ON THE METAMATHEMATICS OF RINGS AND INTEGRAL DOMAINS

BY
BRUNO SCARPELLINI

Introduction. In this paper we are concerned with the metamathematics of the first order theory of rings R_0 and integral domains JD_0. The purpose of the paper is to characterize derivability from R_0 and JD_0 respectively by algebraic notions pertaining to the theory of polynomial ideals. The essential tool from logic needed is an improved version of Gentzen's extended Hauptsatz to be derived in §I. §§II and III contain some remarks and introduce new notations. In §IV we prove a syntactical counterpart of Hilbert's Nullstellensatz. Although this syntactical result could easily be proved with the aid of Hilbert's Nullstellensatz and the completeness theorem we think that its metamathematical proof has some interest in itself (see Lemma 4*). In §V we combine the results of §§I and IV in order to prove an algebraic version of Gentzen's extended Hauptsatz for R_0 and JD_0. Applications of the techniques developed in §§I–IV are presented in §§VI and VII. Lemma 4*, a constructive version of Lemma 4, has been suggested by G. Kreisel. There is an interesting application of Lemma 4* to a problem considered by G. Kreisel. This application lies somewhat outside the scope of this paper, hence we omit it. It will be presented, together with some related topics, in a separate note.

NOTATIONS. (1) By $\boldsymbol{I}$ and $\boldsymbol{R}$ we denote the set of integers and the set of rationals respectively. $\boldsymbol{I}[x_1, \ldots, x_n]$ and $\boldsymbol{R}[x_1, \ldots, x_n]$ (or briefly $\boldsymbol{I}[\mathbf{x}]$, $\boldsymbol{R}[\mathbf{x}]$) are the rings of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\boldsymbol{I}$ and $\boldsymbol{R}$ respectively. Notions such as prime ideal, primary decomposition, basis of an ideal will be used frequently. For details concerning them we refer to [4].

(2) At many places, vectors whose components are terms (from a certain theory) will be used. For particular vectors such as $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_m)$ we will use sometimes the abbreviations $\mathbf{x}_n$, $\mathbf{x}$ and $\mathbf{y}_m$, $\mathbf{y}$.

(3) Let $g_1, \ldots, g_n$ be polynomials in $R[\mathbf{x}]$; by $\boldsymbol{B}(g_1, \ldots, g_n)$ we denote the ideal consisting of all polynomials of the form $\sum_1^n h_i g_i$ with $h_i \in \boldsymbol{R}[\mathbf{x}]$ for $i \leqq n$. If $g_1, \ldots, g_n \in \boldsymbol{I}[\mathbf{x}]$ then $\boldsymbol{B}^*(g_1, \ldots, g_n)$ denotes the ideal consisting of all polynomials $\sum_1^n h_i g_i$ with $h_i \in \boldsymbol{I}[\mathbf{x}]$ for $i \leqq n$. Several notations will be introduced as they will be needed, as, e.g. at the end of §III.

(4) Existential and universal quantifiers will be denoted by $\exists$ and $\forall$ respectively but in order to save space we delete the $\forall$ in formulas and write universal quantification over x more simply as (x); at some places a sequence of universal quantifiers

Received by the editors April 3, 1967 and, in revised form, January 5, 1968.

will be abbreviated as $(x_1, \ldots, x_n)$ or even more simply as $(\mathbf{x}_n)$ or $(\mathbf{x})$. Quantifiers will also be denoted by such symbols as P, Q, P_k^i, Q_k^i, etc.

(5) Formulas in prenex normal form will often be denoted by notations as, e.g. $(Q_1x_1, \ldots, Q_sx_s)A(x_1, \ldots, x_s)$; here the Q_i's denote quantifiers while $A(x_1, \ldots, x_s)$ is assumed to contain no quantifiers. We call $(Q_1x_1, \ldots, Q_sx_s)$ the prefix of the formula and $A(x_1, \ldots, x_s)$ the quantifier-free part of the formula (the notion "matrix" will be used otherwise.

(6) Conjunctions or disjunctions over formulas A_i or A_{ij} $(i \leqq n, j \leqq m_i)$ will be written as $\bigwedge_{i=1}^n A_i$ or in general more briefly $\bigwedge_i A_i$ and similarly $\bigvee_{i=1}^n A_i$, $\bigvee_i A_i$, $\bigwedge_{ij} A_{ij}$, $\bigvee_{ij} A_{ij}$. The sign $\rightarrow$ is the arrow of sequential calculus; implication is denoted by $\supset$. The greek symbols Γ, Δ, Σ, Π appearing in sequents (such as, e.g. $\Gamma \rightarrow \Delta$ or $A, \Gamma \rightarrow \Delta$) denote sequences of formulas. In connection with sentential calculus we adopt quite generally the notation used in [3]. The symbol $\prod$ is used in connection with products over many factors: $\prod_i A_i$, $\prod_{ij} A_{ij}$.

I. **A sharpening of Gentzen's extended Hauptsatz.** For use in later sections it is necessary to have available a sharpening of Gentzen's extended Hauptsatz referred to in the sequel as GEH. The result in question will be given below but we will content ourself with a rather condensed form of the proof; the parts omitted do not involve any difficult point, however they would have increased the size of the paper considerably.

We start by introducing some notions. A proof of GEH is given in [3, p. 448], and the notion of pure variable proof is introduced in [3, p. 451]. A prenex formula is said to have standard form or to be a standard prenex formula if

(1) no variable occurs free and bound in it,

(2) every bound variable occurs exactly once in the prefix,

(3) every bound variable occurs explicitly in the quantifier-free part. We denote such a formula, e.g. by $(Q_1x_1, \ldots, Q_sx_s)A(x_1, \ldots, x_s)$ where the Q_i's are quantifiers, the x_k's distinct variables and $A(x_1, \ldots, x_s)$ a quantifier-free formula. Other, similar notations will be used. A proof in the sentential calculus $G1$ is called a standard proof if it satisfies the following requirements:

(1) it is a cut free proof and has the properties of the proofs described by GEH,

(2) its end-sequent contains only closed prenex standard formulas,

(3) every free variable in the proof occurs at least once (and hence exactly once) as the variable to which one of the rules $\exists \rightarrow$, $\rightarrow \forall$ is applied.

We assume that at least one individual constant is contained in the language under consideration. Using this it is easy to show that every sequent of closed prenex standard formulas which is provable at all is provable by means of a standard proof. A further notion needed is that of the final part of a standard proof: it is that part of the proof whose first sequent is the midsequent and which ends with the endsequent. We denote the final part of a standard proof P by $S_1, \ldots, S_n$, i.e. S_1 is the midsequent of P, S_n the endsequent and S_{i+1} follows from S_i by means of

thinning, contraction, interchange or a quantifier rule. From the subformula property it follows that a standard proof contains only standard prenex formulas. Now we come to some definitions.

DEFINITION 1. Let C_L be the relation defined for pairs of formulas such that $C_L(F, H)$ iff

(a) F is $(x)G(x)$ and H is $G(t)$ for some term t, or

(b) F is $(Ex)G(x)$ and H is $G(y)$ for some variable y free for x.

The relation C_R is defined similarly but with the roles of existential and universal quantifiers interchanged.

By C_L^* and C_R^* we denote the closures of C_L and C_R respectively, that is $C_L^*(F, H)$ holds iff there is a list $F_0, \ldots, F_n$ with $F=F_0$, $H=F_n$ and $C_L(F_i, F_{i+1})$; the relation C_R^* is defined similarly. We note: if F is $(Q_1x_1, \ldots, Q_sx_s)A(x_1, \ldots, x_s)$ with A quantifier-free and containing exactly $x_1, \ldots, x_s$ as free variables, if $C_L^*(F, H)$ or $C_R^*(F, H)$ then H has the form $(Q_{j+1}x_{j+1}, \ldots, Q_sx_s)A(t_1, \ldots, t_j, x_{j+1}, \ldots, x_s)$ for some terms $t_1, \ldots, t_j$ and some $j \geqq 0$. All sequents to be considered below will be assumed to contain only standard prenex formulas.

DEFINITION 2. A function ψ is said to connect the sequent S' with the sequent S if it maps the formulas of S' into formulas of S such that

(a) $\psi(A)$ is in the antecedent of S iff A is in the antecedent of S',

(b) $C_L^*(\psi(A), A)$ or $C_R^*(\psi(A), A)$ according to whether A is in the antecedent or succedent of S'.

Let $S_1, \ldots, S_n$ be the final part of a standard proof P. In connection with the subformula property of cut free proofs one can associate with each pair S_i, S_{i+1} in a natural way a map ψ_{i+1}^i which connects S_i with S_{i+1}. Consider, e.g., the case where S_i and S_{i+1} are $\Gamma \to \Delta_1B_1B_2\Delta_2$ and $\Gamma \to \Delta_1B_2B_1\Delta_2$ respectively:

(1) if A is in Γ or in Δ_j then $\psi_{i+1}^i(A)$ is the corresponding A in Γ or Δ_j of S_{i+1},

(2) if A is B_j then $\psi_{i+1}^i(A)$ is the corresponding B_j in S_{i+1}.

How to define ψ_{i+1}^i in case of the other inferences should be obvious. Now maps ψ_i connecting S_i with S_n are defined inductively as follows:

$$\psi_{n-1} = \psi_n^{n-1}, \tag{1}$$

$$\psi_i = \psi_{i+1}^i \circ \psi_{i+1} \quad \text{for } i < n-1 \text{ (where } (f \circ g)(x) = f(g(x))). \tag{2}$$

That ψ connects S_{n-i} with S_n is easily proved by induction with respect to i. Let $A(x_1, \ldots, x_s)$ be a quantifier-free formula whose free variables are precisely $x_1, \ldots, x_s$ and let H be $(Q_{j+1}x_{j+1}, \ldots, Q_sx_s)A(t_1, \ldots, t_j, x_{j+1}, \ldots, x_s)$ with t_i terms. A term t is said to occupy the kth place of H if $k \leqq j$ and $t=t_k$. It is easy to show that two different terms cannot occupy the same place of H. In the following definition ψ connects S' with S, where S is supposed to contain only prenex closed standard formulas. A relation R (depending on S, S' and ψ) whose domain are triples (H, y, k) with H a formula in S', y a variable, k an integer >0, is introduced in

DEFINITION 3. Let $\psi(H)$ be $(Q_1x_1, \ldots, Q_sx_s)A(x_1, \ldots, x_s)$ with A quantifier-free and containing exactly $x_1, \ldots, x_s$ as free variables. Then $R(H, y, k)$ holds iff y occupies the kth place in H and if either

(a) H is in the antecedent of S' and Q_k is $\exists$ or

(b) H is in the succedent of S' and Q_k is $\forall$.

If we consider the final part of a standard proof $S_1, \ldots, S_n$ and if $\psi = \psi_i$, $S' = S_i$, $S = S_n$ then the relation R just introduced is denoted by R_i. In the Definitions 4 and 5 below the symbols ψ, S', S, H and R have the same meaning as in Definition 3.

DEFINITION 4. The relation e (depending on ψ, S', S) has as its domain the pairs (y_1, y_2) of free variables occurring in S'. Moreover $e(y_1, y_2)$ is true iff the following holds: there is a formula H in S', a term t and integers n, m such that

(a) $n < m$,

(b) the term t occupies the nth place of H and contains y_1 explicitly,

(c) the relation R applies to (H, y_2, m), that is $R(H, y_2, m)$ holds.

In case of the final part of a standard proof $S_1, \ldots, S_n$ we denote the relation e associated with S_i, S_n and ψ_i by e_i. The last definition needed is

DEFINITION 5. Two formulas F, G in S' are called congruent with respect to $k \geqq 1$ (expressed by $F \underset{k}{\sim} G$) iff

(a) $\psi(F) = \psi(G)$,

(b) there is a list of terms $t_1, \ldots, t_{k-1}$ such that t_i occupies the ith place of both F and G $(i \leqq k-1)$.

In case $k = 1$ the condition (b) is vacuous. Although Definitions 3–5 are somewhat cumbersome they express simple syntactic situations. Call a sequent S' a propositional identity if it contains only quantifier-free formulas and if it is provable from the propositional part of $G1$ alone.

