ALGORITHMS IN ALGEBRA

Abraham Robinson

[*Robinson planned to deliver a lecture on the topic of "algorithms in algebra" at the meeting on algebra and logic held at Monash University (Australia) in January–February 1974. However, his illness made it impossible for him to attend the meeting; it also prevented him from ever finishing the paper. What he left was a preliminary manuscript.*

It seemed clear that the paper was worth publishing in some form, and we attempted to produce a revised version adhering as closely as possible to Robinson's own plan and ideas. The most substantial changes were made in sections 5 and 8; in the former case we benefited from a set of notes from a lecture Robinson gave on the subject at Yale.

It goes without saying that in publishing this manuscript we accept responsibility for any errors. —D. H. Saracino and V. B. Weispfenning, editors of *Model Theory and Algebra: A Memorial Tribute to Abraham Robinson*]

1. *Introduction.* The notion of a computable function or relation in the domain of natural numbers is by now standard, and the fact that it is explicated correctly by the notion of recursivity (Church's thesis) is no longer open to doubt. Even so it is an intriguing philosophical problem to what category exactly this notion belongs (e.g., depending on one's school of thought, analytic, synthetic a priori, theoretical, empirical). Let me begin this talk by drawing your attention to the fact that the notion of computability in algebra is less clear, and that here it is even not obvious whether we are aiming at the explication of an objectively given notion, or at the description of the various activities of a number of individuals which they considered to be "effective" or "realizable in a finite number of steps."

A major figure in the history of effective methods in algebra was Kronecker. Among other things, he proposed [7] a method by which the reducibility of a polynomial of one variable with rational coefficients can be tested, and another by which the reducibility of polynomials of several variables is reduced to the reducibility of polynomials in a single variable. In a more advanced area he showed how to determine, effectively, the irreducible components of an algebraic variety (see below). However, the formal tools available in Kronecker's time precluded a precise determination of the notion of effectiveness, even if he had been disposed philosophically to embark on such an enterprise.

Kronecker was not the first mathematician to employ effective methods. He was the first to do so consciously, because until about 1850 mathematicians were not even aware of a possible distinction between abstract and effective mathematics. Thus, the determination of the number of real roots of a polynomial in a given interval, which

antedates that period (Sturm) is a beautiful example of an effective method, and, as you know, it is the basis of Tarski's decision method for the algebraic theory of real numbers. But even earlier (as in the first book which contains the term in its title) "Algebra" was regarded as a practical method of computation, and the name of the author of that book (al-Khowarizmi) was immortalized in the very word "algorithm."

2. *Previous work.* The first paper that discusses the notion of effectiveness in algebra is that of Shepherdson and Frölich [15]. They reduce the notion of effectiveness in algebra to the corresponding notion in arithmetic by assuming that the structure within which a certain problem is to be solved effectively is given *recursively*, i.e. that it is, or is represented by, recursive functions. Among the questions treated by Shepherdson-Frölich is that of the existence of an effective method to test the reducibility of an equation. They conclude, following an earlier argument of van der Waerden, that there is no general decision procedure for this problem (uniformly applicable to all fields). More precisely, they "construct" (in the indicated sense) a particular field which has no decision procedure for this problem.

It may be argued that an effective procedure in *an* algebraic structure should be independent of the recursive nature of the structure, more generally it should be equally applicable to an algebraic structure (of a given type) which is not countable. In this vein, there exist several papers (Fraissé [3], Peter [9], Lambert [8]). Lambert introduces a kind of mixed recursive schemes which involve both elements of a given algebraic structure and natural numbers. The motivation for this is that even in an arbitrary algebraic structure, e.g. a group, which does not involve natural numbers a priori, they may intervene as soon as we try to introduce the powers of an element, by definition, as a function of two variables, a in the structure and n in the natural numbers. A theory of inductive definitions which has some similarities with Lambert's has been developed more recently by Moschovakis and others.

A theory of algebraic algorithms which is closer in spirit to contemporary model theory on the one hand and to computer programming on the other, has been developed in recent years by Erwin Engeler [2]. Let M be a model-theoretic structure. Engeler considers programs consisting of commands of the following kind. (i) operational instructions: do ψ then go to j (where ψ is an operation and j is the label of another instruction), and (ii): if ϕ then go to j, else go to k, where ϕ is a statement concerning the structure whose truth or falsehood is revealed by oracle (i.e., is supposed known, for the purpose of carrying out the program). The operations are of the form $x_j := g_k(x_{j_1}, \ldots, x_{j_k})$, e.g. $x_j := x_{j+1}$, which implies that we may delete the content of cell x_j and replace it by the content of cell x_{j+1}. Engeler associates a formula of an infinitary language with each program, so that it holds in a structure iff the program is effective for it (terminates).

Finally, it is appropriate to mention here a notion introduced by Paul J. Cohen in connection with his work on decision procedures [1]. The papers listed above have stimulated the present work in varying degrees. However, they do not address themselves to the main problem considered here (see below).

3. *Purpose of Present Investigation.* In the present paper, we shall study the connections between (i) the availability of an algebraic algorithm, (ii) definability in a first-order theory, and (iii) the existence of certain bounds in relation to an algebraic property.

The fact that (iii) can be a stepping stone to (i) is a matter of common experience. For example, suppose that we are given a field F and polynomials $f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ in $F[x_1, \ldots, x_n]$, for specified n, all of degrees less than positive integer d. We are asked to decide whether or not g belongs to the ideal generated by $f_1, \ldots, f_k$, in other words, whether or not

$$* \qquad g = \Sigma\, h_j f_j$$

where $h_1, \ldots, h_k$ are again polynomials in the given $F[x_1, \ldots, x_n]$. It is not obvious how to determine this. However, once we are told that there is a bound $b = b(n, d)$ such that if (*) is satisfiable at all then it is satisfiable by polynomials h_j of degrees less than or equal to b, then we may substitute a polynomial of degree b with unknown coefficients in (*) and we then obtain a system of linear equations whose solvability settles the problem. It is in fact the actual determination of such a bound which seems involved historically, either directly, or through the proof of its existence by model-theoretic means. Moreover, as long as no bound is known, the solvability of (*) is represented by a predicate which is an infinite disjunction of existential predicates of the coefficients of f_j, g, but this is reduced to a finite disjunction and hence to a predicate of the lower predicate calculus, once a bound is known. Conversely, if we know that the infinite disjunction is equivalent to a predicate of the lower predicate calculus then it must already be equivalent to a finite subdisjunction, by the compactness theorem. While in the case under consideration this is not the way things went in the first place, there are other cases, in particular in connection with Hilbert's seventeenth problem, where the existence of such a bound was so determined in the first place.

