time using (A) and (E) of Lemma 3, of the following three statements:

(i) $\varphi_\nu(\bar{\tau}) = 0$ $(\nu = 1, 2, \ldots, N)$;
(ii) $\{\bar{\tau}\}$ occurs in a specialization $\{\bar{\zeta},\bar{\tau}\}$ of $\{\zeta,\tau\}$ over K where $\{\bar{\zeta}\}$ is a set of independent indeterminates over $K(\bar{\tau})$;
(iii) $\{\bar{\tau}\}$ occurs in a specialization $\{\bar{\xi},\bar{\lambda},\bar{\zeta},\bar{\tau}\}$ of $\{\xi,\lambda,\zeta,\tau\}$ over K with $\{\bar{\xi},\bar{\lambda}\}$ infinite, $\{\bar{\zeta},\bar{\tau}\}$ finite.

The proof is complete.

If $\{\bar{\tau}\}$ is a set of elements in K, it is clear that the polynomial $F(x,\bar{\tau}) \in K[x]$ belongs to M. To see that N such polynomials, corresponding to different sets $\{\bar{\tau}\}$, will in general generate M, we need the following

Lemma 5. *If $\{{}^k t_j^i \mid k = 1, 2, \ldots, N;\ j = 1, 2, \ldots, n-d-1;\ i = 1, 2, \ldots, n\}$ is a system of independent variables over K, consisting of N copies $\{{}^k t\}$ $(k = 1, 2, \ldots, N)$ of the set $\{t\}$, then the determinant*

$$|\varphi_\nu({}^k t)|_{\nu,\, k=1,2,\ldots,N}$$

does not vanish.

Proof. Let us show by induction on N that, if $\{\varphi_\nu(t)\}_1^N$ is any system of polynomials of $K[t]$, linearly independent over K, then the above determinant is not zero. This is clear for $N = 1$. To pass from $N-1$ to N, we expand the determinant according to the elements of the first column, thus obtaining a sum

$$\varphi_1({}^1 t)\,C_1 + \cdots + \varphi_N({}^1 t)\,C_N$$

where the cofactors $C_1, \ldots, C_N$ belong to $K[{}^2 t, \ldots, {}^N t]$. The sum cannot vanish, for the $\varphi_\nu({}^1 t)$ are linearly independent over K, hence also over $K({}^2 t, \ldots, {}^N t)$, and the C_ν are different from zero by the induction hypothesis.

5. Proof that M satisfies the condition of Lemma 2 with respect to $\mathfrak{p}$

First we note that $M \subset \mathfrak{p}$ since, by Lemma 4, ξ is a zero of $f_1, \ldots, f_N$. As $\mathfrak{p} \neq (0)$, there are real elements of K^n which are not zeros of $\mathfrak{p}$. If $\{\alpha_\mu\}_1^\infty$ denotes an arbitrary sequence of such elements, we shall determine an infinite subset J of the natural numbers and a generating system $\{g_\nu\}_1^N$ of M such that

$$\liminf_{\mu \in J} \frac{d(\alpha_\mu;\, g_\nu)}{d(\alpha_\mu;\, \mathfrak{p})} > 0 \quad (\nu = 1, 2, \ldots, N). \tag{5.1}$$

(It is understood that $\mu \to \infty$.) Obviously this will show that the condition of Lemma 2 is satisfied.

We begin by determining J. By Lemma 4 we know that, for each μ, at least one of the numbers $f_\nu(\alpha_\mu)$ $(\nu = 1, 2, \ldots, N)$ is not zero. Thus there are numbers $c_\mu \in K$ $(\mu = 1, 2, 3, \ldots)$ such that

$$\sum_{\nu=1}^{N} |c_\mu f_\nu(\alpha_\mu)| = 1.$$

We now choose J such that each of the N limits

$$d_\nu = \lim_{\mu \in J} c_\mu f_\nu(\alpha_\mu) \quad (\nu = 1, 2, \ldots, N)$$

exists. Evidently, the $d_\nu (\nu = 1, 2, \ldots, N)$ cannot all be zero. Putting

$$\phi (t) = \sum_{\nu=1}^{N} d_\nu \varphi_\nu (t), \tag{5.2}$$

we have

$$\lim_{\mu \in J} c_\mu F(\alpha_\mu; t) = \phi (t) \tag{5.3}$$

in the sense that the coefficients of the several power products in t converge separately. The polynomial $\phi(t)$ is not identically zero. This follows from (5.2) since the $\varphi_\nu(t)$ are linearly independent over K and the d_ν are not all zero.