THEOREM 1. *Let S be a sequent of closed prenex standard formulas. Then S is provable from $G1$ iff there is a propositional identity S' and a function ψ which connects S' with S such that the following holds:*

(a) *for each free variable y occurring in S' there is a formula H in S' and an integer $k > 0$ such that $R(H, y, k)$ holds,*

(b) *if there is a variable y and formulas F, G in S' such that $R(F, y, k)$ and $R(G, y, j)$ for some k, j then $\psi(F) = \psi(G)$, $k = j$ and $F \underset{k}{\sim} G$,*

(c) *there are no y_i $(i \leqq n)$ such that $e(y_1, y_n)$ and $e(y_{i+1}, y_i)$ for all $i < n$.*

Proof. We do not give the proof in full detail but restrict ourself to discuss the main points.

(a) If $G1 \vdash S$ then there is a standard proof of S with final part S_i $(i \leqq n)$ where $S = S_n$. One shows by induction with respect to i that (a)–(c) above are satisfied with respect to ψ_{n-i}, S_{n-i}, S_n. Since S_1 is a propositional identity the statement follows by putting $i = n-1$. The induction is straightforward and will be omitted.

(b) In order to prove the converse we prove a slightly more general statement in which S' is allowed to be an arbitrary sequent of prenex standard formulas:

if ψ connects S' with S such that (a)–(c) are satisfied, then S is provable from S' by means of quantifier and structural rules (without cut) alone. The proof is by induction with respect to the number of free variables occurring in S'.

Case 1. Let S' contain no free variables and denote by $d(S')$ the number of formulas F in S' for which $F \neq \psi(F)$. If $d(S')$ is zero there is nothing to prove. Let $d(S') > 0$ and assume, e.g., S' to be F, $\Gamma \to \Delta$ such that F and $\psi(F)$ are

$$(Q_{j+1}x_{j+1}, \ldots, Q_s x_s)A(t_1, \ldots, t_j, x_{j+1}, \ldots, x_s)$$

and $(Q_1 x_1, \ldots, Q_s x_s)A(x_1, \ldots, x_s)$ respectively with $j \geqq 1$ and A quantifier-free. We claim: $Q_\alpha = \forall$ for $\alpha \leqq j$. If $Q_k = \exists$ for some $k \leqq j$ then by Definitions 1 and 2 and the fact that ψ connects S' with S, a free variable y would occupy the kth place in F, contradicting the assumption. Thus applying j times the rule $\forall \to$ we obtain the sequent $S'' = \psi(F)$, $\Gamma \to \Delta$ which is obviously still connected with S by a suitably modified ψ_0 and for which $d(S'') < d(S')$. Hence an induction with respect to $d(S')$ yields the statement.

Case 2. S' contains free variables. For notational purposes we discuss a special case which however contains all the difficulties of the general case. From (c) it follows that there is a free variable y maximal with respect to e that is such that for no other y' we have $e(y, y')$. A preparatory step is needed in case S' contains formulas F with the following property P: the y occurs free in F but there is no k with $R(F, y, k)$. Assume for simplicity that there is just one such F and that S' has the form $F, \Gamma \to \Delta$. Let F and $\psi(F)$ be $(Q_{j+1}x_{j+1}, \ldots, Q_s x_s)A(t_1, \ldots, t_j, x_{j+1}, \ldots, x_s)$ and $(Q_1 x_1, \ldots, Q_s x_s)A(x_1, \ldots, x_s)$ respectively; let furthermore t_k be the first term from the left in the list $t_1, \ldots, t_j$ which contains y explicitly. We claim $Q_\alpha = \forall$ for $k \leqq \alpha \leqq j$. Clearly $Q_k = \forall$ since otherwise $R(F, y, k)$, contradicting the assumption. If $Q_\beta = \exists$ for a β with $k < \beta \leqq j$ then $t_\beta = y'$ for some y' and hence $R(F, y', \beta)$; but according to Definition 4 this would imply $e(y, y')$, contradicting the maximality of y. Hence by applying $\forall \to$ a number of times to S' we arrive at a sequent S'' of the form $F', \Gamma \to \Delta$ with $F' = (Q_k x_k, \ldots, Q_s x_s)A(t_1, \ldots, t_{k-1}, x_k, \ldots, x_s)$ which does not contain any formula with property P, but which is still connected with S by means of a function ψ_0, the latter being easily obtained from S', S and ψ. The case where S' contains several formulas with property P is handled similarly. Hence we may assume that there is no F in S' with property P.

According to (a) of the theorem there is a U in S' and a k such that $R(U, y, k)$. Assume for simplicity that there is just one other formula V in S' and a j such that $R(V, y, j)$; from (b) of the theorem we obtain $k = j$. Since $\psi(U) = \psi(V)$ by (b), both U, V are on the same side of the arrow; hence let, e.g., S' be $U, V, \Gamma \to \Delta$. Let U, V and $\psi(U)$ be

$$(Q_{n+1}x_{n+1}, \ldots, Q_s x_s)A(t_1, \ldots, t_{k-1}, y, t_{k+1}, \ldots, t_n, x_{n+1}, \ldots, x_s),$$

$$(Q_{m+1}x_{m+1}, \ldots, Q_s x_s)A(t_1, \ldots, t_{k-1}, y, t'_{k+1}, \ldots, t'_m, x_{m+1}, \ldots, x_s),$$

and

$$(Q_1 x_1, \ldots, Q_s x_s)A(x_1, \ldots, x_s)$$

respectively (this notation takes into account that $U \underset{k}{\sim} V$ as implied by (b)). As before $Q_\alpha = \exists$ is excluded for $k+1 \leqq \alpha \leqq \max(n, m)$ since otherwise $t_\alpha = y'$ or $t'_\alpha = y'$ for some y' and hence $e(y, y')$ thus contradicting the maximality of y. Therefore by some applications of $\forall \rightarrow$, interchange and contraction we arrive at a sequent S'' of the form $(Q_{k+1}x_{k+1}, \ldots, Q_s x_s)A(t_1, \ldots, t_{k-1}, y, x_{k+1}, \ldots, x_s), \Gamma \rightarrow \Delta$.

In addition there is no t_i $(1 \leqq i \leqq k-1)$ containing y since this would contradict the maximality of y. This means that S'' satisfies the restriction of variables with respect to y and so we are allowed to apply $\exists \rightarrow$ to S''. The result is a sequent S^* which contains one free variable less than S' and which is still connected with S by means of a ψ^* in such a way as to satisfy (a)–(c) of the theorem; the function ψ^* is constructed in an obvious way from S', S and ψ.

There is a sharpening of Theorem 1, namely

THEOREM 2. *Let S be as in Theorem 1. Then $G1 \vdash S$ iff there is a propositional identity S' and a function ψ which connects S' with S such that* (a)–(c) *of Theorem 1 and in addition the following condition* (d) *are satisfied*: if U, V, y, y' *and* k *are such that* $\psi(U) = \psi(V)$, $R(U, y, k)$ *and* $R(V, y', k)$ *then* y *and* y' *are the same.*

We omit the detailed proof in favor of an outline. If (a)–(d) are satisfied then in particular (a)–(c), hence $G1 \vdash S$ by Theorem 1. Assume $G1 \vdash S$. Then by Theorem 1 there is a propositional identity $S' = F_1, \ldots, F_n \rightarrow G_1, \ldots, G_m$ and a ψ such that (a)–(c) of Theorem 1 are satisfied by S, S' and ψ. Write $y \equiv y'$ if $y \neq y'$ and if there are U, V and a k such that $\psi(U) = \psi(V)$, $R(U, y, k)$ and $R(V, y', k)$. Assume $y \equiv y'$. If we replace every occurrence of y' in S' by y then we obtain a new sequent $S^* = F'_1, \ldots, F'_n \rightarrow G'_1, \ldots, G'_m$. Define a function ψ^* on S^* by putting $\psi^*(F'_1) = \psi(F_i)$. Obviously ψ^* connects S^* with S. We want to show that ψ^*, S^* and S satisfy (a)–(c) of Theorem 1. The verification of (a) and (b) is rather easy. Let e^* be the relation associated with ψ^*, S^*, S according to Definition 4. Making use of (b) and (c) one verifies that there is no list $y_0, \ldots, y_p$ with $y_0 = y$, $y_p = y'$ such that $e(y_i, y_{i+1})$ for $1 < p$. This in turn implies that e^* satisfies (c) of Theorem 1. The verification of these two points presents no difficulties. Proceeding this way we arrive after finitely many steps at a sequent S_0 and a function ψ_0 such that

(1) ψ_0 connects S_0 with S,

(2) conditions (a)–(c) of Theorem 1 are satisfied,

(3) there are no y, y' in S_0 such that $y \equiv y'$.

But (3) means that (d) of Theorem 2 is satisfied.

A very special case of Theorem 2 is the following

COROLLARY 1. *Let the closed prenex standard formulas F_i $(i \leqq s)$ and G be $(x_1, \ldots, x_{n(i)})A(x_1, \ldots, x_{n(i)})$ and $(y_1, \ldots, y_p)B(y_1, \ldots, y_p)$ respectively where A and B are quantifier-free. Then $G1 \vdash F_1, \ldots, F_s \rightarrow G$ iff there are terms $t^i_{\alpha k}$ $(k \leqq n(i)$, $\alpha \leqq m(i))$ containing no other variables than $y_1, \ldots, y_p$ such that $\bigwedge_{i,\alpha} A(t^i_{\alpha 1}, \ldots, t^i_{\alpha n(i)}) \rightarrow B(y_1, \ldots, y_p)$ is a propositional identity.*

The proof follows easily from Theorem 2 by specialization, but of course one could prove the statement directly from GEH without making the detour via the complex Theorem 2.

II. A convenient notation and some remarks.

1. Let $q(x_1, \ldots, x_s)$ and $A(x_1, \ldots, x_s)$ be a term and a quantifier-free formula respectively, whose free variables are among $x_1, \ldots, x_s$. Let an ordered s-tuple $\boldsymbol{v}=(t_1, \ldots, t_s)$ of terms be given; we call such an s-tuple briefly a vector. If we replace x_i by t_i (for all $i \leqq s$) in q and in A respectively we obtain new expressions $q(t_1, \ldots, t_s)$ and $A(t_1, \ldots, t_s)$ which will also be denoted by $q[\boldsymbol{v}]$ and $A[\boldsymbol{v}]$ respectively. Let F be the closed prenex standard formula $(Q_1x_1, \ldots, Q_sx_s)A(x_1, \ldots, x_s)$ with A quantifier-free containing precisely $x_1, \ldots, x_s$ free. A vector $\boldsymbol{v}=(t_1, \ldots, t_n)$ is called a left-vector of F if $n=s$ and if $C_L^*(F, A[\boldsymbol{v}])$ holds, with C_L^* introduced in connection with Definition 1. Similarly $\boldsymbol{v}$ is called a right-vector of F if $C_R^*(F, A[\boldsymbol{v}])$ holds. By a left-matrix of F we understand a finite set (possibly empty) $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s\}$ of left-vectors of F and by a right-matrix of F a finite set of right-vectors of F. Matrices will be denoted by such symbols as M, M', M_i, etc. A finite set of vectors, all having the same number of components, will be briefly called a matrix. We say that M is a matrix in $y_1, \ldots, y_s$ if every term which appears as component of some $\boldsymbol{v} \in M$ contains only variables from $y_1, \ldots, y_s$.

Consider two sequences $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$ of closed prenex standard formulas, F_i and G_k having $A_i(x_1, \ldots, x_{s_i})$ and $B_k(x_1, \ldots, x_{t_k})$ as its quantifier-free parts respectively. Assume that for $i \leqq s$ and $k \leqq t$ we are given a left-matrix $M_i = \{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i\alpha_i}\}$ of F_i and a right-matrix $M_k' = \{\boldsymbol{w}_{k1}, \ldots, \boldsymbol{w}_{k\beta_k}\}$ of G. Now we introduce two sequents S, S' and a map ψ as follows:

(1) S is $F_1, \ldots, F_s \rightarrow G_1, \ldots, G_t$,

(2) the antecedent of S' contains precisely those formulas F which are of the form $A_i[\boldsymbol{v}_{ij}]$ where M_i is not empty,

(3) the succedent of S' contains precisely those formulas F which are of the form $B_k[\boldsymbol{w}_{kj}]$ where M_k' is not empty,

(4) $\psi(A_i[\boldsymbol{v}_{ij}]) = F_i$, $\psi(B_k[\boldsymbol{w}_{kj}]) = G_k$.

It is clear from the definition of left- and right-matrix that ψ connects S' with S. In the following definition S, S', ψ, F, G, M, M' are the same as above.

DEFINITION 6. The two lists of matrices $M_1, \ldots, M_s$ and $M_1', \ldots, M_t'$ are said to satisfy condition E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$ if ψ, S' and S introduced above satisfy (a)–(c) of Theorem 1 and (d) of Theorem 2. They are said to satisfy condition E^* with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$ if ψ, S' and S satisfy (b) and (c) of Theorem 1 and (d) of Theorem 2.