In the present paper, we consider the converse question. Does the existence of an algebraic algorithm always imply the definability of the predicate in question in the lower predicate calculus, and hence, in cases where the predicate is known to be equivalent to an infinite disjunction, a reduction to a finite subdisjunction? We shall show that this is indeed the case, for an appropriate definition of the notion of an algebraic algorithm. Whether this definition is the right one is, as in the arithmetical case, not a matter of a purely mathematical argument. In the present context the argument is evidently stronger the weaker the definition. Accordingly, we shall base our argument on an algorithm whose effectiveness is in fact relative to a particular oracle, and discuss various possibilities within that definition subsequently.

The main application of our result will be a clarification of the situation in Differential Algebra where a number of important decision problems still await solution.

4. *Auxiliary results from model theory.* Let K be a consistent set of axioms in the lower *PC* including equality, relations and functions, and let Σ be the class of models of K.

We suppose that Σ is closed under unions of ascending chains. By the theorem of Chang-Łoś-Suszko this is the same as to assume that K is logically equivalent to a set of $\forall\exists$ sentences. Accordingly, we shall assume that K *is* a set of $\forall\exists$ sentences.

A set K^* in the vocabulary of K with class of models Σ^* is called the model completion of K if the following conditions are satisfied. (i) $\Sigma \supset \Sigma^*$, (ii) every $M \in \Sigma$ can be embedded in an $M^* \in \Sigma^*$, (iii) if $M \in \Sigma$ and $M_1, M_2 \in \Sigma^*$ are such that $M \subset M_1$, $M \subset M_2$, then for any sentence X in the vocabulary of M (i.e. with constants for any of the individuals of M), $M_1 \models X$ if and only if $M_2 \models X$.

It is known that for any given K as specified there can be up to logical equivalence not more than one K^* and to this extent we are justified in talking of *the* model completion [12]. The model completion of the theory of commutative fields (and also of course integral domains) is the theory of algebraically closed fields and the model completion of the theory of ordered fields is the theory of real closed ordered fields. The theory of groups and the theory of formally real fields have no model completions (although they have substitutes which do not concern us here [14]). K^*, if it exists, is also inductive and hence may be supposed to consist of $\forall\exists$ sentences.

Let $Q^*(x_1, \ldots, x_n)$, $n \geq 1$, be any predicate in the language of K and let K^* be the model completion of K. Then there exists an existential predicate $Q(x_1, \ldots, x_n)$ such that the following condition is satisfied.

Let $M \in \Sigma$, $M^* \in \Sigma^*$, $M^* \supset M$, and let $a_1, \ldots, a_n$ denote any elements of M. Then $M \models Q(a_1, \ldots, a_n)$ if and only if $M \models Q(a_1, \ldots, a_n)$. Q is called a *resultant* or *test* for Q. Moreover, if the theory of Σ is universal, i.e. if K may be taken to consist of universal axioms only, then for $n \geq 1$, $Q(x_1, \ldots, x_n)$ may be chosen so as to be free of quantifiers.

5. *Algorithmic Instructions.* The language in which we shall formulate our algorithmic operations is the same as before, but in addition we use IF, PUT, and a symbol: $=$ (We use PUT where in a computer language we might use DO, because DO is not appropriate to instantiations (see below).) We also use variables called *computational variables:* $\alpha, \beta, \ldots$

Let V be a fixed vocabulary, R a k-ary relation symbol not in V, and g a k-ary function symbol not in V. Q, Q', will always denote well-formed formulae in the vocabulary V.

We distinguish the following kinds of instructions.

5.1. A *standard instruction I* is of the form

$$\text{IF } Q(\beta_1, \ldots, \beta_m) \cdot \quad \text{PUT } \gamma := f(\xi_1, \ldots, \xi_n),$$

where γ is not one of the $\beta_1, \ldots, \beta_m, \xi_1, \ldots, \xi_n$ but where some of these may coincide. If $m = 0$ and $Q(x_1, \ldots, x_m)$ is a tautology then we call the instruction unconditional. Here, f is a composite function of our language. We say γ *is introduced by* I.

5.2. An *instantiation I* is of the form

$$\text{IF } (\exists z_1) \ldots (\exists z_n)\, Q(\beta_1, \ldots, \beta_m, z_1, \ldots, z_n)$$
$$\text{PUT } \xi_1, \ldots, \xi_n : Q(\beta_1, \ldots, \beta_m, \xi_1, \ldots, \xi_n),$$

where $\xi_1, \ldots, \xi_n$ are not among $\beta_1, \ldots, \beta_m$. We say $\xi_1, \ldots, \xi_n$ *are introduced by I*.

5.3. *Final Instructions*. These are of one of the following forms:

(i) IF $Q(\beta_1, \ldots, \beta_m)$ PUT $R(\alpha_1, \ldots, \alpha_k)$
(ii) IF $Q(\beta_1, \ldots, \beta_m)$ PUT $\neg R(\alpha_1, \ldots, \alpha_k)$
(iii) IF $Q(\beta_1, \ldots, \beta_m)$ PUT $\alpha_k = g(\alpha_1, \ldots, \alpha_{k-1})$, $k > 0$.

We refer to instructions of form (i) and (ii) as *positive* and *negative final* instructions, respectively, and to $\alpha_1, \ldots, \alpha_k$ as final *computational variables*.

Fix a k-tuple $\alpha_1, \ldots, \alpha_k$ of computational variables. By a *deduction d* for R or g, respectively, with *initial variables* $\alpha_1, \ldots, \alpha_k$ we mean a finite sequence of instructions as above, such that the following conditions are satisfied. The last and only the last instruction in d is a final instruction I of form 5.3 (i), (ii) or 5.3 (iii), respectively. In particular the final variables in I coincide with the initial variables of d. Every computational variable occurring in an instruction I in d is either an initial variable of d or has been introduced by a standard instruction or an instantiation I' in d preceding I. A computational variable introduced by a standard instruction or an instantiation I in d does not occur in any instruction I' in d preceding I.

We now regard a deduction as a rule for interpreting the computational variables as elements of a specific structure, except for the final instruction which we interpret as defining an instance of a relation or function. In fact, the procedure is obvious. Suppose we are given a structure M which *includes* V in its vocabulary, $\alpha_1, \ldots, \alpha_k \in M$, and a deduction d with initial variables $\alpha_1, \ldots, \alpha_k$. We interpret $\alpha_1, \ldots, \alpha_k$ by $\alpha_1, \ldots, \alpha_k$, respectively. If γ is introduced by a standard instruction of form 5.1 and $\beta_1, \ldots, \beta_m, \xi_1, \ldots, \xi_n$ have already been interpreted by $b_1, \ldots, b_m, c_1, \ldots, c_n \in M$, then we interpret γ by $f(c_1, \ldots, c_n) \in M$, if $M \models Q(b_1, \ldots, b_m)$. Otherwise we stop. If $\xi_1, \ldots, \xi_n$ are introduced by an instantiation of form 5.2 and $\beta_1, \ldots, \beta_m$ have already been interpreted by $b_1, \ldots, b_m \in M$, then we interpret $\xi_1, \ldots, \xi_n$ —to some extent arbitrarily—by any n-tuple $c_1, \ldots, c_n$ of elements of M which makes $Q(b_1, \ldots, b_m, c_1, \ldots, c_n)$ true in M in case $M \models (\exists z_1) \ldots (\exists z_n)\, Q(b_1, \ldots, b_m, z_1, \ldots, z_n)$. Otherwise we stop. We say d *is effective at* $a_1, \ldots, a_k \in M$, if *some* such assignment of elements of M to computational variables mapping $\alpha_1, \ldots, \alpha_k$ onto $\alpha_1, \ldots, \alpha_k$ can be carried out for *all* instructions in d (i.e. does not stop before the final instruction of d).

