Introduction

A natural way of studying the computability of an algebraic structure or process is to apply some of the theory of the recursive functions to the algebra under consideration through the manufacture of appropriate coordinate systems from the natural numbers. Let us say an algebraic structure $\mathcal{U} = (A; \sigma_1, \ldots, \sigma_k)$ is computable if it possesses a recursive coordinate system in the following precise sense: associated to $\mathcal{U}$ there is a pair (α, Ω) consisting of a recursive set of natural numbers Ω and a surjection $\alpha : \Omega \to A$ so that (i) the relation defined on Ω by $n \equiv_\alpha m$ iff $\alpha(n) = \alpha(m)$ in $\mathcal{U}$ is recursive, and (ii) each of the operations of $\mathcal{U}$ may be effectively followed in Ω, that is, for each (say) r-ary operation σ on A there is an r argument recursive function $\bar{\sigma}$ on Ω which commutes the diagram $A^r \xrightarrow{\sigma} A$, wherein α^r is r-fold $\alpha \times \ldots \times \alpha$.

$$\begin{array}{ccc} A^r & \xrightarrow{\sigma} & A \\ {\scriptstyle \alpha^r}\uparrow & & \uparrow{\scriptstyle \alpha} \\ \Omega^r & \xrightarrow{\bar{\sigma}} & \Omega \end{array}$$

This concept of a computable algebraic system is the independent technical idea of M.O. Rabin [18] and A.I. Mal'cev [14]. From these first papers one may learn of the strength and elegance of the general method of coordinatising; noteworthy for us is the fact that computability is a finiteness condition of Algebra - an isomorphism invariant possessed of all finite algebraic systems - and that it serves to set upon an algebraic foundation the combinatorial idea that a system can be combinatorially presented and have effectively decidable term or word problem.

A point of departure for this paper is Rabin's article in which he announced his discovery that a finitely generated group of matrices over any field is computable as a group [18, p. 351]. The principal purpose of this paper is to give Rabin's proof of this fact and to study a family of generalisations of his result in a direction away from groups (of matrices over a field) toward general algebraic structures (embedded in the affine spaces over a field); we propose to prove the following results.

Let F be a field and let F^n denote the space of all n-tuples of elements of F, the n-dimensional affine space over F.

A mapping $f : A \subset F^n \to F^m$ is said to be polynomial over F if the m coordinate functions $f_i : A \to F$ into which it decomposes may be defined by polynomials in n arguments over F. Thinking of a general algebraic structure embedded in F^n:

The Affine Theorem

Let $\mathcal{A} = (A; \sigma_1, \ldots, \sigma_k)$ be a universal algebra with domain $A \subset F^n$ and operations σ_i polynomial over F. If $\mathcal{U}$ is finitely generated then $\mathcal{U}$ is computable as an algebra.

This represents a direct generalisation of Rabin's theorem to general affine systems (as we might refer to such $\mathcal{U}$) and is, along with Rabin's theorem, of some considerable algebraic interest since such structures are ubiquitous in mathematics, but the practical significance of the theorem may only partially engage us here (I have written about this

in [26]). Some deeper theoretical results are possible:

A mapping $f : A \subset F^n \to F^m$ will be said to be elementary or first-order algebraic if its m coordinate functions may be defined by first-order expressions of the theory of fields. Then

The Definability Theorem for Algebraically Closed Fields

Let F be algebraically closed. Let $\mathcal{U}$ be an algebraic structure within F^n whose operations are elementary algebraic. If $\mathcal{U}$ is finitely generated then $\mathcal{U}$ is computable.

The key to this theorem is A. Tarski's technique for the effective elimination of quantifiers from the first-order expressions of the theory of algebraically closed fields [23]. The strategy of its proof suggests that an analogous result might be true for real closed fields for which elimination of quantifiers is also possible; this eventuality is analysed and ruled out because of the singular behaviour of the algebra of fields with orderings. A "best possible" result is this:

A mapping $f : A \subset F^n \to F^m$ will be said to be elementary or first-order geometric if its m coordinate functions may be defined by first-order expressions of the theory of fields with orderings.