REMARK. If $s=0$ or if all M_i are empty then we simply say that $M_1', \ldots, M_t'$ satisfy E (or E^*) with respect to $G_1, \ldots, G_t$ since it will always be clear from the context that the formulas denoted here by G_i will be on the right side of the arrow.

If we use the fact that $\bigwedge_i^s U_i \supset \bigvee_k^t W_k$ is provable in ordinary predicate calculus

iff $U_1, \ldots, U_s \to W_1, \ldots, W_k$ is provable in $G1$ then we can rephrase Theorem 2 with the aid of our new terminology as follows

THEOREM 2*. *Let $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$ be two lists of closed standard prenex formulas, F_i and G_k having $A_i(x_1, \ldots, x_{s_i})$ and $B_k(x_1, \ldots, x_{t_k})$ respectively as quantifier-free part. The formula $\bigwedge_i F \supset \bigvee_k G_k$ is provable in ordinary predicate calculus iff there are two lists of matrices $M_i = \{v_{i1}, \ldots, v_{i\alpha_i}\}$ and $M'_k = \{w_{k1}, \ldots, w_{k\beta_k}\}$ $(i \leqq s, k \leqq t)$ such that*

(a) *M_i is a left-matrix of F_i and M'_k a right-matrix of G_k,*

(b) *the lists $M_1, \ldots, M_s$ and $M'_1, \ldots, M'_k$ satisfy E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$,*

(c) *the formula $\bigwedge_{i,j} A_i[v_{ij}] \supset \bigvee_{k,j} B_k[w_{kj}]$ is a tautology of propositional calculus.*

In this form the theorem makes no allusions to sentential calculus. Of course conditions (a)–(d) involved in E make use of the relations R and e associated with ψ, S', S introduced above; hence the notion of sequence is used in their definitions. But it is clear that this use of sequent has nothing to do with sentential calculus since the arrow appearing in a sequent turns out to be merely a syntactical aid to distinguish between left and right. Once given $F_1, \ldots, F_s$, $G_1, \ldots, G_t$ and $M_1, \ldots, M_s$, $M'_1, \ldots, M'_t$ we could consider the two lists $A_i[v_{ij}]$ and $B_k[w_{kj}]$ and then rephrase the Definitions 3 and 4 so as to make no use of S', S and ψ.

LEMMA 1. (a) *Let F_i, G_k $(i \leqq s, k \leqq t)$ be as in Theorem 2* and let the matrices M_i, M'_k $(i \leqq s, k \leqq t)$ be left- and right-matrices of F_i and G_k respectively. Let furthermore $M_1, \ldots, M_s$ and $M'_1, \ldots, M'_t$ satisfy E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$. If $\overline{M}_i$ and $\overline{M}'_k$ $(a \leqq i \leqq s, b \leqq k \leqq t)$ are such that $\overline{M}_i \subseteq M_i$ and $\overline{M}'_k \subseteq M'_k$ then $\overline{M}_a, \ldots, \overline{M}_s$ and $\overline{M}'_b, \ldots, \overline{M}'_t$ satisfy E* with respect to $F_a, \ldots, F_s$ and $G_b, \ldots, G_t$.*

(b) *If in particular $F_1, \ldots, F_n$ are purely universal $(n \leqq s)$, that is if F_i is $(x_1, \ldots, x_{n_i}) \cdot A_i(x_1, \ldots, x_{n_i})$, then $M_{n+1}, \ldots, M_s$ and $\overline{M}'_1, \ldots, \overline{M}'_t$ still satisfy E with respect to $F_{n+1}, \ldots, F_s$ and $G_1, \ldots, G_t$.*

LEMMA 2. *Let F_i, G_k $(i \leqq s, k \leqq t)$ be as in Theorem 2* and let M_i, M'_k $(i \leqq s, k \leqq t)$ be left- and right-matrices of F and G respectively. Assume that M_i and M'_k are matrices in $y_1, \ldots, y_n$ for all $i \leqq s$, $k \leqq t$. If $M_1, \ldots, M_s$ and $M'_1, \ldots, M'_t$ satisfy E* with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$ then there is a subset $y_{\alpha_1}, \ldots, y_{\alpha_m}$ such that for any constant c the following holds: if we replace in M_i and M'_k all $y_{\alpha_1}, \ldots, y_{\alpha_m}$ by c then the resulting lists $\overline{M}_1, \ldots, \overline{M}_s$ and $\overline{M}'_1, \ldots, \overline{M}'_t$ satisfy E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$.*

The proofs of Lemmas 1 and 2 follow directly from Definitions 3, 4 and 6 and will be omitted.

2. Let $\{F_1, \ldots, F_s, G_1, \ldots, G_t\}$ and S be two sets of closed prenex standard formulas. It is easy to verify that the proof of Theorem 1 (in particular part (b)) combined with Definition 6 yields the following statement: if $M_i = \{v_{i\alpha}\}$ and M_k

$=\{w_{k\beta}\}$ $(i \leqq s, k \leqq t)$ are matrices which satisfy (a) and (b) of Theorem 2* with respect to F_i and G_k, if in addition $S \vdash \bigwedge_{i,\alpha} A_i[v_{i\alpha}] \supset \bigvee_{k\beta} B_k[w_{k\beta}]$ then $S \vdash \bigwedge_i F_i \supset \bigvee_k G_k$. The converse of this statement is in general not true as counterexamples (number theory) show. However

THEOREM 3. *Let S be a set of closed prenex standard formulas, all having the form $(x_1, \ldots, x_n)D(x_1, \ldots, x_n)$, D quantifier-free; let F_i, G_k $(i \leqq s, k \leqq t)$ be closed prenex standard formulas having $A_i(x_1, \ldots, x_{s_i})$ and $B_k(x_1, \ldots, x_{t_k})$ as quantifier-free parts respectively. Then $S \vdash \bigwedge_i F_i \supset \bigvee_k G_k$ iff there are matrices $M_i = \{v_{i\alpha}\}$, $M'_k = \{w_{k\beta}\}$, $(i \leqq s, k \leqq t)$ such that*

(a) *M_i and M'_k are left- and right-matrices of F_i and G_k respectively,*

(b) *$M_1, \ldots, M_s$ and $M'_1, \ldots, M'_t$ satisfy the condition E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$,*

(c) $S \vdash \bigwedge_{i,\alpha} A_i[v_{i\alpha}] \supset \bigvee_{k,\beta} B_k[w_{k\beta}]$.

The proof, being an immediate consequence of the definitions, will only be outlined.

Proof. One half of the statement is settled by the remark preceding Theorem 3. In order to prove the other half, assume $S \vdash \bigwedge_i F_i \supset \bigvee_k G_k$. Then $\vdash \bigwedge_i F_i \wedge \bigwedge_j H_j \supset \bigvee_k G_k$ for some formulas $H_1, \ldots, H_p$ belonging to the set S. Let H_j be $(x_1, \ldots, x_{p_j}) \cdot D_j(x_1, \ldots, x_{p_j})$. By Theorem 2* there are matrices $N_j = \{u_{j\alpha}\}$, $M_i = \{v_{i\beta}\}$, $M'_k = \{w_{k\gamma}\}$ $(j \leqq p, i \leqq s, k \leqq t)$ with the following properties:

(a) N_j and M_i are left-matrices of H_j and F_i respectively while M'_k is a right-matrix of G_k,

(b) the lists $N_1, \ldots, N_p$, $M_1, \ldots, M_s$ and $M'_1, \ldots, M'_t$ satisfy E with respect to $H_1, \ldots, H_p$, $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$,

(c) the formula $\bigwedge_{j,\alpha} D_j[u_{j\alpha}] \wedge \bigwedge_{i,\beta} A_i[v_{i\beta}] \supset \bigvee_{k,\gamma} B_k[w_{k\gamma}]$ is a tautology of propositional calculus.

From Lemma 1, part (b) it follows that the lists $M_1, \ldots, M_s$ and $M'_1, \ldots, M'_t$ still satisfy E with respect to $F_1, \ldots, F_s$ and $G_1, \ldots, G_t$. On the other hand, using the fact that all H_j's are purely universal one can easily derive from the identity (c) above the relation

$$H_1, \ldots, H_p \vdash \bigwedge_{i,\beta} A_i[v_{i\beta}] \supset \bigvee_{k,\gamma} B_k[w_{k\gamma}]$$

which proves the statement.

III. **Theory of rings and integral domains.** In the sequel, axioms for ring theory and the theory of integral domains are given. Some of the axioms are redundant; this has no influence since only three of the axioms below will turn out to be important for our further consideration. There are constants 0, 1 and binary operations $+$, $-$, $\times$; the symbol $\times$ stands for multiplication but for easy reading we write ab or $a \cdot b$ instead of $a \times b$.

The axioms are:

(1) $x = y \supset y = x$
(2) $x = y \wedge y = z \supset x = z$
(3) $x = x$
(4) $x = y \supset x+z = y+z$
(5) $x+0 = x$
(6) $x+y = y+x$
(7) $x = y \supset x-z = y-z$
(8) $x = y \supset z-x = z-y$
(9) $x+(y-x) = y$
(10) $x+z = y \supset z = y-x$
(11) $x = y \supset x(z-y) = y(z-y)$
(12) $xy = yx$
(13) $x(y+z) = xy+xz$
(14) $x(y-z) = xy-xz$
(15) $x1 = x$
(16) $x = y \vee y = z \vee (x-y)(z-y) \neq 0$

The ith axiom is denoted by $A_i(x, y, z)$. The axioms of R_0 are the logical axioms and $(x, y, z)A_i$ for $i \leqq 15$; JD_0 has all the axioms of R_0 and in addition $(x, y, z)A_i$. The theories R_1 and JD_1 have the axioms of R_0 and JD_0 respectively and in addition $n \neq 0$ with n for $1+1+\cdots+1$ (n times). R_0 is the theory of commutative rings with unity, JD_0 the theory of commutative integral domains with unity, while JD_1 is the theory of commutative integral domains of characteristic 0. By a polynomial in the variables $x_1, \ldots, x_s$ we understand an element of the integral domain $\boldsymbol{I}[x_1, \ldots, x_s]$. With every term t containing at most $x_1, \ldots, x_s$ as variables we can associate a polynomial $|t|$ in $\boldsymbol{I}[x_1, \ldots, x_s]$ in an obvious way:

(a) $|0|$ and $|1|$ are zero element and unity of $\boldsymbol{I}$,
(b) $|t_1 \pm t_2| = |t_1| \pm |t_2|$,
(c) $|t_1 \times t_2| = |t_1| \times |t_2|$.

An alternative possibility would be to associate with every term t the equivalence class $P(t)$ of terms such that $t' \in P(t)$ iff $R_0 \vdash t = t'$ (or equivalently $JD_1 \vdash t = t'$) and call $P(t)$ a "polynomial". It is rather obvious to show that $|t'| = |t|$ iff $t' \in P(t)$. Before proceeding further we reexamine the way in which a quantifier-free formula is considered as an identity of propositional calculus; the meaning is that two expressions $t_1 = t_2$ and $t_1' = t_2'$ represent the same propositional variable iff t_1 is t_1' and t_2 is t_2'. In this case we call the formula under consideration an identity in the syntactical sense. Another possibility is described by

DEFINITION 7. A quantifier-free formula A is an identity with respect to R_0, JD_0 if and only if the expression obtained from A by means of the following substitutions is a tautology of propositional calculus:

(a) a formula $t_1 = t_2$ such that $0 \in P(t_1 - t_2)$ is replaced by the truth-value T ("truth"),

(b) two expressions $t_1 = t_2$, $t_1' = t_2'$ such that neither $0 \in P(t_1 - t_2)$ nor $0 \in P(t_1' - t_2')$ are replaced by the same propositional variable iff $P(t_1 - t_2) = P(t_1' - t_2')$ or $P(t_2 - t_1) = P(t_1' - t_2')$.

The formula A is an identity with respect to R_1, JD_1 if and only if the expression obtained from A by means of the following substitutions is a tautology of propositional calculus:

(a') a formula $t_1=t_2$ such that $n\in P(t_1-t_2)$ is replaced by T or the truth value F ("false") according to whether $n=0$ or $n\neq 0$,

(b') two expressions $t_1=t_2$, $t_1'=t_2'$ such that neither $n\in P(t_1-t_2)$ nor $n\in P(t_1'-t_2')$ $(n<\infty)$ denote the same propositional variable iff $P(t_1-t_2)=P(t_1'-t_2')$ or $P(t_2-t_1)=P(t_1'-t_2')$.