Now let Σ be an arithmetical class of models, with vocabulary V, and let π be a set of deductions for R with common initial variables $\alpha_1, \ldots, \alpha_k$. Then we say π is a *program for R* in Σ, if

5.4. (i) (completeness condition) for all $M \in \Sigma$, $a_1, \ldots, a_k \in M$, there exists $d \in \pi$ such that d is effective at $a_1, \ldots, a_k \in M$,
and (ii) (consistency condition) for all $d, d' \in \pi$, all $M \in \Sigma$ and all $a_1, \ldots, a_k \in M$, if d and d' are effective at $a_1, \ldots, a_k$ in M, then the final instructions of d and d' are both positive or both negative.

Similarly, we define a set π of deductions for g with common initial variables $\alpha_1, \ldots, \alpha_k$, $k > 0$, to be a *program for g in* Σ, if

5.5. (i) (completeness condition) for all $M \in \Sigma$, and all $a_1, \ldots, a_{k-1} \in M$ there exists $a_k \in M$ and $d \in \pi$ such that d is effective at $a_1, \ldots, a_k$,
and (ii) (consistency condition) for all $M \in \Sigma$, and all $a_1, \ldots, a_{k-1} \in M$ there is at most one $a_k \in M$ such that a $d \in \pi$ is effective at $a_1, \ldots, a_k$.

Thus a program π for R (g) in Σ defines on every $M \in \Sigma$ a relation $R \subset M^k$ (a function $g: M^{k-1} \to M$).

We will also consider the case that the relation R (or the function g) is defined in advance on every $M \in \Sigma$. Then we say the program π is *correct* if the relation (or function) defined by π coincides with R (with g).

Next, we associate with every deduction d with initial variables $\alpha_1, \ldots, \alpha_k$ a formula $X_d(x_1, \ldots, x_k)$ in the vocabulary V. Choose a set of ordinary variables $x, y, \ldots$ in one-to-one correspondence with the computational variables. Denote the variables corresponding to $\alpha_1, \ldots, \alpha_k$ by $x_1, \ldots, x_k$. Let Y_d be the conjunction of all the following formulas:

(i) For every standard instruction of form 5.1 in d the formula $Q(y_1, \ldots, y_m) \wedge \wedge z = f(z_1, \ldots, z_n)$, where $y_1, \ldots, y_m, z, z_1, \ldots, z_n$ correspond to $\beta_1, \ldots, \beta_m, \gamma, \xi_1, \ldots, \xi_n$.
(ii) For every instantiation of form 5.2 in d the formula $Q(y_1, \ldots, y_m, z_1, \ldots, z_n)$, where $y_1, \ldots, y_m, z_1, \ldots, z_n$ correspond to $\beta_1, \ldots, \beta_m, \xi_1, \ldots, \xi_n$.
(iii) If d has final instruction of form 5.3, the formula $Q(y_1, \ldots, y_m)$, where $y_1, \ldots, y_m$ correspond to $\beta_1, \ldots, \beta_m$.

Let $X_d(x_1, \ldots, x_k)$ be the formula resulting from Y_d by existential quantification of all the free variables in Y_d except $x_1, \ldots, x_k$.

It is now apparent from the definition of X_d that d is effective at $a_1, \ldots, a_k \in M$ if and only if $M \models X_d(a_1, \ldots, a_k)$. As a consequence conditions 5.4 and 5.5 can be expressed in terms of the formulas X_d: Let K be a set of sentences in the vocabulary V and let Σ be the class of models of K. Then 5.4 (i) and (ii) are equivalent to

5.6. (i) $K \vdash (\forall x_1) \ldots (\forall x_k) \vee_{d \in \pi} X_d(x_1, \ldots, x_k)$
and (ii) $K \vdash \wedge_{d \in \pi^+,\, d' \in \pi^-} (\forall x_1) \ldots (\forall x_k) \neg (X_d(x_1, \ldots, x_k) \wedge X_{d'}(x_1, \ldots, x_k))$

where π^+ (π^-) is the set of deductions in π with positive (negative) final instruction. Similarly, 5.5 (i) and (ii) are equivalent to

5.7. (i) $K \vdash (\forall x_1) \ldots (\forall x_{k-1}) \bigvee_{d \in p} (\exists x_k) X_d(x_1, \ldots, x_k)$
and (ii) $K \vdash \bigwedge_{d,d' \in \pi} (\forall x_1) \ldots (\forall x_{k-1}) (\forall x_k) (\forall y) (X_d(x_1, \ldots, x_k) \wedge X_{d'}(x_1, \ldots, x_{k-1}, y) \rightarrow x_k = y)$.

Two programs are said to be *equivalent in* Σ, if they determine the same relation or function on every $M \in \Sigma$. Notice that every subset π' of a program π which is itself a program is equivalent in Σ to π.

We now see without difficulty:

5.8. *Basic Principle*. Every program π contains an equivalent subprogram π' which is finite.

Proof. Suppose π is a program for R in Σ and $\Sigma = \mathrm{Mod}(K)$.
Then by 5.6 (*i*)

$$K \models \bigvee_{d \in \pi} X_d(c_1, \ldots, c_k)$$

where $c_1, \ldots, c_k$ are new constants not in V. By the compactness theorem there exists a finite subset π' of π such that

$$K \models \bigvee_{d \in \pi'} X_d(c_1, \ldots, c_k), \text{ and so}$$
$$K \models (\forall x_1) \ldots (\forall x_k) \bigvee_{d \in \pi'} X_d(x_1, \ldots, x_k).$$

Since 5.6 (ii) is trivially satisfied for π', π' is also a program for R in Σ and hence equivalent to π.

If π is a program for a function g in Σ the argument is similar using 5.7 instead of 5.6. This proves our assertion.

As a consequence we have now the following.

Theorem 5.9. Let Σ be an arithmetical class and let π be a program for a relation R or a function g in Σ. Then R or g, respectively, is definable in Σ by a formula in the vocabulary V.