Having determined J, we turn to the generators $g_\nu (\nu = 1, 2, \ldots, N)$. For each of the systems $\{{}^k t\}$ $(k = 1, 2, \ldots, N)$ of Lemma 5, choose values $\{{}^k \bar{\tau}\}$ in K such that

$$\det |\varphi_\nu ({}^k \bar{\tau})|_{\nu, k=1, 2, \ldots, N} \neq 0, \tag{5.4}$$

$$\phi ({}^k \bar{\tau}) \neq 0 \quad (k = 1, 2, \ldots, N). \tag{5.5}$$

Such a choice is possible since K is an infinite field. Put

$$g_k(x) = F(x, {}^k \bar{\tau}) \quad (k = 1, 2, \ldots, N).$$

The polynomials $g_k(x)$ are contained in M, and it follows readily from (5.4) that they generate M. It remains to prove that the inequalities (5.1) hold true, or, since the ordering of the sets $\{{}^k \bar{\tau}\}$ is quite arbitrary, that

$$\liminf_{\mu \in J} \frac{d(\alpha_\mu; F(x, {}^1 \bar{\tau}))}{d(\alpha_\mu; \mathfrak{p})} > 0. \tag{5.6}$$

Let us first present our argument in a more intuitive form. We assume all points, vectors etc. to be complex. Denote by D the set of those directions in n-space that can be represented by vectors that are linear combinations of ${}^1\bar{\tau}_1, \ldots, {}^1\bar{\tau}_{n-d-1}$. Call D-line every line whose direction belongs to D. It can be shown that the set of zeros of $F(x, {}^1\bar{\tau})$ consists of all D-lines which contain some zero of $\mathfrak{p}$. Combining (5.3) and (5.5) we see that, if $\{\bar{\tau}\}$ is an arbitrary set sufficiently close to $\{{}^1\bar{\tau}\}$, and if $\mu \in J$ is large enough, then $F(\alpha_\mu, \bar{\tau}) \neq 0$. This means that there is a neighbourhood N of D such that α_μ does not belong to any N-line which contains a zero of $\mathfrak{p}$, provided that $\mu > \mu_0, \mu \in J$. Thus the distance from α_μ to a D-line through a zero $\bar{\xi}$ of $\mathfrak{p}$ is never less than some fixed fraction of the distance from α_μ to $\bar{\xi}$, provided that $\mu > \mu_0, \mu \in J$. Hence the result.

Now we proceed to the formal proof of (5.6). Since $F(x, {}^1\bar{\tau}) \in \mathfrak{p}$ and since $\mathfrak{p} \neq (1)$, it follows that $F(x, {}^1\bar{\tau})$ is not a non-zero constant and that, hence, it has complex zeros. Let $\bar{\zeta}$ be a complex zero of $F(x, {}^1\bar{\tau})$. Then $\{\bar{\zeta}, {}^1\bar{\tau}\}$ is a specialization of $\{\zeta, \tau\}$ over K. Extend this specialization to a specialization $\{\xi, \lambda, \zeta, \tau\} \to \{\bar{\xi}, \bar{\lambda}, \bar{\zeta}, {}^1\bar{\tau}\}$ with $\{\bar{\xi}, \bar{\lambda}\} \subset \{K, \infty\}$ (see [5], the proof of Theorem 6 of Chap. II, pp. 30, 31). By (5.4), $\{{}^1\bar{\tau}\}$ is not a common zero of $\varphi_\nu(t)$ $(\nu = 1, 2, \ldots, N)$. On account of Lemma 4, $\{\bar{\xi}, \bar{\lambda}\}$ must therefore be finite, and by (3.1) we have the vector equation

$$\bar{\zeta} = \bar{\xi} + \bar{\lambda}_1 {}^1\bar{\tau}_1 + \cdots + \bar{\lambda}_{n-d-1} {}^1\bar{\tau}_{n-d-1}.$$

Denote by $\mathfrak{L}$ the linear subspace of K^n spanned by the vectors ${}^1\bar{\tau}_1, \ldots, {}^1\bar{\tau}_{n-d-1}$. From the above expression for $\bar{\zeta}$ it follows that

$$d(\alpha_\mu; F(x, {}^1\bar\tau)) = \inf_{\bar\xi, \bar\eta} \| \alpha_\mu - \bar\xi - \bar\eta \|,$$

where $\bar\xi \in K^n$ is a specialization of ξ over K, and $\bar\eta \in \mathfrak{L}$. It is then obvious that the fraction in the left hand side of (5.6) is not less than

$$\inf_{\bar\xi, \bar\eta} \frac{\| \alpha_\mu - \bar\xi - \bar\eta \|}{\| \alpha_\mu - \bar\xi \|},$$

or, since $\mathfrak{L}$ is linear,

$$\inf_{\bar\xi, \bar\eta} \left\| \frac{\alpha_\mu - \bar\xi}{\| \alpha_\mu - \bar\xi \|} - \bar\eta \right\|, \tag{5.7}$$

where, as before, $\bar\xi \in K^n$ is a specialization of ξ over K, and $\bar\eta \in \mathfrak{L}$.