Obviously an identity in the syntactical sense is an identity with respect to R_0, JD_0 and R_1, JD_1 but not conversely (in general). The next lemma is obvious.

LEMMA 3. *Let i be 0 or 1. If A is an identity with respect to R_i, JD_i then $R_i\vdash A$ and $JD_i\vdash A$. If A and $A\supset B$ are identities with respect to R_i, JD_i then so is B.*

For typographical reasons we adopt the following convention: if in a certain algebraic context we have to do with the polynomials $|t_1|,\ldots,|t_s|$ associated with the terms $t_1,\ldots,t_s$ then we denote this polynomial just by its terms. Thus if, e.g., $f, g_1,\ldots,g_s$ are terms then $B(g_1,\ldots,g_s)$ is the polynomial ideal $\boldsymbol{B}(|g_1|,\ldots,|g_s|)$ and $f\in\boldsymbol{B}(g_1,\ldots,g_s)$ means $|f|\in\boldsymbol{B}(|g_1|,\ldots,|g_s|)$. More generally if $\boldsymbol{v}_i=(t_1^i,\ldots,t_{s_i}^i)$ $(i\leqq s)$ are vectors whose components are terms then $\boldsymbol{B}(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_s)$ denotes the ideal (with respect to $\boldsymbol{R}$) whose basis consists precisely of all the polynomials $|t_k^i|$. The same convention is used in case of ideals $\boldsymbol{B}^*(|t|,\ldots)$.

IV. **Universal formulas.** In what follows we will prove a lemma which enables us to characterize those universal formulas which can be proved from R_i, JD_i $(i=0, 1)$ respectively. The proof could easily be given by using simple algebraic facts such as Hilbert's Nullstellensatz (abbreviated as HNS in the sequel) in the case of JD_i. The proof given below is metamathematical; it is somewhat more involved than the purely algebraic proof. However it may have some interest in itself to have a metamathematical deduction of this lemma since it is the syntactical counterpart of HNS.

LEMMA 4. *Let $f_i(x_1,\ldots,x_{s_i})$ $(i\leqq s)$ and $g_k(x_1,\ldots,x_{t_k})$ $(k\leqq t)$ be terms.*

(a) $R_0\vdash\bigvee_i f_i=0\vee\bigvee_k g_k\neq 0$ *iff at least one f_i is in $B^*(g_1,\ldots,g_t)$.*

(b) $JD_0\vdash\bigvee_i f_i=0\vee\bigvee_k g_k\neq 0$ *iff there is an integer $e\geqq 0$ such that*

$$\left(\prod_i f_i\right)^e\in\boldsymbol{B}^*(g_1,\ldots,g_t).$$

Proof. We start with (a). Obviously the nontrivial part consists in proving the implication from left to right. Hence we assume $R_0\vdash\bigvee_i f_i=0\vee\bigvee_k g_k\neq 0$. The nonlogical axioms of R_0 are the formulas $(x, y, z)A_i(x, y, z)$ $(i\leqq 15)$ given in §III; the formula $\bigvee_i f_i=0\vee\bigvee_k g_k\neq 0$ is denoted by $\boldsymbol{B}(x_1,\ldots,x_m)$ where $x_1,\ldots,x_m$ are the variables appearing in an f_i or a g_k. Denote $(x, y, z)A_i$ and $(x_1,\ldots,x_m)B$ by F_i and G respectively. According to Corollary 1 (of Theorem 2) there are vectors $\boldsymbol{v}_{i\alpha}=(t_{\alpha 1}^i, t_{\alpha 2}^i, t_{\alpha 3}^i)$ $(\alpha\leqq m_i)$ with $t_{\alpha k}^i$ terms whose variables are among $x_1,\ldots,x_m$ such that $\bigwedge_{i,\alpha}A_i[\boldsymbol{v}_{i\alpha}]\supset B(x_1,\ldots,x_m)$ is a tautology of propositional calculus, and therefore also an identity with respect to R_0. But all formulas $A_i[\boldsymbol{v}_{i\alpha}]$

except for $i=2, 11$ are already identities with respect to R_0, as is easily verified. Hence by Lemma 3 it follows that

$$\bigwedge_{\alpha} A_2[v_{2\alpha}] \wedge \bigwedge_{\alpha} A_{11}[v_{11\alpha}] \supset \boldsymbol{B}(x_1, \ldots)$$

is an identity with respect to R_0. Let us put $t^2_{\alpha 1}=a_\alpha$, $t^2_{\alpha 2}=b_\alpha$, $t^2_{\alpha 3}=c_\alpha$, $t^{11}_{\alpha 1}=\boldsymbol{u}_\alpha$, $t^{11}_{\alpha 2}=\boldsymbol{v}_\alpha$, $t^{11}_{\alpha 3}=\boldsymbol{w}_\alpha$ and $m_2=p$, $m_{11}=q$. With this notation, and taking care of the special form of A_2 and A_{11}, we find that

$$\text{(I)} \qquad \bigvee_{\alpha}^{p} (a_\alpha = b_\alpha \wedge b_\alpha = c_\alpha \wedge a_\alpha \neq c_\alpha) \vee \bigvee_{\beta}^{q} (u_\beta = v_\beta \vee u_\beta w_\beta \neq v_\beta w_\beta) \vee \bigvee_{i} f_i = 0 \vee \bigvee_{k} g_k \neq 0$$

is an identity with respect to R_0. First we show by induction on p: if $f_1, \ldots, f_s$, $g_1, \ldots, g_t$, a_α, b_α, c_α $(1 \leqq \alpha \leqq p)$ are terms such that the formula

$$\text{(II)} \qquad \bigvee_{\alpha}^{p} (a_\alpha = b_\alpha \wedge b_\alpha = c_\alpha \wedge a_\alpha \neq c_\alpha) \vee \bigvee_{i} f_i = 0 \vee \bigvee_{k} g_k \neq 0$$

is an identity with respect to R_0 then $f_i \in B^*(g_1, \ldots, g_t)$ for some i. If $p=0$, that is, if the a_α, b_α, c_α are absent then either $|f_i|=0$ or $|f_i|=|g_k|$ or $|f_i|=-|g_k|$ for some i, k; in either of these cases the statement holds. Assume that the statement has been proved for $p \leqq p_0$ and that the expression (II), but with p replaced by p_0+1, is an identity with respect to R_0. We denote $\bigvee_{\alpha}^{p} (a_\alpha=b_\alpha \wedge b_\alpha=c_\alpha \wedge a_\alpha \neq c_\alpha)$ by P and $a_{p_0+1}, b_{p_0+1}, c_{p_0+1}$ by a, b and c respectively. Identity (II) can now be rewritten as follows:

$$P \vee (a = b \wedge b = c \wedge a \neq c) \vee \bigvee_{i} f_i = 0 \vee \bigvee_{k} g_k \neq 0.$$

From this it easily follows that $P \vee a-b=0 \vee \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ and $P \vee b-c=0 \vee \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ and $P \vee \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0 \vee a-c \neq 0$ are identities with respect to R_0. If $f_i \notin \boldsymbol{B}^*(g, \ldots, g)$ for all i, then the induction hypothesis applied to the identities just given yields $a-b \in \boldsymbol{B}^*(g_1, \ldots, g_t)$, $b-c \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ and $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t, a-c)$ for some i and hence $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t)$, contradicting the assumption. Next we treat the full expression (I), that is we consider p as fixed and proceed by induction with respect to q. If $q=0$, that is if the u_α, v_α, w_α are absent, then we are in the case just treated.

Now assume the following: for all p, if $q \leqq q_0$ and if $f_1, \ldots, f_s$, $g_1, \ldots, g_t$, a_α, b_α, c_α, u_β, v_β, w_β $(\alpha \leqq p, \beta \leqq q)$ are terms such that expression (I) is an identity with respect to R_0 then $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ for some i. We denote

$$\bigvee_{\alpha} (a_\alpha = b_\alpha \wedge b_\alpha = c_\alpha \wedge a_\alpha \neq c_\alpha) \vee \bigvee_{\beta} (u_\beta = v_\beta \wedge u_\beta w_\beta \neq v_\beta w_\beta)$$

by P and put $u_{q_0+1}=u$, $v_{q_0+1}=v$, $w_{q_0+1}=w$; we assume that

$$P \vee (u = v \wedge uw \neq vw) \vee \bigvee_{i} f_i = 0 \wedge \bigvee_{k} g_k \neq 0$$

is an identity with respect to R_0. Again one concludes that $P \vee u-v=0 \vee \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0$ and $P \vee \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0 \vee (uw-vw) \neq 0$ are identities with respect to R_0. If $f_i \notin \boldsymbol{B}^*(g_1, \ldots, g_t)$ for all i, then an application of the induction hypothesis yields $u-v \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ and $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t, w(u-v))$ for some i. But then $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t)$, contrary to the assumption.

Now we come to the proof of (b). In addition to the axioms $(x, y, z)A_i$, $i=2, 11$ we have to take into account $(x, y, z)A_{16}(x, y, z)$. By arguing the same way as at the beginning of the proof of part (a) one concludes: if $JD_0 \vdash \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0$ then there are terms $a_\alpha, b_\alpha, c_\alpha, u_\beta, v_\beta, w_\beta, s_\gamma, t_\gamma$, $(\alpha \leqq p, \beta \leqq q, \gamma \leqq r)$ such that the expression

$$\bigvee_\alpha^p (a_\alpha = b_\alpha \wedge b_\alpha = c_\alpha \wedge a_\alpha \neq c_\alpha) \vee \bigvee_\beta^q (u_\beta = v_\beta \wedge u_\beta w_\beta \neq v_\beta w_\beta) \vee \bigvee_\gamma^r (s_\gamma \neq 0 \wedge t_\gamma \neq 0 \wedge s_\gamma \cdot t_\gamma = 0) \vee B$$

(with B denoting $\bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0$) is an identity with respect to JD_0. We denote this last expression by (II) in the sequel. We show by induction with respect to r that this implies the existence of an integer $e \geqq 0$ such that $(\prod_i f_i)^e \in \boldsymbol{B}^*(g_1, \ldots, g_t)$. If $r=0$ the statement follows from (a) (since (II), being an identity with respect to JD_0, is also an identity with respect to R_0). Assume the statement to be proved up to r_0; let P be the expression

$$\bigvee_\alpha^p (a_\alpha = b_\alpha \wedge b_\alpha = c_\alpha \wedge a_\alpha \neq c_\alpha) \vee \bigvee_\beta^q (u_\beta = v_\beta \wedge u_\beta w_\beta \neq v_\beta w_\beta) \vee \bigvee_\gamma^{r_0} (s_\gamma \neq 0 \wedge t_\gamma \neq 0 \wedge s_\gamma t_\gamma = 0)$$

and denote s_{γ_0+1}, t_{γ_0+1} by s and t respectively. We assume that

$$P \vee (s \neq 0 \wedge t \neq 0 \wedge st = 0) \vee \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0$$

is an identity with respect to JD_0. It follows by a short calculation that the following formulas are identities with respect to JD_0 too:

$$P \vee \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0 \vee s \neq 0, \quad P \vee \bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0 \vee t \neq 0,$$

$$P \vee \bigvee_i f_i = 0 \vee st = 0 \vee \bigvee_k g_k \neq 0.$$

Application of the induction hypothesis yields the existence of an e such that

(1) $(\prod_i f_i)^e \in \boldsymbol{B}^*(g_1, \ldots, g_t, s)$,

(2) $(\prod_i f_i)^e \in \boldsymbol{B}^*(g_1, \ldots, g_t, t)$,

(3) $(st)^e (\prod_i f_i)^e \in \boldsymbol{B}^*(g_1, \ldots, g_t)$.

Put $(\prod_i f_i) = A$, and denote $\boldsymbol{B}^*(g_1, \ldots, g_t)$ by I. By (1) there is a polynomial h such that $A + hs \in I$. Consider the expressions $s^{e-k-1} A^{k+1} t^e (A+hs)$; by virtue of (1) they are all in I. By an easy induction on k one shows $s^{e-k} A^{k+1} t^e \in I$: for $k=0$ it

follows from (3), for $k+1$ it follows from $s^{e-k-1}A^{k+2}t^e+hs^{e-k}A^{k+1}t^e \in I$ and from the induction hypothesis. For $k=e$ one obtains $A^{e+1}t^e \in I$. By (2) there is a polynomial h' such that $A+h't \in I$. Consider the expressions $t^{e-k-1}A^{e+k+1}(A+h't)$: by virtue of (2) they are all in I. By induction on k one shows $t^{e-k}A^{e+k+1} \in I$: for $k=0$ the statement has just been proved, for $k+1$ it follows from $t^{e-k-1}A^{e+k+2}+h't^{e-k}A^{e+k+1} \in I$ and from the induction hypothesis. For $k=e$ we obtain $A^{2e+1} \in I$, which concludes the proof of part (b) of the lemma.