Proof. Suppose first that we are dealing with the case of a program π for a relation R in $\Sigma = \mathrm{Mod}(K)$. We may assume by the basic principle that π is finite.
Let

$$X^+(x_1, \ldots, x_k) = \bigvee_{d \in \pi^+} X_d(x_1, \ldots, x_k).$$

and let

$$X^-(x_1, \ldots, x_k) = \bigvee_{d \in \pi^-} X_d(x_1, \ldots, x_k).$$

Then by 5.6

$$K \vdash (\forall x_1) \ldots (\forall x_k) (X^+(x_1, \ldots, x_k) \vee X^-(x_1, \ldots, x_k))$$

and

$$K \vdash (\forall x_1) \ldots (\forall x_k) \neg (X^+(x_1, \ldots, x_k) \wedge X^-(x_1, \ldots, x_k)),$$

in other words the exclusive 'or'. Thus we may conclude that

$$(\forall x_1) \ldots (\forall x_k) (X^+(x_1, \ldots, x_k) \equiv R(x_1, \ldots, x_k))$$

and

$$(\forall x_1) \ldots (\forall x_k) (X^-(x_1, \ldots, x_k) \equiv \neg R(x_1, \ldots, x_k))$$

holds in Σ.

If π defines a function g in Σ, we may assume as above that π is finite. Then by 5.7 the formula

$$X(x_1, \ldots, x_k) = \bigvee_{d \in \pi} X_d(x_1, \ldots, x_k)$$

defines

$$g(x_1, \ldots, x_{k-1}) = x_k \text{ in } \Sigma.$$

Remark. Let π be a program for R in Σ. Suppose in particular that for all $d \in \pi$ the conditions Q occurring on the left hand side of the instructions in d are all existential. In that case X^+ and X^- are also existential, so that $R(x_1, \ldots, x_k)$ and its negation are both existential.

6. *Discussion*. We now have to consider the question to what extent our computations may be said to be *algorithmic*. First of all, can we really carry out each individual step? This must be supposed to be the case if the conditions are all quantifier-free, since the ability to carry out an actual basic operation must be presumed. Equally, we cannot really be said to decide an arbitrary well-formed formula except by "oracle." However, if a predicate is D, i.e. both existential and universal, the question does not have a clear answer.

For suppose

$$Q(x_1, \ldots, x_n) \equiv (\exists y_1) \ldots (\exists y_m) Q_1(x_1, \ldots, x_n, y_1, \ldots, y_m)$$
$$\equiv (\forall z_1) \ldots (\forall z_k) Q_2(x_1, \ldots, x_n, z_1, \ldots, z_k),$$

where Q_1 and Q_2 are free of quantifiers. Then

$$\neg Q(x_1, \ldots, x_n) \equiv (\exists z_1) \ldots (\exists z_k) \neg Q_2(x_1, \ldots, x_n, z_1, \ldots, z_k).$$

It follows that if the structure M has an effective enumeration as would be the case if M is recursive in any of the senses mentioned above (Shepherdson-Frölich-Rabin) then we can actually check in each particular case whether or not $Q(x_1, \ldots, x_n)$ is verified. In particular, if in this case a program π has the property that all conditions occurring in instructions in π are D, then the relation or function determined by π is calculable. Also, in this case, we may find the x_j which are introduced by instantiation.

If we have elimination of quantifiers, then all predicates are equivalent to quantifier-free predicates. And in this case also, the predicate as given may be

existential, so if it has first been verified, by elimination of quantifiers, we may then, in the case of a recursive structure, as before, again find the examples of the instantiation by enumeration.

Notice that our deductions are not programs, in the sense that they have no go-to instructions. This is irrelevant to the main conclusion in which we are interested here.

However, once we have reduced the given program to one, π', consisting of a finite number of deductions, it is not difficult to turn this into a practical program, e.g. in the sense of Engeler. For this purpose, we need only a finite number of cells. We number the elements of π, $1, \ldots, k$, and in each of these we number the instructions $a_{j\ell}$, $1 \leq \ell \leq \lambda_j$. We now interpret the variables in one-to-one correspondence with cells. No erasing is necessary. The processing unit is supposed to carry out the individual step, i.e. enter data as by $x_j := a$ in the first available cell, verify conditions (by appealing to an oracle), and generally enter the name of an element of the given structure in the appropriate cell. In the case of instantiation this is somewhat indeterminate as indicated above. Here in fact, only if the structure is countable, and we are given an effective enumeration, is there any hope for success. In the case, we "play" the various deductions simultaneously, knowing that sooner or later one will arrive at a conclusion.

Let us now consider the converse problem. Suppose that we are given a program in the sense of Engeler. Can we transform it into a deduction of our kind?

The last step in Engeler's program is that a relation is to hold if the program terminates. Suppose that we also have another program which terminates if and only if the first program does not. We take our Engeler program, and apply to each variable x_j a second subscript which is raised by one whenever the variable occurs in an equation of the form $x_j :=$ an expression involving x_j.

Thus $x_j := x_j + 1$ becomes $x_{j,\ell+1} = x_{j,\ell} + 1$. And in any subsequent situation we also use the highest subscript that appeared previously. It is not difficult to see how to produce from finite pieces of the Engeler programs for R and $\neg R$ a set of deduction which constitute a program for R in our sense.

By contrast, our computability cannot be compared to the computability in the sense of Shepherdson-Frölich-Rabin. Thus, let us take the relative reducibility of polynomials in fields. This is expressed by an existential sentence. As such it is already computable by an existential condition in our language, although we know that it is not a computable problem in the sense of S-F-R. (Note here, that absolute reducibility is computable by all standards, since it permits elimination of quantifiers.) However, if our conditions are all quantifier-free, then our computations can be carried out in any recursive model.

Finally, we notice that in our set-up we do not have any reference to any universal bounds which may occur in a computation, for example the degree of a polynomial (see below). This is due to the fact that we are considering separately each given set of n data, e.g. the coefficients of a given polynomial. Since we have a total bound on the length of our computation it then follows that the number of coefficients of any other polynomial or even power series which may intervene must be subject to this bound also. We cannot go beyond this statement without further formalization.

7. *Introduction of functions.* The introduction of functions in place of existential quantifiers on one hand simplifies formulae. Also, it makes our computations subject to the supplement to the ϵ − theorems [6], as follows.

Suppose, we are given a universal set of axioms K. Suppose also that we have as a conclusion from it a sentence of the form

$$(\forall x_1) \ldots (\forall x_n)\,(\exists y_1) \ldots (\exists y_m)\, Q(x_1, \ldots, x_n, y_1, \ldots, y_m),$$

Q free of quantifiers. Then [6] asserts that there exist $t_{kj}\,(x_1, \ldots, x_n)$ such that

$$Q(x_1, \ldots, x_n, t_{11}(x_1, \ldots, x_n), \ldots, t_{1m}(x_1, \ldots, x_n)) \vee \ldots \vee \\ \vee Q(x_1, \ldots, x_n, t_{\ell 1}(x_1, \ldots, x_n), \ldots, t_{\ell m}(x_1, \ldots, x_n))$$

also is deducible from K. For $n = 0$, the terms in question are constant terms.