The Definability Theorem for $\mathbb{R}^n$

Let $\mathbb{R}$ be the field of real numbers. Let $\mathcal{U}$ be an algebraic structure within $\mathbb{R}^n$ whose operations are elementary geometric. If $\mathcal{U}$ is finitely generated by vectors

involving computable real numbers only, then u is computable.

The argument which leads to this theorem involves work of A. Lachlan and E.W. Madison, see [10] and [12].

These three theorems are proved in sections numbered two, three and four respectively. In passing, one or two illustrative applications are included which I hope may be of some independent interest. Section one is a resumé of the ideas and results we shall need.

The principal results were determined while I was a resarch student at the University of Bristol, England. I am indeed in the debt of my supervisor, Dr. J.P. Cleave, for his encouragement and guidance. I wish to thank Prof. Rabin for explaining his proof of his theorem and Prof. J.C. Shepherdson for bringing to my attention the work of Lachlan and Madison. I am happy to express my gratitude to Prof. J.E. Fenstad and his colleagues at Oslo for their hospitality, and to the Officers of the Royal Society, London for the indispensible support of a fellowship through their European Programme.

1. Preparatory concepts and results about computable algebraic systems and computable fields

Here is collected together most, although not all, of the technicalities and theorems we employ in our proofs, this material concerns universal algebras, general sets, rings and fields. Ideally, the prospective reader ought to be familiar with the papers of Rabin and Mal'cev and with a paper of

A. Fröhlich and J.C. Shepherdson [7] and ought not to expect illumination from these notes.

$\mathbb{N},\mathbb{Z},\mathbb{Z}_p,\mathbb{Q},\mathbb{R},\mathbb{C}$ stand for the natural numbers, the integers, the integers modulo p, the rational numbers, the reals, and the complex numbers respectively.

Computable universal algebras

For the theory of universal algebras we depend upon the books of P.M. Cohn [4] and Mal'cev [15]. For the theory of computable universal algebras we shall cite [14] whilst habitually borrowing from [25].

A coordinatisation α of an algebra $\mathcal{U} = (A; \sigma_1,\ldots,\sigma_k)$ consists of a surjection $\alpha : \Omega_\alpha \subset \mathbb{N} \to A$ together with numerical functions $\bar{\sigma}_1,\ldots,\bar{\sigma}_k$ which track the operations of $\mathcal{U}$ in the set of codes Ω_α; precisely, for σ_i an r_i-ary operation on A, $\bar{\sigma}_i$ is an r_i-ary operation on Ω_α and the diagram

$$\begin{array}{ccc} A^{r_i} & \xrightarrow{\sigma_i} & A \\ \uparrow{\scriptstyle \alpha^{r_i}} & & \uparrow{\scriptstyle \alpha} \\ \Omega_\alpha^{r_i} & \xrightarrow{\bar{\sigma}_i} & \Omega_\alpha \end{array}$$

commutes for $i = 1,\ldots,k$. (Clearly, a coordinatisation of $\mathcal{U}$ is an algebra of natural numbers $(\Omega_\alpha; \bar{\sigma}_1,\ldots,\bar{\sigma}_k)$ and an epimorphism $\alpha : \Omega_\alpha \to \mathcal{U}$.) The congruence on Ω_α induced by α we denote $\equiv_\alpha$: for $n,m \in \Omega_\alpha$, $n \equiv_\alpha m$ iff $\alpha(n) = \alpha(m)$ in $\mathcal{U}$.

(A coordinatisation α will be variously called a numbering or a coding, its domain will be usually denoted Ω_α and we will operate an important technical convention in avoiding the number 0 in our coordinate systems so if Ω is a set of codes then $0 \notin \Omega$.)

A coordinatisation α is effective if the set of numbers Ω_α is recursive and the tracking functions $\bar{\sigma}_i$ are recursive.

$\mathcal{U}$ is computable under coordinatisation α iff α is effective and the relation $\equiv_\alpha$ is recursive.