COROLLARY 2. (a) $R_1 \vdash \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ *iff either* $f_i \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ *for some* i *or* $n \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ *for some* $n>0$.

(b) $JD_1 \vdash \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ *iff there is an* $e>0$ *such that*

$$\left(\prod_i f_i\right)^e \in \boldsymbol{B}(g_1, \ldots, g_t).$$

Proof. Part (a) follows immediately from Lemma 4 (a), taking into account that R_1 is R_0 plus the axioms $1 \neq 0, 2 \neq 0, \ldots$. Consider (b). If $(\prod_i f_i)^e \in \boldsymbol{B}(g_1, \ldots, g_t)$ then $n(\prod_i f_i)^e \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ for some $n \neq 0$. Then $\bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ follows from JD_1, as is easy to see. Assume conversely $JD_1 \vdash \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$. Then $JD_0, 1 \neq 0, \ldots, n \neq 0 \vdash \bigvee_i f_i=0 \vee \bigvee_k g_k \neq 0$ for some $n>0$. Lemma 4 (b) implies $(\prod_i f_i)^e K \in \boldsymbol{B}^*(g_1, \ldots, g_t)$ for some integer $K>0$ and hence $(\prod_i f_i)^e \in \boldsymbol{B}(g_1, \ldots, g_t)$.

Actually the proof of Lemma 4 gives a slightly sharper result. Due to the fact that the passage from an arbitrary proof in sentential calculus to a cut free proof is described in a primitive recursive way, one obtains, after a slight reorganization of the proof of Lemma 4 a more constructive version of this lemma. In order to state it, let $p_0, p_1, \ldots$ be the list of primes in increasing order and put $\langle n_0, \ldots, n_s \rangle = p_0^{n_0+1} \cdots p_s^{n_0+1}$; in addition, given any term t, let t^0 be its Goedel number in any suitable numbering. Then we have

LEMMA 4*. *There is a primitive recursive function* ϕ *with the property: if* p *is (the Goedel number of) a proof of* $(\mathbf{x})(\bigwedge_i^t g_i=0 \supset f=0)$ *from* JD_0 *then* $\phi(p)=\langle e, h_1^0, \ldots, h_t^0 \rangle$ *such that* $f^e=\sum h_i g_i$.

V. **An algebraic version of GEH.** Lemma 4 and Theorem 2* permit a reformulation of GEH in terms of polynomials and ideals. To this end let us remember the notation introduced at the end of §III: if $v_i=(t_1^i, \ldots, t_{s_i}^i)$ $(i \leqq s)$ are vectors whose components are terms then $B(v_1, \ldots, v_s)$ denotes the polynomial ideal with coefficients from $\boldsymbol{R}$ generated by the polynomials $|t_k^i|$; similarly $\boldsymbol{B}^*(v_1, \ldots, v_s)$ denotes the ideal generated by the polynomials $|t_k^i|$, but with coefficients from $\boldsymbol{I}$. First we need

LEMMA 5. *Let* $f_{k\alpha}^i, g_{k\beta}^i$ $(i \leqq s, k \leqq t, \alpha \leqq n, \beta \leqq m)$ *be terms. Then*

$$JD_1 \vdash \bigvee_i \bigwedge_k \left(\bigvee_\alpha f_{k\alpha}^i = 0 \vee \bigvee_\beta g_{k\beta}^i \neq 0\right)$$

iff there is an integer $e>0$ *such that for every function* $k(x)$ *defined for* $i \leqq s$ *with*

values $k(i) \leqq t$ *we have*

$$\left(\prod_{i,\alpha} f^i_{k(i)\alpha}\right)^e \in \boldsymbol{B}(\mathbf{g}^1_{k(1)}, \ldots, \mathbf{g}^t_{k(t)})$$

where $\mathbf{g}^i_k$ *is the vector* $(g^i_{k1}, \ldots, g^i_{km})$.

Proof. Denote the formula quoted in the lemma by F. The conjunctive normal form F' of F is the conjunction of all formulas G of the following type: $\bigvee_{i,\alpha} f^i_{k(i)\alpha} = 0 \vee \bigvee_{i,\beta} g^i_{k(i)\beta} \neq 0$ where $k(x)$ is any function defined for $i \leqq s$ with values $k(i) \leqq t$. Obviously $JD_1 \vdash F$ iff $JD_1 \vdash G$ for all such G. On the other hand it follows from the corollary of Lemma 4 that a fixed such G (determined by $k(x)$) is provable from JD_1 iff there is a $q \geqq 0$ (depending on $k(x)$) such that

$$\text{(I)} \qquad \left(\prod_{i,\alpha} f^1_{k(i)\alpha}\right)^q \in \boldsymbol{B}(\mathbf{g}^1_{k(1)}, \ldots, \mathbf{g}^t_{k(t)}).$$

It follows that if there is an e as stated by the lemma, then $JD_1 \vdash G$ for all G of the above type, that is $JD_1 \vdash F'$, hence $JD_1 \vdash F$. If conversely $JD_1 \vdash F$, then for every $k(x)$ with the above properties there is a q such that (I) holds. By choosing e larger than all finitely many q's, the statement follows.

THEOREM 4. *Let* $\phi, f_{k\alpha}, g_{k\beta}$ $(k \leqq t, \alpha \leqq a, \beta \leqq b)$ *be terms and let* B *be the formula* $\bigwedge_k (\bigvee_\alpha f_{k\alpha} = 0 \vee \bigvee_\beta g_{k\beta} \neq 0)$. *We assume that* ϕ *and* B *contain precisely the variables* $y_1, \ldots, y_m$ *and* $x_1, \ldots, x_n$ *respectively. For any list* $Q_1, \ldots, Q_n$ *of quantifiers we have*

$$JD_1, (\mathbf{y})\phi \neq 0 \vdash (Q_1x_1, \ldots, Q_nx_n)B$$

iff there is a left-matrix $M = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_p\}$ *and a right-matrix* $M' = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_q\}$ *of* $(\mathbf{y})\phi = 0$ *and* $(Q_1x_1, \ldots, Q_nx_n)B$ *respectively and an integer* $e \geqq 0$ *such that*

(a) M *and* M' *satisfy condition* E *of Definition* 6 *with respect to* $(\mathbf{y})\phi \neq 0$ *and* $(Q_1x_1, \ldots, Q_nx_n)B$,

(b) $(\prod_\gamma \phi[\boldsymbol{u}_\gamma])^e (\prod_{i,\alpha} f_{k(i)\alpha}[\boldsymbol{v}_i])^e \in \boldsymbol{B}(\mathbf{g}^1_{k(1)}, \ldots, \mathbf{g}^q_{k(q)})$ *for all functions* $k(x)$ *defined for* $i \leqq p$ *with values* $k(i) \leqq t$; *the vectors* $\mathbf{g}^i_k$ *are abbreviations for* $(g_{k(i)1}[\boldsymbol{v}_i], \ldots, g_{k(i)b}[\boldsymbol{v}_i])$.

Proof. Denote $(\mathbf{y})\phi \neq 0$ and $(Q_1x_1, \ldots, Q_nx_n)B$ by F and G respectively. According to Theorem 3, if $JD_1, F \vdash G$ then there are matrices $M = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_p\}$ and $M' = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_q\}$ such that

(1) M is a left-matrix of F and M' is a right-matrix of G,

(2) the formula $\bigwedge_\gamma \phi[\boldsymbol{u}_\gamma] \neq 0 \supset \bigvee_i B[\boldsymbol{v}_i]$ is provable from JD_1,

(3) M and M' satisfy E with respect to F and G.

Denote $f_{k\alpha}[\boldsymbol{v}_i]$ and $g_{k\beta}[\boldsymbol{v}_i]$ by $f^i_{k\alpha}$ and $g^i_{k\beta}$ respectively. Define $h^i_{k\alpha}$ as follows: for $\alpha \leqq a$ we put $h^i_{k\alpha} = f^i_{k\alpha}$, for $\alpha = a + d$ $(1 \leqq d \leqq p)$ we put $h^i_{k\alpha} = \phi[\boldsymbol{u}_d]$. By propositional calculus we find that

$$\text{(II)} \qquad \bigvee_i \bigwedge_k \left(\bigvee_\alpha h^i_{k\alpha} = 0 \vee \bigvee_\beta g^i_{k\beta} \neq 0\right)$$

is provable from JD_1. By Lemma 5 there is a $c \geqq 0$ such that for all functions $k(x)$

defined for $i \leqq p$ with values $k(i) \leqq t$ we have

$$\text{(III)} \qquad \left(\prod_{i,\alpha} h^i_{k(i)\alpha}\right)^c \in \boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)}),$$

that is

$$\text{(IV)} \qquad \left(\prod_{\lambda} \phi[\boldsymbol{u}_\lambda]\right)^{pc} \left(\prod_{i,\alpha} f^i_{k(i)\alpha}\right)^c \in \boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)})$$

and hence

$$\text{(V)} \qquad \left(\prod_{\lambda} \phi[\boldsymbol{u}_\lambda]\right)^{pc} \left(\prod_{i,\alpha} f^i_{k(i)\alpha}\right)^{pc} \in \boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)})$$

where $\mathfrak{g}^i_k$ denotes $(g_{k1}[\boldsymbol{v}_i], \ldots, g_{kb}[\boldsymbol{v}_i])$. By putting $pc = e$ the necessity of (a) and (b) follows. Assume conversely (a) and (b) of the theorem to be true and let $h^i_{k\alpha}, f^i_{k\alpha}, g^i_{k\beta}$ be the same as above. If we multiply in (b) the element on the left by $(\prod_\lambda \phi[\boldsymbol{u}_\lambda])^{pe-e}$ we reobtain the relation (IV) above but with e in place of c. By performing the above reasoning in the reverse direction we conclude from Lemma 5 that $\bigwedge_\lambda \phi[\boldsymbol{u}_\lambda] \supset \bigvee_i \boldsymbol{B}[\boldsymbol{v}_i]$ is provable from JD_1. This, combined with (a) and Theorem 3 implies $JD_1, F \vdash G$, which completes the proof.

REMARKS. (1) The case $JD_1 \vdash (Q_1x_1, \ldots, Q_nx_n)B$ can be treated as a special case of Theorem 4 by taking for ϕ the constant 1 and by putting $m = 0$; the effect is that the factor $(\prod_\lambda \phi[\boldsymbol{u}_\lambda])^e$ in (b) can be omitted.

(2) In the case of R_0 a statement similar to Theorem 4 holds whose proof is even more simple.

In the next corollary we retain the notation used in Theorem 4.

COROLLARY 3. *Let $\phi, f^i_{k\alpha}, g^i_{k\beta}$ and B be the same as in Theorem* 4. *Assume that JD_1, $(\mathrm{y})\phi \neq 0 \vdash (Q_1x_1, \ldots, Q_nx_n)B$ holds and that $(Q_1x_1, \ldots, Q_nx_n)B$ is not provable from JD_1. Let $M = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_p\}$ and $M' = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_q\}$ be a left-matrix and a right-matrix of $(\mathrm{y})\phi \neq 0$ and $(Q_1x_1, \ldots, Q_nx_n)B$ respectively such that* (a) *and* (b) *of Theorem* 4 *are satisfied. Then there is at least one function $k(x)$ defined for $i \leqq p$ with values $k(i) \leqq t$ and at least one isolated component P of $\boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)})$ such that $\phi[\boldsymbol{u}_\lambda] \in P$ for some λ.*

Proof. Assume the contrary and denote $(\mathrm{y})\phi \neq 0$ and $(Q_1x_1, \ldots, Q_nx_n)B$ again by F and G respectively. Let $k(x)$ be a fixed function defined for $i \leqq p$ with values $k(i) \leqq t$. From (b) of Theorem 4, and from our assumption, it follows that for every isolated component P of $\boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)})$ there are numbers i, α such that $f^i_{k(i)\alpha} \in P$ (using the fact that P is a prime ideal). From this and the ideal-property of P one deduces the existence of a number c such that

$$\text{(I)} \qquad \left(\prod_{i,\alpha} f^i_{k(i)\alpha}\right)^c \in \boldsymbol{B}(\mathfrak{g}^1_{k(1)}, \ldots, \mathfrak{g}^q_{k(q)})$$

(where c depends on $k(x)$). By choosing e sufficiently large one concludes that for every function $k(x)$ defined for $i \leqq p$ with values $k(i) \leqq t$ the relation (I), but with e

in place of c, holds. Since F is purely universal it follows from Lemma 1 that M' satisfies E with respect to G (see remark following Definition 6). This means that conditions (a) and (b) of Theorem 4 are satisfied but with $(\mathbf{y})\phi \neq 0$ absent. According to the remark following Theorem 4 this means that $JD_1 \vdash G$ holds, contradicting the assumption.