Now suppose that we have a set of $\forall\exists$ -axioms for a model-completion. We "Skolemize" the formulae by replacing each existential quantifier by a corresponding Skolem function symbol (e.g. in the case of an algebraically closed field). Then a certain measure of arbitrariness is introduced. For example, if ϕ_1 corresponds to $(\exists x)\,(x^2 - 2 = 0)$ and ϕ_2 corresponds to $(\exists x)(x^4 - 2 = 0)$ which are instances of the assertions that monic quadratic and biquadratic polynomials have a root then we cannot decide whether $\phi_2{}^2 - \phi_1 = 0$ or $\phi_2{}^2 + \phi_1 = 0$. In fact, given any field M one of these conditions may be satisfied in one algebraically closed extension of M and the other in another. Nevertheless in some cases we may still assume that the resulting set of axioms is model complete.

To see this, consider the theory of real closed ordered fields. Let M be a real closed ordered field, and suppose that M' is an extension in which a particular existential sentence

$$X = (\exists x_1) \ldots (\exists x_n)\, Q\,(x_1, \ldots, x_n)$$

holds. (Note that, because of the indeterminacy mentioned above it is not true that the algebraic closure with respect to the Skolemized language of any field is uniquely determined by that field (i.e. we do not know if $(\sqrt[4]{t})^2 = \sqrt[2]{t}$ or $(\sqrt[4]{t})^2 = -\sqrt[2]{t}$).) We define the square root function of a polynomial as its positive square root and the real root function of a polynomial of odd degree as its smallest. This can be represented by universal axioms, say

$$(\forall x_1) \ldots (\forall x_{2k+1})\,[\,(\phi(x_1, \ldots, x_{2k+1}))^{2k+1} + x_1\,\phi^{2k} + \ldots + x_{2k+1} = 0]$$ and

$$(\forall x_1) \ldots (\forall x_{2k+1})\,(\forall z)\,[z^{2k+1} + x_1 z^{2k} + \ldots + x_{2k+1} = 0 \supset \phi(x_1, \ldots, x_{2k+1}) \leq z].$$

With these definitions, it is not difficult to see that any ordered field has a unique extension which is prime for the situation. For this purpose, we only have to take the real closure and to define the ϕ as positive (in the case of a square root) or as the smallest root (in the case of polynomial of odd degree).

Relative model completeness can now be proved exactly as for real closed ordered fields in the usual language. Accordingly, we have elimination of quantifiers, because

we started out with a universal theory. Moreover, we even have completeness, because the real algebraic numbers prove to be a prime model.

The elimination of quantifiers makes instantiation more concrete in this case. Thus, suppose that we have a condition which is an existential statement

$$(\exists x_1) \ldots (\exists x_n)\, Q(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_m).$$

In the first place we may suppose here that Q is free of quantifiers. In the second place, the entire predicate is equivalent to some $Q_1(\alpha_1, \ldots, \alpha_m)$ which is quantifier-free. Also, if the given set of axioms is recursive then we may compute Q_1 from Q by proving $(\exists x_1) \ldots (\exists x_n)\, Q \equiv Q_1$.

In particular we now have

$$Q_1(y_1, \ldots, y_m) \supset (\exists x_1) \ldots (\exists x_n)\, Q(x_1, \ldots, x_n, y_1, \ldots, y_m).$$

Hence by the second ϵ-theorem, we have terms

$$t_{11}(y_1, \ldots, y_n), \ldots, t_{jr}(y_1, \ldots, y_n)$$

which instantiate the x, and we may actually find them by trial and error a finite number of times.

I can see no similar way to complement the corresponding set of axioms for algebraically closed fields.

[*Editors' note:* See the paper by Winkler in this volume.]

8. *On a theorem of Polya.* We mentioned at the beginning of this paper one way to establish the existence of bounds for certain polynomial solutions: In the case of real numbers the representability of a positive definite polynomial by sums of squares of rational functions which is realized for *all* real closed fields, implies the existence of a bound on the number of squares required and on the degrees of the numerators and denominators (for a given bound on the degree of the polynomial and the number of variables). This yields a result even for the classical case of the real numbers. It is trivial that generally speaking the validity of the argument ceases if we have the equivalence of an infinite disjunction to a *LPC* condition only in one model of the arithmetical class, e.g., the real numbers alone. Thus, $x=x$ is certainly equivalent in that case to

$$y=0 \vee y^2>x \vee y^2+y^2 > x \vee y^2+y^2+y^2 > x \vee \ldots.$$

Yet this ceases to be true if we replace the disjunction by a finite subdisjunction, even in that model alone. A less trivial example is revealed by a study of a theorem of Polya which is given in [4] as a (supposedly simpler) companion of Artin's theorem. Let $F(x_1, \ldots, x_n)$ be a form (homogeneous polynomial of degree $k > 0$), such that $F(x_1, \ldots, x_n)$ is strictly positive for $x_j \geq 0$, $\Sigma\, x_j > 0$. We confine ourselves to the domain of reals. Polya's theorem states that $F = G/H$ where G and H are forms with positive coefficients only. (More particularly we may choose $H = (x_1+\ldots+x_n)^m$ for some m). I am going to show that even if we allow general forms (there is clearly no point in permitting arbitrary nonhomogeneous polynomials) we can in this case not impose a bound on the degrees of the G and H in question. But even here, it is useful to consider in the first place an arbitrary real closed field R' such that $R \subset R'$, rather than the real numbers R.

An element $a \in R'$ is *infinitesimal* or infinitely close to zero (opposite: infinitely large) if $|a| < r$ for all positive $r \in R$ and *finite* if $|a| < r$ for some positive $r \in R$. Let $F(x_1, \ldots, x_n)$ be a form of degree $k \geq 1$ with coefficients in R', $F = \Sigma\, \alpha_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$, $\Sigma i_m = k$. A point $x_1, \ldots, x_n$ is *finite* if all its coordinates are finite. Then we have the following theorem.

Let $Q_{R'}$ denote the set of all points $(x_1, \ldots, x_n)$ in R'^n such that $x_i \geq 0$ for $1 \leq i \leq n$ and $\Sigma x_i \neq 0$.

Theorem 8.1. Let $F(x_1, \ldots, x_n)$ be a form with coefficients in R'. Suppose that all the coefficients of F are finite and that the non-zero ones are not infinitesimal. In order that there exist forms G and H with positive coefficients in R' such that $F = G/H$ and such that the coefficients of H are all finite and non-infinitesimal, it is necessary and sufficient that for all finite points $(x_1, \ldots, x_n)$ such that $x_i \geq 0$ for $1 \leq i \leq n$ and $\Sigma n_i \neq 0$, $F(x_1, \ldots, x_n)$ be positive non-infinitesimal.