Let $\mathcal{U}$ contain $\mathcal{V}$ as a subalgebra. If $\mathcal{U}$ is computable under α then to say that $\mathcal{V}$ is an (α-)computable subalgebra of $\mathcal{U}$ means that the preimage $\alpha^{-1}\mathcal{V}$ is recursively enumerable.

1.1 Lemma A finitely generated subalgebra of a computable algebra is a computable subalgebra.

See Mal'cev [14, p. 193].

Let $\mathcal{U}$ be an arbitrary algebraic structure. $\mathcal{U}$ is said to be locally computable iff every finitely generated subalgebra of $\mathcal{U}$ is a computable algebra. (This idea we use in a rather superficial way, it is an interesting finiteness condition for uncountable structures [25, 26].)

Finally, we would do well to explain the elaborate process of constructing an effective coordinate system for a structure $\mathcal{U}$ based upon a set of generators. Working within an arbitrarily chosen species of structures of signature τ, recall the term descriptions of its systems, [4, p. 116] and [15, p. 111].

Let X be an non-empty set. The (τ-)terms over X are inductively defined by declaring (i) any element of X is a term and (ii) if $t_1,\ldots,t_r$ are terms and σ is an r-ary operation symbol for the species then $\sigma(t_1,\ldots,t_r)$ is a term and (iii) nothing beyond the stipulations of clauses (i) and (ii) is a term.

Let $\mathbf{T}(X)$ denote the set of all terms over X, $T(X)$ is an algebra of the species since clause (ii) asserts it is closed under the application of operation symbols; two terms are equal iff they are syntactically identical. Clearly $T(X)$ represents by construction the formal skeleton of any algebra of the species generated by X. Define <u>term length</u> $L : T(X) \to \mathbb{N}$ in the usual manner: the elements of X are terms of length = 0, if $t = \sigma(t_1,\ldots,t_r)$ then $L(t) = \max(L(t_1),\ldots,L(t_r))+1$.

The term algebras are uniquely determined by the cardinality of their generating sets: for X,Y sets, $T(X)$ is isomorphic to $T(Y)$ iff $\mathbf{card}(X) = \mathrm{card}(Y)$, this cardinal is called the <u>rank</u> of the term algebra, see [4, p. 117]. The term algebras enjoy the following universal mapping property: if $\mathcal{U}$ is an algebra of the species and X is any non-empty set then any map $\varphi : X \to \mathcal{U}$ extends uniquely to a homomorphism $\bar{\varphi} : T(X) \to \mathcal{U}$ (the term algebras are free algebras for the species), see [4, p. 120]. Through this property we describe the combinatorial form of $\mathcal{U}$. We assume a set of <u>indeterminate symbols</u> $X = \{X_i : i \in I\}$ is available for each cardinality (we shall need only finite sets). Let $\{a_i : i \in I\}$ be a generating set for $\mathcal{U}$ and define from the given indexing I the <u>subsitution function</u> $X_i \to a_i$, this extends to a homomorphism v of $T(X)$ onto $\mathcal{U}$, this epimorphism we refer to as a <u>valuation map</u>.

Quite easily, the term algebras of finite and countably infinite rank can be shown to be computable. We shall assume available a <u>standard computable coordinatisation</u> γ_* of each

$T(X)$. By this is understood a computable numbering $\gamma_* : \Omega_{\gamma_*} \to T(X)$ with the special feature that it has associated to it a recursive decomposition function which tells of an element $n \in \Omega_{\gamma_*}$ whether or not it labels an indeterminate and, if it does, it can tell which or, if it does not, it can provide a decomposition into codes for the subterms of $\gamma_*(n)$. To be more precise, a recursive function $d : \mathbb{N} \times \Omega_{\gamma_*} \to \mathbb{N}$ is hypothesised with the following properties if $d(0,n) = 0$ then $\gamma_*(n) = X_i$ where $i = d(1,n)$, if $d(0,n) = i$ and $1 \leq i \leq k$ then $\gamma_*(n) = \sigma_i(\gamma_* d(1,n), \ldots, \gamma_* d(r_i,n))$. From this term length is computable. The standard coding of Mal'cev, which uses the arithmetic of prime numbers, is an example of such a numbering [14, p. 202]. It is worth mentioning that it is possible to prove that standard coordinatisations of $T(X)$, as defined, compose an equivalence class of codings under the natural concept of identity between numberings, that of their recursive equivalence [14, p. 188], so our choice of standard coding is immaterial, see [25].