At this point a remark concerning Theorem 4 (and Theorem 3) seems to be appropriate. Theorem 4 can be considered as consisting of two parts, a logical one and an algebraic one. The logical part consists of (a) (involving E) together with the requirement that M and M' are a left- and a right-matrix of $(\mathbf{y})\phi \neq 0$ and $(Q_1 x_1, \ldots, Q_n x_n)B$ respectively. The logical part imposes certain restrictions of order on the matrices M and M'. Clause (b) of Theorem 4 represents the algebraic part and imposes certain algebraic restrictions on M and M'. The possibility of characterizing derivability from JD_1 in the way described by Theorem 4 depends

(1) on the fact that the axioms of JD_1 are purely universal,

(2) the special characterization of derivability for formulas $\bigvee_i f_i = 0 \vee \bigvee_k g_k \neq 0$ given by Lemma 4.

Concerning Theorem 3 we may say that the reason for rephrasing the results of §1 in the form given by Theorem 3 is that in the frame of ordinary predicate calculus the formalism of GEH is easier to handle if the notion of matrix is used. Another reason is that in many cases we need not know how the restrictions imposed by condition E (which is just (a)–(c) of Theorem 1 and (d) of Theorem 2) on the matrices M and M' really look like; all that is used in these cases is that E has the properties described by Theorem 3 and Lemmas 1 and 2.

VI. **Some applications.** In this section we consider some applications of Theorem 3 combined with Lemma 4. Let us start with a lemma.

LEMMA 6. *Let $f^i_{k\alpha}$, g_β be terms $(1 \leqq i \leqq s,\ 1 \leqq k \leqq t,\ 1 \leqq \alpha \leqq m,\ 1 \leqq \beta \leqq n)$ and denote $\bigvee_i (\bigwedge_k \bigvee_\alpha f^i_{k\alpha} = 0) \vee \bigvee_\beta g_\beta \neq 0$ by F.*

(a) *$R_0 \vdash F$ if and only if there is an i such that for every k there is an $\alpha(k)$ with $f^i_{k\alpha(k)} \in \boldsymbol{B}^*(g_1, \ldots, g_n)$.*

(b) *If $\boldsymbol{B}(g_1, \ldots, g_n)$ is a prime ideal, then $JD_1 \vdash F$ if and only if there is an i such that for every k there is an $\alpha(k)$ with $f^i_{k\alpha(k)} \in \boldsymbol{B}(g_1, \ldots, g_n)$.*

Proof. We content ourself with proving the "only if" part of (b). The "only if" part of (a) is proved in quite the same way, making use of Lemma 4 (a). Both for (a) and (b) the "if" part follows rather easily from the axioms of JD_1 and R_0 respectively and a small amount of predicate calculus. Hence assume $JD_1 \vdash F$; in order to obtain a contradiction we assume that there is no i of the kind required by (b). If we put $g^i_{k\beta} = g_\beta$ for all i, k then F acquires the same form as the formula appearing in Lemma 5. Now we apply this lemma and keep in mind that

$$\boldsymbol{B}(\mathbf{g}^1_{k(1)}, \ldots, \mathbf{g}^t_{k(t)})$$

is nothing else than $\boldsymbol{B}(g_1, \ldots, g_n)$. Then there is an e such that for every $k(x)$

defined for $i \leqq s$ with values $k(i) \leqq t$ the relation

$$\text{(I)} \qquad \left(\prod_{i,\alpha} f^i_{k(i)\alpha}\right)^e \in \boldsymbol{B}(g_1, \ldots, g_n)$$

holds. From our additional assumption it follows that for every i there is a $k(i)$ such that $f^i_{k(i)\alpha} \notin \boldsymbol{B}(g_1, \ldots, g_n)$ for all α. But for this special $k(x)$ again relation (I) holds. Since the ideal on the right side of (I) is a prime ideal there is at least one i and one α such that $f^i_{k(i)\alpha} \in \boldsymbol{B}(g_1, \ldots, g_n)$ is true. But this is in contradiction with our special choice of $k(x)$.

COROLLARY 4. *Let f^i_k, g_β be terms ($i \leqq s$, $k \leqq t$, $1 \leqq \beta \leqq n$) and denote*

$$\bigvee_i \left(\bigwedge_k f^i_k = 0\right) \vee \left(\bigvee_\beta g_\beta \neq 0\right)$$

by F.

(a) *$R_0 \vdash F$ iff there is an i such that $f^i_k \in \boldsymbol{B}^*(g_1, \ldots, g_n)$ for all k.*

(b) *If $\boldsymbol{B}(g_1, \ldots, g_n)$ is prime, then $JD_1 \vdash F$ if there is an i such that*

$$f^i_k \in \boldsymbol{B}(g_1, \ldots, g_n) \quad \textit{for all } k.$$

Proof. The statement follows from Lemma 6 by putting there $f^i_{k\alpha} = f^i_k$ and $m = 1$.

1. Let F be the closed prenex standard formula

$$(x_1)(Ey_1)\cdots(x_s)(Ey_s)\left(\bigvee_i \bigwedge_k f_{ik} = 0\right) \qquad (i \leqq s, k \leqq t).$$

If $JD_1 \vdash F$ then according to Theorem 3 there is a right-matrix $M = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of F such that $JD_1 \vdash \bigvee_j \bigvee_i \bigwedge_k f_{ik}[\boldsymbol{v}_j] = 0$. From the last corollary, (with g_β all absent or equivalently all 0) we find that there are i, j such that $f_{ik}[\boldsymbol{v}_j] = 0$ for all k. If we investigate the restrictions imposed on $\boldsymbol{v}_j$ by E (that is, in particular, by (c) of Theorem 1), we find that $\boldsymbol{v}_j$ has the following form:

$$(x_1, t'_1(x_1), x_2, t'_2(x_1, x_2), \ldots, x_s, t'_s(x_1, \ldots, x_s))$$

where the t'_i may contain additional variables $y_1, \ldots, y_m$, all different from $x_1, \ldots, x_s$. After replacing the y_i's by 0 we have the following result: if $JD_1 \vdash F$ then there is an i and terms $t_1(x_1)$, $t_2(x_1, x_2), \ldots, t_s(x_1, \ldots, x_s)$ such that

$$f_{ik}(x_1, t_1, \ldots, x_s, t_s) = 0 \quad \text{for all } k.$$

It is easy to show that this property is in turn sufficient to ensure $R_0 \vdash F$ and hence $JD_1 \vdash F$. If we specialize to the very particular case where F is $(x)(Ey)f(x, y) = 0$ we find (using a result from [1]) that there is no method to decide whether a formula F of the given form is derivable from JD_1 or not.

2. For the next application we introduce two classes of formulas. A_1 is the class of quantifier-free formulas whose inductive definition is as follows:

(a) $f \neq 0$ is in A_1 for any term f,

(b) if A, B are in A_1 then so are $A \wedge B$ and $A \vee B$.

The class A_2 consists of all closed prenex standard formulas $(Q_1x_1, \ldots, Q_sx_s) \cdot B(x_1, \ldots, x_s)$ with B in A_1.

THEOREM 5. *Let $F_1, \ldots, F_n$ be formulas from A_2. Let $g_1, \ldots, g_m$ be terms such that the formula $\bigvee_k g_k \neq 0$ contains precisely $x_1, \ldots, x_s$ as variables. Assume in addition that $B(g_1, \ldots, g_m)$ is prime. If*

$$JD_1, F_1, \ldots, F_n \vdash (x_1, \ldots, x_s)\Big(\bigvee_k g_k \neq 0\Big)$$

then there is an i_0 such that already $JD_1, F_{i_0} \vdash (x_1, \ldots, x_s)(\bigvee_k g_k \neq 0)$.

Proof. Denote $\bigvee_k g_k \neq 0$ by $C(x_1, \ldots, x_s)$ and $(x_1, \ldots, x_s)C(x_1, \ldots, x_s)$ by G. Without restriction we can assume that F_i has the form

$$(Q_1^i x_1, \ldots, Q_{n(i)}^i x_{n(i)})\Big(\bigvee_j \bigwedge_k f_{jk}^i \neq 0\Big);$$

denote $\bigvee_j \bigwedge_k f_{jk}^i \neq 0$ by A. Assume finally $JD_1, F_1, \ldots, F_n \vdash G$. According to Theorem 3 we find left-matrices $M_i' = \{\boldsymbol{v}_n^i, \ldots, \boldsymbol{v}_{\alpha(i)}^i\}$ of F_i $(i \leqq n)$ and a right-matrix $M' = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_q\}$ of G such that

(a) $M_1, \ldots, M_n$ and M' satisfy E with respect to $F_1, \ldots, F_n$ and G,

(b) $\bigwedge_{i\alpha} A_i[\boldsymbol{v}_\alpha^i] \supset \bigvee_\lambda C[\boldsymbol{w}_\lambda]$ is provable from JD_1.

An easy inspection of condition E (in particular subcondition (d) of Theorem 2) shows that M' must necessarily consist of precisely one right-vector $\boldsymbol{w}$ which in addition has the form $(x_1, \ldots, x_s)$. Hence we conclude from (b) above that

$$\bigwedge_{i,\alpha} A_i[\boldsymbol{v}_\alpha^i] \supset \bigvee_k g_k \neq 0$$

is provable from JD_1. This in turn implies that

$$\bigvee_{i,\alpha}\Big(\bigwedge_j \bigvee_k f_{jk}^i[\boldsymbol{v}_\alpha^i] = 0\Big) \vee \bigvee_\beta g_\beta \neq 0$$

is provable from JD_1. From Lemma 6 applied to the present situation it follows that there are i_0, α_0 such that for every j there is a $k(j)$ with $f_{jk(j)}^{i_0}[\boldsymbol{v}_{\alpha_0}^{i_0}] \in \boldsymbol{B}(g_1, \ldots, g_m)$. Combining this with the "if" part of Lemma 6 (b) putting $s=1$ there, we find that

$$\Big(\bigwedge_j \bigvee_k f_{jk}^{i_0}[\boldsymbol{v}_{\alpha_0}^{i_0}] = 0\Big) \vee \bigvee_\beta g_\beta \neq 0$$

or equivalently $A_{i_0}[\boldsymbol{v}_{\alpha_0}^{i_0}] \supset \bigvee_\beta g_\beta \neq 0$ are provable from JD_1. From Lemma 1 (a) it follows that $\{\boldsymbol{v}_{\alpha_0}^{i_0}\}$ and $\{\boldsymbol{w}\}$ (that is $\{(x_1, \ldots, x_s)\}$) satisfy E^* with respect to F_{i_0} and G. After replacing eventually superfluous variables in $\boldsymbol{v}_{\alpha_0}^{i_0}$ by 0 we obtain by Lemma 2 a left-matrix $\boldsymbol{v}$ of F_{i_0}, a right-matrix $\{(x_1, \ldots, x_s)\}$ of G such that E is satisfied with respect to F and G and such that $JD_1 \vdash A_{i_0}[\boldsymbol{v}] \supset C[\boldsymbol{w}]$ holds. From Theorem 3 we conclude $JD_1 \vdash F_{i_0} \supset G$ that is $JD_1, F_{i_0} \vdash G$, which proves the statement.

In order to obtain a few corollaries we note the following

LEMMA 7. *Let $\phi_1, \ldots, \phi_s$ be terms containing only variables from the list $x_1, \ldots, x_t$. Let $q_1 \cap \cdots \cap q_n$ be a primary decomposition of $\boldsymbol{B}(\phi_1, \ldots, \phi_s)$ and p_i the prime ideal associated with q_i. Finally let $g^i, \ldots, g_{\alpha(i)}^i$ be a basis of p_i. Then*

$$JD_1 \vdash (x_1, \ldots, x_s)\Big(\bigvee_i \phi_i \neq 0\Big) \leftrightarrow \bigwedge_i (x_1, \ldots, x_s)\Big(\bigvee_j g_{ij} \neq 0\Big).$$

We do not give the proof, which is easily obtainable by predicate calculus and elementary algebra.