Remark. When we say that all the coefficients of G and H are positive, we mean that every possible monomial of appropriate degree must actually occur nontrivially.

Proof. The condition is necessary. Clearly, if $F(x_1, \ldots, x_n) \leq 0$ at some finite point in $Q_{R'}$ then F cannot be written in the assumed form. To see that F does not take infinitesimal values on finite points in $Q_{R'}$, we argue as follows. Let $(\xi_1, \ldots, \xi_n)$ be such a point. Say ξ_j is not infinitesimal and consider the point $(0, \ldots, 0, \xi_j, 0, \ldots, 0)$ in $Q_{R'}$.

Let a be the coefficient of x_j^d in F (where d is the degree of F). Considering $F(0, \ldots, 0, \xi_j, 0, \ldots, 0)$ shows that $a > 0$ by the strict positivity of F in $Q_{R'}$. Furthermore a is not infinitesimal by assumption. The equation $H(0, \ldots, 0, \xi_j, 0, \ldots, 0) \cdot F(0, \ldots, 0, \xi_j, 0, \ldots, 0) = G(0, \ldots, 0, \xi_j, 0, \ldots, 0)$ implies that the coefficient b of x_j^r in G is not infinitesimal (where $r = \deg G$). Therefore $G(\xi_1, \ldots, \xi_n)$ is not infinitesimal. Thus the equation $H(\xi_1, \ldots, \xi_n) \cdot F(\xi_1, \ldots, \xi_n) = G(\xi_1, \ldots, \xi_n)$ implies that $F(\xi_1, \ldots, \xi_n)$ is not infinitesimal.

Now we prove sufficiency. Although we are dealing with an arbitrary real closed field and not necessarily with a model of nonstandard analysis, we may use some of the notions and techniques of that subject [19]. Thus, every finite number $r \in R'$ is infinitely close to a unique standard real number ${}^0r$ called the *standard part* of r, ${}^0r - r \simeq 0$, and the standard parts of sums and products of finite numbers are the sums and products of the standard parts of these numbers, respectively. The proof of sufficiency follows the outline of the "standard" proof and the reader is referred to it. The first step (for the example of three variables) involves taking the minimum of $F(x, y, z)$ for $x \geq 0$, $y \geq 0$, $z \geq 0$, $x+y+z = 1$.

By Tarski's theorem on real closed fields [16], this minimum ν exists also for a form in R', and there are (x_0, y_0, z_0) such that $F(x_0, y_0, z_0) = \nu$. Moreover, since $(x_0, y_0, z_0) \in Q_{R'}$, ν is not infinitesimal by the assumption on F. Accordingly we have a positive $\mu \in R$ such that ${}^0\nu > \mu$.

Next Polya introduces a function

$$\phi(x, y, z, t) = t^n \Sigma_n a_{\alpha\beta\gamma} \binom{xt^{-1}}{\alpha} \binom{yt^{-1}}{\beta^{-1}} \binom{zt^{-1}}{\gamma},$$

where

$$F(x,y,z) = \Sigma_n a_{\alpha\beta\gamma} \frac{x^\alpha y^\beta z^\gamma}{\alpha!\beta!\gamma!},$$

the summation in both cases being over all triples (α,β,γ) of integers with $\alpha \geq 0$, $\beta \geq 0, \gamma \geq 0, \alpha+\beta+\gamma = n$, and proves the identity, for every $k \geq n$,

$$(x+y+z)^{k-n} F(x, y, z) = (k-n)!k^n \Sigma_k \phi \left(\frac{a}{k}, \frac{b}{k}, \frac{c}{k}, \frac{1}{k}\right) \frac{x^a y^b z^c}{a!b!c!}$$

which holds in any field of characteristic zero. Here again Σ_k denotes the sum over all triples (a, b, c) such that $a \geq 0, b \geq 0, c \geq 0, a+b+c = k$.

Now, $\phi(x, y, z, t) \to F(x, y, z)$ as $t \to 0$ which, since the coefficients are finite, may be interpreted in the standard sense. There is a positive $\epsilon \in R$ such that

$$\phi(x, y, z, t) > F(x, y, z) - \frac{1}{2}\mu > \frac{1}{2}\mu > 0$$

for $0 < t < \epsilon$, in particular for $t = \frac{1}{k}$, where k is sufficiently large. This proves the theorem.

Remark 8.2. The proof shows that H can in fact be chosen to be just $(x_1+ \ldots +x_n)^m$ for some m. Also G can be chosen to have all its coefficients non-infinitesimal.

For the special case $R' = R$, the sufficiency content of our theorem does not add anything to Polya's. From the necessity part, however, we may derive the following "standard" result. Note that for $R' = R$ the statement $(x_1, \ldots, x_n) \in Q_R$ reduces to the "standard" statement that each $x_i \geq 0$ and $\Sigma x_i > 0$.

Theorem 8.3. Suppose that we are given a form $F_\tau = \Sigma a_{i_1 \ldots i_n}(\tau) x_1^{i_1} \ldots x_n^{i_n}$ where the a_i depend on a parameter τ which ranges over a set T in m-dimensional real space. Assume moreover that $|a_{i_1 \ldots i_n}(\tau)|$ is bounded away from zero for all $i_1, \ldots, i_n$ and that F_τ is positive definite on Q_R for all $\tau \in T$. Suppose that there is a point $P \in R^m$ and a point $(\xi_1, \ldots, \xi_n) \in Q_R$ such that $F_\tau(\xi_1, \ldots, \xi_n) \to 0$ as $\tau \to P$ through values in T. Let k be any natural number. Then there is a neighborhood of P in T such that for every τ is this neighborhood F_τ cannot be represented by positive forms of degrees $< k$.

For the proof we use an enlargement $*R$ of R. The previous theorem applies to $*R$. It follows that if n is any infinite positive integer then within a radius $\frac{1}{n}$ around P in $*T$, F cannot be represented by positive forms of finite degree with non-infinitesimal coefficients, in particular not by forms G, H such that deg $G, H < k$ and such that all the coefficients of H are greater than some positive $r \in R$ (although it can be represented by forms of infinite degrees). This assertion can be represented by a sentence $X(n, r)$ in the full language of R. But since the sentence is true for all infinite n it will also be true for sufficiently large finite n, by a well-known principle of nonstandard analysis. This proves the theorem.

For example, consider the form $x^2 - \tau xy + y^2$ where $1 < \tau < 2$. We choose the point P as $\tau = 2$ and $\xi_1 = \xi_2 = \frac{1}{2}$. Then the conditions of the theorem are satisfied. It follows that although for each τ in the range in question the form is strictly positive, the degrees of forms G_τ, H_τ representing $F_\tau = x^2 - \tau xy + y^2$ tend to ∞ as τ approaches 2.