Now given an algebra $\mathcal{U}$ and an indexed set of generators $\{a_i : i \in I\}$ we construct the standard numbering of $\mathcal{U}$ defined by the generating set (together with its indexing) by taking the standard term algebra of rank = card(I) (in the species of $\mathcal{U}$) with its standard computable numbering γ_* and defining the valuation map $v : T(X) \to \mathcal{U}$ from the generating set, and then composing $\gamma = v\gamma_* : \Omega_{\gamma_*} \to \mathcal{U}$; γ is our required effective coordinatisation. This procedure demonstrates that, theoretically, one's idea as to the complexity of a system $\mathcal{U}$ can be reduced to that of the equality

relation between its elements.

Sets

If X and Y are sets computable under α and β respectively and $\varphi : X \to Y$ then φ is computable (with respect to α and β) if there is a recursive function $f : \Omega_\alpha \to \Omega_\beta$ which tracks φ : so that the following diagram commutes,

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ \Omega_\alpha & \xrightarrow{f} & \Omega_\beta \end{array}$$

If X is a computable set under α then the set FinSeq(X) of all finite sequences of the elements of X is a computable set. The truth of this is evident if one thinks of a method of coding by prime numbers, for example, of coding $(\alpha(n_1),\ldots,\alpha(n_r))$ by $2^{n1},\ldots,p_r^{nr}$. As in the case of T(X) it is worth pointing out that precisely what we are interested in is any coding of FinSeq(X) in which X and all its cartesian products are computable subsets. So it is that we arrive at the idea that a standard coordinatisation β of FinSeq(X) derived from a coordinatisation α of X is a numbering to which there is associated a recursive unpacking function $u : \mathbb{N} \times \Omega_\beta \to \Omega_\alpha \cup \{0\}$ which calculates the **α-code** of the i-th entry of the sequence with β-code n to be $u(i,n)$ and from which sequence length may be effectively calculated. To constructively manipulate finite sequences one needs length and unpacking to be constructive. Under this formalisation of a standard coding, the procedure of coordinatising sets of sequences can be shown to be unique up

to the coordinatisation of X , see [26].

Rings and fields

For the algebra of fields we depend on van der Waerden's [28] to which reference can be made for any concept or result in this paper which may be unfamiliar. It was a fine study of the computability of field-theoretic constructions by Fröhlich and Shepherdson which first demonstrated the significance of the idea of analysing the complexity of general algebraic processes in terms of recursive function theory, so stimulating the general programmes of Rabin and Mal'cev. Fortunately for the reader, their paper is required reading for ours.

We shall need the following theorems about computing in rings and fields.

1.2 Lemma If R is a computable commutative ring then the polynomial ring $R[X_1,\ldots,X_n]$ over R is computable containing R as a computable subring and the evaluation action $e(p,\underline{r}) = p(\underline{r})$ is computable $R[X_1,\ldots,X_n] \times R^n \to R$.

See [7, pp. 412-413]; the uniformity of calculating polynomials we must leave to the reader. By working through the basic constructions of field theory, following [7], one is led to this theorem which is our basic tool.

1.3 Lemma Let E be an extension field of a computable field F . Any extension of F by a finite number of elements of E is computable and contains F as a computable subfield.

The proof of this contains some important points and should be reconstructed from [7, pp. 413-414]. The result is essentially proved in van der Waerden's [27, pp. 134-135]. Finally, we shall need the harder theorem of Rabin [18, pp. 354-356],

1.4 Lemma If F is a computable field then its algebraic closure $\bar{F}$ is a computable field and contains F as a computable subfield.