It now suffices to prove that the expression (5.7) is larger than some positive constant if $\mu \in J$ is large enough. To do this we shall show that there are an integer μ_0 and a closed set $\mathfrak{F}$ of K^n such that

$$\frac{\alpha_\mu - \bar\xi}{\| \alpha_\mu - \bar\xi \|} \in \mathfrak{F} \quad \text{if } \mu > \mu_0,\ \mu \in J, \tag{5.8}$$

$$\mathfrak{F} \cap \mathfrak{L} \text{ is empty,} \tag{5.9}$$

where, in (5.8), $\bar\xi$ ranges over all specializations of ξ over K which lie in K^n. Then, for $\mu > \mu_0, \mu \in J$, the expression (5.7) will not be less than the distance between the closed and disjoint sets $\mathfrak{F}$ and $\mathfrak{L}$.

Denote by $\{\bar\tau\}$ a variable system of values in K indexed in the same way as $\{\tau\}$. By (5.3) and (5.5) we can find $\delta > 0$ and an integer μ_0 such that,

if

$$\mu > \mu_0,\ \mu \in J,$$

$$|\bar\tau_j^i - {}^1\bar\tau_j^i| < \delta \quad (j = 1, 2, \ldots, n-d-1;\ i = 1, 2, \ldots, n), \tag{5.10}$$

then

$$F(\alpha_\mu, \bar\tau) \neq 0. \tag{5.11}$$

We define $\mathfrak{F}$ as the set of all vectors of unit norm in K^n which cannot be written as linear combinations of any system of $n-d-1$ vectors $\bar\tau_1, \ldots, \bar\tau_{n-d-1}$ satisfying (5.10).

$\mathfrak{F}$ is closed. For let γ be a vector of K^n not in $\mathfrak{F}$. Then either $\|\gamma\| \neq 1$ or

$$\gamma = \bar\lambda_1 \bar\tau_1 + \cdots + \bar\lambda_{n-d-1} \bar\tau_{n-d-1}$$

with $\{\bar\tau\}$ satisfying (5.10) and $\bar\lambda_j \neq 0$ for at least one value of j. Suppose that $\bar\lambda_1 \neq 0$. Then by varying $\bar\tau_1$ within the limits determined by (5.10) we obtain a neighbourhood of γ which does not belong to $\mathfrak{F}$. This shows that the complement of $\mathfrak{F}$ in K^n is open.

If (5.8) were false, then for some $\mu > \mu_0$, $\mu \in J$, and some $\bar\xi$, we could write $\alpha_\mu - \bar\xi$ as a linear combination of vectors $\bar\tau_1, \ldots, \bar\tau_{n-d-1}$ satisfying (5.10):

$$\alpha_\mu = \bar\xi + \bar\lambda_1 \bar\tau_1 + \cdots + \bar\lambda_{n-d-1} \bar\tau_{n-d-1}.$$

Then, evidently, $\{\bar\xi, \bar\lambda, \alpha_\mu, \bar\tau\}$ would be a specialization of $\{\xi, \lambda, \zeta, \tau\}$ over K so that in particular $F(\alpha_\mu, \bar\tau) = 0$. But this contradicts (5.11), and so (5.8) must be true.

The validity of (5.9) is an immediate consequence of the definition of $\mathfrak{F}$.

The proof that M satisfies the condition of Lemma 2 with respect to $\mathfrak{p}$ is thus complete, hence also the proof of the theorem.

REFERENCES

1. Hörmander, L., On the theory of general partial differential operators. Acta Math. *94* (1955), 161–248.
2. —— Differentiability properties of solutions of systems of differential equations. Ark. mat. *3*. (1958) 527–535.
3. Northcott, D. G., Ideal theory. Cambridge Tracts in Math. and Math. Phys. *42*. Cambridge, 1953.
4. van der Waerden, B. L., (Moderne) Algebra II. E.g. 3rd ed., Berlin 1955.
5. Weil, A., Foundations of Algebraic Geometry. New York, 1946.

Tryckt den 27 november 1958

Uppsala 1958. Almqvist & Wiksells Boktryckeri AB