Remark. We note that we may associate with Polya's theorem a diophantine problem with side conditions. The question is whether one can solve $HF = G$ for given F and unknown forms H and G subject to the conditions that their coefficients are positive. The answer is that this problem has no algorithm in the sense of the present paper. By contrast, we have that the condition that F be strictly positive can be formulated in the LPC and hence can even be expressed in quantifier-free form in terms of addition, multiplication, subtraction and equality. But these are just not the same conditions for all real closed fields. We may mention here that [4] contains an erroneous statement that Polya's theorem provides a decision procedure for deciding whether or not a form is strictly positive. "We multiply repeatedly by Σx, and if the form is positive, we shall sooner or later obtain a form with positive coefficients"[4]. However, this is not a decision procedure, for if the form is not strictly positive then the procedure will never terminate. Of course, the elimination of quantifiers provides a decision procedure, as stated.

9. *Algebraic and differential field theory.* Consider as a simple example the assertion which says that a system of linear equations has a solution.

Let

$$\begin{aligned} a_1^1 x_1 + \ldots + a_n^1 x_n &= b_1 \\ a_1^2 x_1 + \ldots + a_n^2 x_n &= b_2 \\ a_1^n x_1 + \ldots + a_n^n x_n &= b_n \end{aligned}$$

be the system in question. The test is that the rank of the augmented matrix is equal to the rank of the (a_j^i). It is not difficult to formulate the statement that the ranks are equal by a quantifier-free formula.

Next, let us consider the following problem. We are given polynomials $f_j(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$ of bounded degrees with variable coefficients.

To decide whether $g \in (f_1, \ldots, f_k)$ (with coefficients in the given field). This can be carried out because there is a known bound on the degrees of $h_1, \ldots, h_k$ for which we might have $g = \sum_i h_i f_i$ [5]. Thus the problem is reduced to one of solvability in terms of the coefficients.

Second problem. To find a basis for $(f_1, \ldots, f_k) : g$ where again bounds are given. (The symbol $(f_1, \ldots, f_k) : g$ stands for division of ideals; $h \in (f_1, \ldots, f_k) : g$ if and only if $hg \in (f_1, \ldots, f_k)$). Notice that this problem is not a priori among the kind considered in our general part, since we do not know the degrees of the basis polynomials and their number from the outset. If we did, then we could regard the coefficients as functions to be calculated in the sense of the general theory. And indeed, the theory of Greta Hermann shows that such bounds exist, and that the coefficients in question can be calculated by rational operations.

Third problem. To find a basis for

$$(f_1, \ldots, f_k) : g^\infty = \bigcup_{n=1}^{\infty} (f_1, \ldots, f_k) : g^n.$$

To do this, we shall show that there is a uniform ν depending only on the degrees of $f_1, \ldots, f_k$, g such that $(f_1, \ldots, f_k) : g^\nu = (f_1, \ldots, f_k) : g^\infty$. First of all, notice that $(f_1, \ldots, f_k) : g^n \subset (f_1, \ldots, f_k) : g^{n+1} = ((f_1, \ldots, f_k) : g^n) : g$. Also, if we have here equality then also $(f_1, \ldots, f_k) : g^{n+1} = (f_1, \ldots, f_k) : g^{n+2}$. For suppose $h \in (f_1, \ldots, f_k) : g^{n+2}$. Then $hg^{n+2} = \Sigma\, h_i f_i$. We have to show that we can replace the left hand side by hg^{n+1}. But at any rate $hg \in (f_1, \ldots, f_k) : g^{n+1}$ and so by assumption $hg \in (f_1, \ldots, f_k) : g^n$, so $h \in (f_1, \ldots, f_k) : g^{n+1}$. Moreover, by Hilbert's basis theorem, for given $(f_1, \ldots, f_k)$ and g, the chain breaks off so there is a first ν for which we have equality, $(f_1, \ldots, f_k) : g^\nu = (f_1, \ldots, f_k) : g_\nu{}^{+1} = (f_1, \ldots, f_k) : g^\infty$.

Now to show that this ν may be chosen uniformly, we proceed as follows. We write down, for each n, the predicate $(f_1, \ldots f_k) : g^n = (f_1, \ldots, f_k) : g^{n+1}$. This only requires writing down that all elements of the basis of $(f_1, \ldots, f_k) : g^{n+1}$ (which have been computed, as described), $k_1, \ldots, k_\ell$ say, belong to $(f_1, \ldots, f_k) : g^n$, i.e. they satisfy $k_j g^n \in (f_1, \ldots, f_k)$. All this requires only rational operations. Since they are completed after a finite number of steps in each case, all this is equivalent to some predicate Q_n of $\{f_1, \ldots, f_k, g\}$. Now consider the axioms of field theory K, together with $\neg Q_1, \neg Q_2, \ldots$ where we have replaced the variable coefficients of the f_j, g by new distinct constants. Then if K, $\neg Q_1, \neg Q_2, \ldots$ is consistent, it has a model in which Hilbert's basis theorem is not satisfied. This is impossible, so $K \vdash Q_1 \vee \ldots \vee Q_\nu$ for some ν. But since $K \vdash Q_\mu \supset Q_\nu$ for all $\mu < \nu$, we have $K \vdash Q_\nu$, proving the assertion.

Next we shall be concerned with prime ideals. We refer the reader to Ritt [11] for the notion of a chain and of a characteristic set. We have the following theorem. Let I_i be the initials of a chain $A_1, A_2, \ldots, A_r$, where A_1 is of positive class, i.e. is not a constant. Let G be any polynomial. Then there exist nonnegative integers t_i, $i = 1, \ldots, r$, and a polynomial R such that

$$I_1^{t_1} \cdot \cdots I_r^{t_r} G \equiv R \bmod (A_1, \ldots, A_r),$$

where R is *reduced* with respect to $A_1, A_2, \ldots, A_r$, that is to say, the degree of R in the last variable which occurs in A_j is lower than the degree of A_j in it.

Put $H = I_1^{t_1} \cdots I_r^{t_r}$ We are going to show:

Theorem 9.1. In order that G belong to the prime ideal J whose characteristic set is $(A_1, \ldots, A_r)$ (provided it is a characteristic set of any prime ideal) it is necessary and sufficient that $R = 0$.

Proof. Notice that every I_j must be reduced with respect to $(A_1, \ldots, A_r)$. For it is lower than A_j and by the definition of a chain must be lower than all other A_i also. If $G \in J$ then the remainder is in J since the congruence is, modulo $(A_1, \ldots, A_r)$. Since the remainder is reduced with respect to the $A_1, \ldots, A_r$, $R = 0$. Conversely since the I_j's are reduced with respect to $A_1, \ldots, A_r$, none of them is in J. So if $R = 0$, then $G \in J$, since J is prime. This proves the assertion.