COROLLARY 5. *For every formula* $(x_1, \ldots, x_s)(\bigvee_i \phi_i \neq 0)$ *there is an integer* $e>0$ *with the property: whenever the formulas* F_i $(i<\omega)$ *belonging to* A_2 *are such that* $JD_1, F_1, \ldots \vdash (x_1, \ldots, x_s)(\bigvee_i \phi_i \neq 0)$ *holds then there is a subset* $F_{i_1}, \ldots, F_{i_e}$ *such that already* $JD_1, F_{i_1}, \ldots, F_{i_e} \vdash (\mathbf{x})(\bigvee_i \phi_i \neq 0)$ *holds.*

Proof. Let $\boldsymbol{B}(\phi_1, \ldots, \phi_n)$ have the primary decomposition $q_1 \cap \cdots \cap q_e$, let p_i be the prime ideal associated with q_i. Assume that $g_1^i, \ldots, g_{\alpha(i)}^i$ is a basis of p_i. Denote $(\mathbf{x})(\bigvee_i \phi_i \neq 0)$ by G and $(\mathbf{x})(\bigvee_k g_k^i \neq 0)$ by G_i. According to the last lemma $JD_1, F_1, F_2, \ldots \vdash G$ implies $JD_1, F_1, F_2, \ldots \vdash G_k$ for all $k \leqq e$. By Theorem 5 there is an i for every $k \leqq e$ such that $JD_1, F_{i_k} \vdash G_k$. By Lemma 7 the desired set is $F_{i_1}, \ldots, F_{i_e}$.

COROLLARY 6. *Let the closed formulas* G_i $(i \leqq n)$ *and* G *be* $(E\mathbf{x})(\bigwedge_k \phi_k^i = 0)$ *and* $(\mathbf{y})(\bigvee_k g_k \neq 0)$ *respectively. Then there is an integer* $e>0$ *with the property: if* F_i $(i<\omega)$ *belongs to* A_2 *and if* $JD_1, G_1, \ldots, G_n, F_1, \ldots \vdash G$ *holds, then there is a subset* $F_{i_1}, \ldots, F_{i_e}$ *such that already* $JD_1, G_1, \ldots, G_n, F_{i_1}, \ldots, F_{i_e} \vdash G$ *holds.*

Proof. The statement follows immediately from the previous corollary by considering instead $JD_1, F_1, F_2, \ldots \vdash \neg G_1 \vee \cdots \vee \neg G_n \vee G$ and by transforming $(\bigvee_i \neg G_i) \vee G$ into prenex normal form.

The last corollary cannot be generalized much further; as soon as we allow formulas F_i of other types as, e.g. $(x)(Ey)p(x, y)=0$, the corollary turns out to be false. This stems from the fact that if, e.g., $(x)(Ey)p(x, y)=0$ is among the F's then ideals of the form

$$\boldsymbol{B}(p(t_0, x_1), p(t_1(x_1), x_2), \ldots, p(t_{s-1}(x_1, \ldots, x_{s-1}), x_s))$$

appear in condition (b) of Theorem 3; no upper bound for s and for the number of prime components can be given. The next example shows that for the theory of rings the situation is somewhat different.

THEOREM 6. *Let* $\boldsymbol{M}$ *be the set of closed prenex standard formulas having the form*

$$(Q_1 x_1, \ldots, Q_s x_s)\Big(\bigwedge_i g_i = 0 \wedge \Big(\bigwedge_j \bigvee_k f_{jk} \neq 0\Big)\Big).$$

Let G *be a closed prenex standard formula having the form*

$$(P_1 y_1, \ldots, P_t y_t)\Big(\bigvee_i \phi_i = 0 \vee \bigvee_k \psi_k \neq 0\Big).$$

Then $R_0, \boldsymbol{M} \vdash G$ *implies the existence of an* i_0 *such that already*

$$\boldsymbol{M}, R_0 \vdash (P_1 y_1, \ldots, P_t y_t)\Big(\phi_{i_0} = 0 \vee \bigvee_k \psi_k \neq 0\Big)$$

is true.

We will give the proof of Theorem 5 only for a special case, which however will contain all the essential features of the general case. The proof of the general case is a somewhat lengthy but straightforward elaboration of the arguments given below; it would require the introduction of a large number of sub- and superscripts. The case which we are going to consider is that where all formulas of $\boldsymbol{M}$ are of the following form:

$$(Q_1x_1, \ldots, Q_sx_s)(a = 0 \wedge (b \neq 0 \vee c \neq 0)).$$

Proof of Theorem 6. Obviously it is sufficient to consider a finite set $\boldsymbol{M} = \{F_1, \ldots, F_n\}$. Let F_i be $(Q_1^i x_1, \ldots, Q_{n_i}^i x_{n_i})(a_i = 0 \wedge (b_i \neq 0 \vee c_i \neq 0))$. Denote the formulas $(a_i \wedge (b_i \neq 0 \vee c_i \neq 0))$, $(\bigvee_i \phi_i = 0 \vee \bigvee_k \psi_k \neq 0)$ and

$$(P_1y_1, \ldots, P_ty_t)\Big(\bigvee_i \phi_i = 0 \vee \bigvee_k \psi_k \neq 0\Big)$$

by A_i, B and G respectively. Assume R_0, $\boldsymbol{M} \vdash G$. By Theorem 3 there is a right-matrix $M' = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_q\}$ of G and a left-matrix $M_i = \{\boldsymbol{v}_1^i, \ldots, \boldsymbol{v}_{P_i}^i\}$ of F_i for all $i \leqq n$ such that

(a) $M_1, \ldots, M_n$ and M' satisfy condition E with respect to $F_1, \ldots, F_n$ and G,

(b) the formula $\bigwedge_{i\alpha} A_i[\boldsymbol{v}_\alpha^i] \supset \bigvee_\beta B[\boldsymbol{w}_\beta]$ is provable from R_0.

After a few propositional transformations we conclude from (b) that

$$\bigvee_{i,\alpha} (b_i[\boldsymbol{v}_\alpha^i] = 0 \wedge c_i[\boldsymbol{v}_\alpha^i] = 0) \vee \Big(\bigvee_{j,\beta} \phi_j[\boldsymbol{w}_\beta] = 0\Big) \vee \Big(\bigvee_{i,\alpha} a_i[\boldsymbol{v}_\alpha^i] \neq 0\Big) \vee \Big(\bigvee_{k,\beta} \psi_k[\boldsymbol{w}_\beta] \neq 0\Big)$$

is provable from R_0. Let $z_1, \ldots, z_N$ be the set of variables occurring in at least one of the M_i's or in M'. Denote by J the polynomial ideal with respect to $\boldsymbol{I}[z_1, \ldots, z_N]$ generated by all the polynomials $a_i[\boldsymbol{v}_\alpha^i]$ and $\psi_k[\boldsymbol{w}_\beta]$. Then according to Corollary 4 either

(1) there is an i and an α such that $b_i[\boldsymbol{v}_\alpha^i]$ and $c_i[\boldsymbol{v}_\alpha^i]$ are in J or else

(2) there is a j_0 and a β_0 such that $\phi_{j_0}[\boldsymbol{w}_{\beta_0}]$ is in J.

Assume first (1). Then it follows from the corollary mentioned that

$$\bigvee_{i,\alpha} (b_i[\boldsymbol{v}_\alpha^i] = 0 \wedge c_i[\boldsymbol{v}_\alpha^i] = 0) \vee \Big(\bigvee_{i,\alpha} a_i[\boldsymbol{v}_\alpha^i] \neq 0\Big) \vee \Big(\bigvee_{k,\beta} \psi_k[\boldsymbol{w}_\beta] \neq 0\Big)$$

or equivalently $\bigwedge_{i,\alpha} A_i[\boldsymbol{v}_\alpha^i] \supset \bigvee_{k,\beta} \psi_k[\boldsymbol{w}_\beta] \neq 0$ is provable from R_0. Denote the term $y_i - y_i$ by $f_i(y_1, \ldots, y_t)$, let G' be the formula

$$(P_1y_1, \ldots, P_ty_t)\Big(\bigvee_i y_i - y_i \neq 0 \vee \bigvee_k \psi_k \neq 0\Big)$$

and denote the quantifier-free part of G' by B'. Obviously M' is a right-matrix of G', furthermore $M_1, \ldots, M_n$ and M' satisfy E with respect to $F_1, \ldots, F_n$ and G', as is easy to see, and finally $\bigwedge_{i,\alpha} A_i[\boldsymbol{v}_\alpha^i] \supset \bigvee_\beta B'[\boldsymbol{w}_\beta]$ is provable from R_0. Hence Theorem 3 implies $R_0, F_1, \ldots, F_n \vdash G'$, that is,

$$R_0, \boldsymbol{M} \vdash (P_1y_1, \ldots, P_ty_t)\Big(\phi_{j_0} = 0 \vee \bigvee_k \psi_k \neq 0\Big)$$

for any j_0 which proves the statement in this case. Now assume case (2). Then we conclude from Corollary 4 that

$$\bigvee_{i,\alpha}(b_i[v_\alpha^i] = 0 \wedge c_i[v_\alpha^i] = 0) \vee \phi_{j_0}[w_{\beta_0}] = 0 \vee \bigvee_{i,\alpha} a_i[v_\alpha^i] \neq 0 \vee \bigvee_{k,\gamma} \psi_k[w_\gamma] \neq 0$$

is a consequence of R_0. Denoting again $y_i - y_i$ by $f_i(y_1, \ldots, y_t)$ we find after a few propositional transformations that

$$\bigwedge_{i,\alpha} A_i[v_\alpha^i] \supset \Big(\phi_{j_0}[w_\beta] = 0 \vee \bigvee_j f_j[w_\beta] \neq 0 \vee \bigvee_k \psi_k[w_\beta] \neq 0\Big)$$

is provable from R_0. Denote $\phi_{j_0} = 0 \vee \bigvee_j f_j \neq 0 \vee \bigvee_k \psi_k \neq 0$ by B'' and

$$(P_1 y_1, \ldots, P_t y_t) B''$$

by G''. Again M' is a right-matrix of G'', furthermore $M_1, \ldots, M_n$ and M' satisfy E with respect to $F_1, \ldots, F_n$ and G'' and finally $\bigwedge_{i,\alpha} A_i[v_\alpha^i] \supset \bigvee_\beta B''[w_\beta]$ is provable from R_0. By Theorem 3 this implies

$$R_0, \boldsymbol{M} \vdash (P_1 y_1, \ldots, P_t y_t)\Big(\phi_{j_0} = 0 \vee \bigvee_k \psi_k \neq 0\Big),$$

which proves the statement also in this case.

A special case of Theorem 5 is

COROLLARY 6. *Let $\boldsymbol{M}'$ be the set of closed formulas of the form*

$$(Q_1 x_1, \ldots, Q_s x_s) p(x_1, \ldots, x_s) = 0.$$

If A_i, B_k $(i, k < \omega)$, $G_1, \ldots, G_n$ and $F_1, \ldots, F_m$ are formulas all in $\boldsymbol{M}'$ such that

$$R_0, A_1, A_2, \ldots, \neg B_1, \neg B_2, \ldots \vdash \bigvee_i G_i \vee \bigvee_k \neg F_k$$

then there is an i such that already

$$R_0, A_1, A_2, \ldots, \neg B_1, \neg B_2, \ldots \vdash G_{i_0} \vee \bigvee_k \neg F_k$$

holds.

A consequence of this is

COROLLARY 7. *Let $\boldsymbol{M}'$ be as in Corollary 5 and let $\boldsymbol{M}^*$ be the smallest set of formulas such that*

(a) *if $A \in \boldsymbol{M}'$ then $A \in \boldsymbol{M}^*$,*

(b) *if $A, B \in \boldsymbol{M}^*$ then $A \wedge B$, $A \vee B$, $\neg A$ in $\boldsymbol{M}^*$.*

With each formula $G \in \boldsymbol{M}^*$ one can associate an integer $e > 0$ with the property: if $R_0, G \vdash \bigvee_i B_i \vee \bigvee_k \neg C_k$ $(i \leqq n, k \leqq m)$ and if $B_i, C_k \in \boldsymbol{M}'$ then there are formulas $B_{i_1}, \ldots, B_{i_e}$ such that already $R_0, G \vdash \bigvee_s B_{i_s} \vee \bigvee_k \neg C_k$ holds.