2. The Affine Theorem

2.1 Rabin's Theorem

A finitely generated group of matrices over any field is computable.

Here is the proof. Let F be a field. F possesses a computable subfield in its prime subfield which is isomorphic to the finite field $\mathbb{Z}_p$ or to the rationals $\mathbb{Q}$ according as the characteristic of F is the prime p or 0 [28, pp. 110-111]; let this prime field be denoted C.

Let $A_1,\ldots,A_m$ be a finite set of $n\times n$ matrices over F generating a group G. We extend the computable field C by all the mn^2 elements of F making up the generators of G. That is, form the extension

$$E = C(\{a_k(i,j) : 1 \leq k \leq m \;\&\; 1 \leq i,j \leq n\})$$

where $a_k(i,j)$ is the (i,j)-th entry of A_k.

E is computable by lemma 1.3 and so G now appears as a finitely generated group of matrices over a computable field E,

such an object is computable because the ring $M(n,E)$ of all $n \times n$ matrices over E is computable (clearly) and the group $GL(n,E)$ of all non-singular matrices over E is computable (for $A \in GL(n,E)$ iff $\det(A) \neq 0$) and G is a finitely generated subgroup of $GL(n,E)$, computable by lemma 1.1.

Reflecting on the mechanisms in the proof, in the context of a general kind of algebraic structure derived from the operations of a field, leads to the following result:

2.2 Theorem Let F be a field and let $\mathcal{U} = (A; \sigma_1,\ldots,\sigma_k)$ be a finitely generated universal algebra whose domain A is a subset of F^n and whose operations σ_i may be defined by polynomials over the prime subfield of F. Then $\mathcal{U}$ is a computable algebra.

We shall concentrate on proving the above statement and obtain the Affine Theorem from its argument on completion.

We start by providing $\mathcal{U}$ with an effective coordinatisation. Let $\{\underline{a}_1,\ldots,\underline{a}_n\} \subset A \subset F^n$ be a set of generators for $\mathcal{U}$. Construct the term algebra $T(X)$ on m indeterminates together with its standard computable numbering γ^* and define from the generating set the valuation $v : T(X) \to \mathcal{U}$. Exactly as explained in the section of preliminaries, we have the standard coordinatisation γ of $\mathcal{U}$ derived from the given generating set; the theorem is proved on showing that the relation $\equiv_\gamma$ is recursive on Ω_γ.

Intuitively the plan of the proof is analogous to that of Rabin's Theorem: take the prime subfield C of F and extend it by all the elements of F making up the generators of $\mathcal{U}$

to form a computable field E. The purpose is to claim that $\mathcal{U}$ may be thought of as an algebra within the computable affine space E^n and, specifically, that this makes it computable. Technically it is this transition which is no longer clear and requires precise demonstration: it must be shown that $\mathcal{U}$ is effectively embedded in E^n. Thus if we let β denote a suitable computable coordinate system for E^n then we must prove the following

2.3 Basic Lemma There is a recursive function $g : \Omega_\gamma \to \Omega_\beta$ such that for $n \in \Omega_\gamma . \gamma(n) = \beta\, g(n)$.

2.4 Corollary $\equiv_\gamma$ is recursive.

Proof: Consider the relation on Ω_γ:

$n \equiv_\gamma m$ iff $\gamma(n) = \gamma(m)$ in $\mathcal{U}$,
iff $\gamma(n) = \gamma(m)$ as elements of F^n,
iff $\gamma(n) = \gamma(m)$ as elements of E^n,
iff $\beta g(n) = \beta g(m)$ by the Basic Lemma,
iff $g(n) \equiv_\beta g(m)$.

So $\equiv_\gamma$ is reduced to $\equiv_\beta$ and hence is recursive.

Q.E.D.