We now come to one of Ritt's major problems in the constructive theory of algebraic equations. It is to determine whether a given chain is a characteristic set of a prime ideal, where the chain is of the form $A_1, A_2, \ldots, A_p$, A_i containing the "parameters" $U_1, \ldots, U_q$ and the variables $Y_1, \ldots, Y_{i-1}$ and introducing the variable Y_i.

We shall show that for each such case, with the A_i having indeterminate coefficients and having given degrees, there is an $\forall\exists$-predicate which determines whether the chain in question is the characteristic set of a prime ideal.

For $p = 1$, Ritt [11, p. 88] shows that the condition is that the polynomial $A_1(Y_1)$ be irreducible regarded as a polynomial with coefficients in $F(U_1, \ldots, U_q)$, where F is a given field whose diagram forms part of the axiomatic system K. The condition of irreducibility can be represented by a universal predicate.

For $p > 1$, Ritt proves that the following condition is necessary and sufficient.

(*i*) $A_1, \ldots, A_{p-1}$ is a characteristic set of a prime polynomial ideal.

(*ii*) If $u_1, \ldots, u_q, y_1, \ldots, y_{p-1}$ is a generic zero of $A_1, \ldots, A_{p-1}$ then when we substitute these for $U_1, \ldots, U_q, Y_1, \ldots, Y_{p-1}$ in A_p, we obtain a polynomial $A_p(Y_p)$ which is irreducible in its field of coefficients.

To interpret these conditons, let us suppose that we have tested—by an $\forall\exists$-predicate—that (*i*) is satisfied and let us consider (*ii*). To substitute the generic zero really amounts to calculating with polynomials in $U_1, \ldots, U_q, Y_1, \ldots, Y_{p-1}$ modulo J_{p-1}, where J_{p-1} is the ideal determined by the generic point. Now, given $A_1, \ldots, A_{p-1}$ we have, from Theorem 9.1 and the third problem,

$$J_{p-1} = (A_1, \ldots, A_{p-1}) : (I_1 \cdots I_{p-1})^\infty = (A_1, \ldots, A_{p-1}) : (I_1 \cdots I_{p-1})^m$$

where m depends only on the given bound for $A_1, \ldots, A_{p-1}$. Accordingly, as mentioned, we can compute a basis for J_{p-1}.

Now, having found J_{p-1}, we know that we obtain a generic point of J_{p-1} simply by taking the residue class of $U_1, \ldots, U_q, Y_1, \ldots, Y_{p-1}$ in $F[U_1, \ldots, U_q; Y_1, \ldots, Y_{p-1}]$ modulo J_{p-1}. In other words the point $(u_1, \ldots, u_q, y_1, \ldots, y_{p-1})$ is a given point in the field F' which is the field of quotients of $F[U_1, \ldots, U_q; Y_1, \ldots, Y_{p-1}] / J_{p-1}$. Any representation $A_p = H \cdot K$ in that field where neither H nor K is constant (*as a polynomial in* Y_p) is equivalent to a representation

$$(1) \qquad G A_p \equiv HK \bmod J_{p-1},$$

where we have obtained G by clearing away denominators, $G \notin J_{p-1}$, and where H and K are not independent of Y_p. Now we may make sure that G is reduced with respect to $A_1, \ldots, A_{p-1}$ by multiplying by appropriate powers of $I_1, \ldots, I_{p-1}$, the result, R, mod J_{p-1} being reduced with respect to $A_1, \ldots, A_{p-1}$ and hence of bounded degree. Hence, we may assume that G is reduced with respect to $A_1, \ldots, A_{p-1}$. Similarly, it is enough to consider H's and K's which are reduced with respect to $A_1, \ldots, A_{p-1}$ and reducibility is now expressed by the $\exists\forall$-assertion that there exist certain coefficients of G and of H and K with not all positive powers of Y_p in H or K having coefficients belonging to J_{p-1} such that $G A_p - HK$ belongs to J_{p-1}.

We have thus obtained an $\forall\exists$- test whether or not $A_1, \ldots, A_p$ is the characteristic set of a prime ideal.

Next suppose we are given a system of polynomials $Q_1, \ldots, Q_m$. We wish to develop a set of characteristic sets of prime ideals whose manifolds make up the manifolds of $Q_1, \ldots, Q_m$. If we get these characteristic sets, we can also get their prime ideals, as above, i.e. their bases . . .

REFERENCES

1. P. J. Cohen, Decision procedures for real and p-adic fields, Communications in Pure and Applied Mathematics, Vol. XXII (1969), 131–152.
2. E. Engeler, *Formal Languages: Automata and Structures*, Lectures in Advanced Mathematics, Markham Publ. Co, Chicago 1968.
3. R. Fraissé, Une notion de recursivité relative, Infinitistic Methods, Proc. Symp. on Foundations of Math., Warsaw 1961, 323–328.
4. Hardy-Littlewood-Polya, *Inequalities*, Cambridge University Press, 1959.
5. G. Hermann, Die Frage der endlichen vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95 (1926), 736–788.
6. D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, Vol. II, Springer-Verlag, Berlin 1939.
7. L. Kronecker, Die Zerlegung der ganzen Größen eines natürlichen Rationalitätsbereichs in ihre irreductiblen Factoren, *Kroneckers Werke*, Teubner Verlag, Leipzig 1895, Vol. 2, 409–416.
8. W. Lambert, A Notion of Effectiveness in Arbitrary Structures, J.S.L. 33 (1968), 577–602.
9. R. Peter, Über die Verallgemeinerung der Theorie der rekursiven Funktionen für abstrakte Mengen geeigneter Struktur als Definitionsbereiche, Acta Math. Acad. Sci. Hung. 12 (3–4) (1961).
10. M. Rabin, Computable Algebra: General Theory and Theory of Computable Fields, AMS Transactions 95 (1960), 341–360.
11. J. F. Ritt, *Differential Algebra*, AMS Colloquium Publications Vol. XXXIII, New York 1950.
12. A. Robinson, *Introduction to Model Theory and to the Metamathematics of Algebra*, North Holland Publ. Co., Amsterdam 1963.
13. ———, *Nonstandard Analysis*, North Holland Publ. Co., Amsterdam 1966.
14. ———, Infinite Forcing in Model Theory, Proc. Second Scandinavian Logic Symposium, North Holland 1971, 317–340.
15. J. C. Shepherdson and A. Frölich, Effective Procedures in Field Theory, Trans. Royal Soc. London, ser. A, 248 (1956), 407–432.
16. A. Tarski and J. C. C. McKinsey, *A Decision Method for Elementary Algebra and Geometry*, 2nd edition, Berkeley and Los Angeles, 1948/1951.

PART IV

Pure Algebra