Proof. Without restriction we may assume that G is $\bigwedge_i \bigvee_j A_{ij}$ where A_{ij} is either a formula of M' or the negation of such a formula; we assume $i \leqq a, j \leqq b_i$. By τ we denote the set of sequences $\alpha = \{\alpha_1, \ldots, \alpha_a\}$ with $\alpha_i \leqq b_i$. Because of R_0, G

$\vdash \bigvee_i B_i \vee \bigvee_k \neg C_k$ and $\bigwedge_i A_{i\alpha_i} \supset G$ for $\alpha \in \tau$ it follows that $R_0, A_{1\alpha_1}, \ldots, A_{a\alpha_a} \vdash \bigvee_i B_i \vee \bigvee_k \neg C_k$ holds for any $\alpha \in \tau$; but this, together with the previous corollary implies the existence of a $B_{k(\alpha)}$ such that already $R_0, \bigwedge_i A_{i\alpha_i} \vdash B_{k(\alpha)} \vee \bigvee_k \neg C_k$ is true. If we now take into account the following identity of propositional calculus

$$\bigwedge_{\alpha\in\tau}\Big(\bigwedge_i A_{i\alpha_i} \supset B_{k(\alpha)} \vee \bigvee_k \neg C_k\Big)\cdot\supset\cdot\Big(\bigwedge_i \bigvee_{\alpha\in\tau} A_{i\alpha_i} \supset \bigvee_{\alpha\in\tau} B_{k(\alpha)} \vee \bigvee_k \neg C_k\Big)$$

the statement of the corollary follows by choosing for e the number of elements in τ.

VII. **Another application.** In this section we discuss a slightly different kind of application. We will only prove the first of the theorems to be mentioned below. The proofs of the other theorems are omitted in view of their length.

THEOREM 7. *Let F_i $(i \leqq m)$ be of the form $(Q_1^i x_1, \ldots, Q_{n_i}^i x_{n_i}) f_i(x_1, \ldots, x_{n_i}) \neq 0$. Let $\phi(z_1, z_2)$ be a term such that $|\phi(z_1, z_2)|$ has no zero (ξ_1, ξ_2) constructible by means of ruler and compass. If $JD_1, F_1, \ldots, F_m, (x)(Ey)(x-y^2=0)$ are consistent then so are $JD_1, F_1, \ldots, F_m, (x)(Ey)(x-y^2=0), (z_1, z_2)\phi=0$.*

Proof. Call for simplicity an n-tuple $(\xi_1, \ldots, \xi_n)$ of real or complex numbers to be c.r.c. if its components ξ_i are constructible by means of ruler and compass.

(a) We first consider the case where all quantifiers Q_k^i are universal. Assume the assumption of the theorem to be true and assume in addition

$$JD_1, F_1, \ldots, F_m, (x)(Ey)(x-y^2 = 0) \vdash (Ez_1, z_2)\phi = 0;$$

we show that a contradiction arises. Denote $x-y^2=0$ by $g(x, y)$ and $(x)(Ey) \cdot (x-y^2=0)$ by G. From Theorem 3 it follows that there are left-matrices $M_i = \{\boldsymbol{u}_1^i, \ldots, \boldsymbol{u}_{p_i}^i\}$ of F_i $(i \leqq m)$, a left-matrix $M = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_q\}$ of G and a right-matrix $M' = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s\}$ of $(Ez_1, z_2)\phi = 0$ such that (b) and (c) of Theorem 3 are satisfied. Condition (c) in particular implies that the following formula is provable from JD:

$$\text{(I)} \qquad \bigvee_{i,\alpha} f_i[\boldsymbol{u}_\alpha^i] = 0 \vee \bigvee_\gamma \phi[\boldsymbol{w}_\gamma] = 0 \vee \bigvee_\beta g[\boldsymbol{v}_\beta] \neq 0.$$

If on the other hand we investigate the restrictions imposed by E on the form of the vectors $\boldsymbol{u}_\alpha^i$, $\boldsymbol{v}_\beta$, $\boldsymbol{w}_\gamma$, we find with a bit of work that there are variables $y_1, \ldots, y_s$ such that after a suitable renumbering of M the following holds:

(1) $\boldsymbol{v}_\beta$ has the form (t_β, y_β) where t_β is a term containing no other variables than $y_1, \ldots, y_{\beta-1}$ (in particular t_1 is a constant term),

(2) all terms which appear as components of an $\boldsymbol{u}_\alpha^i$, $\boldsymbol{w}_\gamma$ contain no other variables than $y_1, \ldots, y_s$.

Lemma 7 applied to formula (I) yields an integer $e > 0$ such that

$$\text{(II)} \qquad \Big(\prod_{i\alpha} f_i[\boldsymbol{u}_\alpha^i]\Big)^e \Big(\prod_\gamma \phi[\boldsymbol{w}_\gamma]\Big)^e \in \boldsymbol{B}(t_1 - y_1^2, \ldots, t_s - y_s^2)$$

holds. Denote the ideal on the right-hand side by J; let $q_1 \cap \cdots \cap q_b$ be a primary decomposition of J and p_i the prime ideal associated with q_i. Every zero of p_i is a zero of J, every zero of J is c.r.c., hence so is every zero of p_i. Therefore $\phi[\boldsymbol{w}_\gamma] \notin p_k$ for all γ, k, that is for every k there are i, α such that $f_i[\boldsymbol{u}_\alpha^i] \in p_k$. This in turn implies the existence of an integer d such that

$$\text{(III)} \qquad \left(\prod_{i\alpha} f_i[\boldsymbol{u}_\alpha^i]\right)^d \in J$$

holds. Combining this with Lemma 4 one finds that

$$\text{(IV)} \qquad \bigvee_{i\alpha} f_i[\boldsymbol{u}_\alpha^i] = 0 \vee \bigvee_{\beta} (t_\beta - y_\beta^2) \neq 0$$

is provable from JD_1. But $M_1, \ldots, M_m$ and M clearly satisfy E with respect to $F_1, \ldots, F_m$ and $(Ex)(y)(x-y\neq 0)$; in addition M_i is a left-matrix of F_i and M a right-matrix of $(Ex)(y)(x-y\neq 0)$. This, together with (IV) and Theorem 3 implies

$$F_1, \ldots, F_m, JD_1 \vdash (Ex)(y)(x-y \neq 0),$$

giving a contradiction.

(b) If the Q_k^i are allowed to be arbitrary quantifiers, the reasoning above remains the same up to the point where the form of the vectors $\boldsymbol{u}_\alpha^i$, $\boldsymbol{v}_\beta$, $\boldsymbol{w}_\gamma$ is investigated. Now one finds variables $x_1, \ldots, x_a$, $y_1, \ldots, y_s$ such that after an eventual renumbering of M the following holds:

(1) $\boldsymbol{v}_\beta$ is (t_β, y_β) and t_β contains no other variables than $x_1, \ldots, x_a, y_1, \ldots, y_{\beta-1}$,

(2) all terms which appear as components of some $\boldsymbol{u}_\alpha^i$, $\boldsymbol{w}_\gamma$ contain only variables from the list $x_1, \ldots, x_a, y_1, \ldots, y_s$. Again one finds relation (II) in part (a) to hold for some e. If we succeed to show that no prime ideal p_i (with p_i, q_i, J as in part (a)) contains a $\phi[\boldsymbol{w}_\gamma]$, then we can proceed as under (a), obtaining thus a contradiction. This is achieved if we can show that each p_i has a zero c.r.c. The reasoning sketched below produces such a zero. First one notes

(1) J has dimension a,

(2) if $\Delta(x_1, \ldots, x_a)$ is a nonvanishing polynomial in $x_1, \ldots, x_a$ then

$$J_\Delta = \boldsymbol{B}(\Delta, t_1 - y_1^2, \ldots, t_s - y_s^2)$$

has dimension $\leqq a-1$.

Now J has dimension a as noted, its basis contains s polynomials and there are $s+a$ variables. According to [2, p. 125] each p_i has dimension a. In addition the $x_1, \ldots, x_a$ are independent with respect to p_i; otherwise there would be a

$$\Delta(x_1, \ldots, x_a) \in p_i,$$

hence the set of zeros of p_i is a subset of the set of zeros of J_Δ, and this together with (2) would contradict the fact that p_i has dimension a. Hence [2, pp. 101–112] there is an a-dimensional complex neighborhood U_i such that for every choice $(\xi_1, \ldots, \xi_a)$

from U_i there are complex numbers $\zeta_1, \ldots, \zeta_s$ such that $(\xi_1, \ldots, \xi_a, \zeta_1, \ldots, \zeta_s)$ is a zero of p_i. If in particular the ξ_k are rational complex numbers, then, since

$$t_j(\xi_1, \ldots, \xi_a, \zeta_1, \ldots, \zeta_{j-1}) - \zeta_j^2 = 0$$

for $j \leqq s$, the ζ_k's are necessarily c.r.c. which concludes the proof.

The argument above, in particular properties (1) and (2) of J, could easily be made rigorous by using elementary devices from algebraic geometry such as presented in [2], [4].

This theorem allows a generalization, namely

THEOREM 8. *Let $F_1, \ldots, F_n$ be a list of formulas with F_i of the form*

$$(E\mathbf{y}_m)p_i(\mathbf{x}_n, \mathbf{y}_m) = 0$$

(with $\mathbf{x}_n$, $\mathbf{y}_m$ as abbreviations for $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_m)$) such that

(a) *$p_i(\mathbf{x}_n, \mathbf{y}_m) \notin I[\mathbf{x}_n]$,*

(b) *if p_i is $\sum A^i_{i_1 \ldots i_m}(\mathbf{x}_n) y_1^{i_1} \cdots y_m^{i_m}$ then 1 is an element of the ideal J_i, whose basis consists precisely of all the polynomials $A^i_{i_1 \ldots i_m}(\mathbf{x}_n)$,*

(c) *each p_i has degree $\leqq 4$ with respect to each y_k.*

Let F be constructed from the F_i's by means of $\wedge$, $\vee$, $\neg$, E, $\forall$ and let $g_1(\mathbf{z}), \ldots, g_s(\mathbf{z})$ be terms such that no $g_i(\mathbf{z})$ has a zero constructible by means of ruler and compass. If F, JD_1 are consistent, then so are $\bigwedge_i (\mathbf{z}) g_i(\mathbf{z}) \neq 0$, F, JD_1.

This theorem can be generalized considerably in two directions: first one can use concepts from Galois theory which are more general than the notion of a number constructible by means of ruler and compass, secondly the class of formulas F_i which serve as basis for the construction of F can be chosen much larger. A variant of Theorem 8 is

THEOREM 9. *Let $F_1, \ldots, F_n$ be as in Theorem 8. Let $g_1(\mathbf{x}), \ldots, g_s(\mathbf{x})$ be terms such that no $g_i(\mathbf{x})$ has a zero constructible by means of ruler and compass, except possibly $(0, \ldots, 0)$. Let $\phi(z_1, \ldots, z_k)$ be a term representing an irreducible polynomial of degree $\leqq 4$ with respect to each z_i; in addition $2 \leqq k$ and $\phi(0, \ldots, 0) = 0$ are assumed. If F, $\bigwedge_i (\mathbf{x})(g_i(\mathbf{x}) = 0 \supset \bigwedge_j x_j = 0)$, JD_1 are consistent then $(\mathbf{z})(\phi(\mathbf{z}) = 0 \supset \bigwedge_j z_j = 0)$ is not provable from this set of formulas.*

The main idea used in the proofs of Theorems 8 and 9 is already present in the proof of Theorem 7. The details however are now much more involved since the ideals which one encounters have a structure which is more complex than that of the J_i in the proof of Theorem 7. In order to handle the singular points which are familiar in elimination theory quite a considerable amount of elementary algebraic geometry is necessary; for this reason we have omitted the proofs of Theorems 8 and 9.

ACKNOWLEDGEMENTS. The author wishes to express his gratitude to Professor G. Kreisel, with whom he had many fruitful discussions on the topics presented

here, to Professor W. Habicht for his helpful suggestions concerning ideal theory and to Battelle Institute Geneva whose financial aid made this work possible.

References

1. M. Davis and H. Putnam, *Diophantine sets over polynomial rings*, Illinois J. Math. 7 (1963), 251–256.
2. W. Gröbner, *Moderne algebraische Geometrie*, Springer-Verlag, Berlin, 1949.
3. S. C. Kleene, *Introduction to metamathematics*, North-Holland, Amsterdam, 1962.
4. B. L. van der Waerden, *Moderne Algebra*, Vol. 2, Springer-Verlag, Berlin, 1937.

University of Basel,
Basel, Switzerland