Consider the assumed properties of $\mathcal{U}$. An r-ary operation $\sigma : A^r \to A$ of $\mathcal{U}$ will decompose into n coordinate functions which we write $\sigma^1, \ldots, \sigma^n : A^r \to F$. The elements of A^r on which these coordinate functions are defined are essentially rn-tuples of elements of F and the hypothesis that σ is polynomial over the prime subfield C of F is precisely that there are n polynomials p^i from $C[X_1, \ldots, X_{rn}]$

defining these σ^i on A, that is, for each $i = 1,\ldots,n$ $\sigma^i(\underline{x}) = p^i(\underline{x})$, for all $\underline{x} \in A^r$. The assumption that each operation of $\mathcal{U}$ be polynomial leads to k n-tuples of many argument polynomials over C, therefore.

Let C now be extended by the coordinates of the generators. Let a_{ij} be the j-th entry of $\underline{a}_i$ and set $E = C(\{a_{ij} : 1 \leq i \leq m \ \& \ 1 \leq j \leq n\})$; E is computable under α say. We can arrange for $\beta = \alpha^n : \Omega_\beta = \Omega_\alpha^n \to E^n$ to be a computable coordinate system for its n-dimensional affine space.

We claim that $A \subset E^n$ and that it is possible to pass effectively from the γ-labels for elements of A to their β-labels; this is the Basic Lemma.

2.5 Lemma $A \subset E^n$

Proof: By induction on the length of terms we show that for each $t \in T(X)$, $v(t) \in E^n$; this is formally the observation that given elements of E^n as generators the operations of $\mathcal{U}$, being polynomial over C, pick out only elements of F^n which also lie in E^n.

Basis. The generators of $\mathcal{U}$ lie in E^n by construction so the terms of length zero all map into E^n.

Induction step. Assume that all terms of length <1 map into E^n under v, let t be any term of length 1. Breaking t down into its component subterms write $t = \sigma(t_1,\ldots,t_r)$ say. Now $v(t) = v(\sigma(t_1,\ldots,t_r)) = \sigma(vt_1,\ldots,vt_r)$ since v is a homomorphism. Let $vt_i = \underline{z}_i$ for $1 \leq i \leq r$ and let $\underline{z} = (\underline{z}_1,\ldots,\underline{z}_r) \in A^r$. We know $\underline{z} \in E^{rn}$ for, by the induction hypothesis, the t_i map into E^n under v. Claim: $\sigma(\underline{z}) \in E^n$. Consider the coordinate functions for σ. For

$1 \leq i \leq n$,

$$\sigma^i(\underline{z}_1,\ldots,\underline{z}_r) = p^i(z_{11},\ldots,z_{1n};\ldots;z_{r1},\ldots,z_{rn})$$

where $\underline{z}_j = (z_{j1},\ldots,z_{jn})$ for $1 \leq j \leq r$. Clearly this is an element of E since p^i is a polynomial over $C < E$ acting exclusively on elements of E . Hence the claim and, by the induction principle, the lemma.

Q.E.D.

To show the exchange of labels is effective we work with the elements of $\mathcal{U}$ through $T(X)$. Each term, being an inductive construction from $X_1,\ldots,X_m$ and the operations $\sigma_1,\ldots,\sigma_k$, is now thought of as essentially a function of m arguments $t(X_1,\ldots,X_m)$ defined on A . The polynomial definition of the σ_i entails that the course of construction of each t leads explicitly to an n-tuple of polynomials over C in mn arguments which defines t as a function of m arguments on A . This decomposition is formally described as a computable association $D : t \to p_t = (p_t^1,\ldots,p_t^n)$ as follows.

The set of n-tuples of polynomials over C in mn indeterminates $P = C[X_1,\ldots,X_{mn}]^n$ is a computable set; this is clear since a multiargument polynomial ring over a computable field is computable (lemma 1.2) and so cartesian products can be taken to construct a computable coordinate system $\gamma_1 : \Gamma_1 \to P$. To say that the decomposition is explicit is to say that there is a recursive function $d : \Omega_\gamma \to \Gamma_1$ tracking D , that is, commuting the following diagram, $T(X) \xrightarrow{D} P$; the truth of

$$\begin{array}{ccc} T(X) & \xrightarrow{D} & P \\ {\scriptstyle\gamma}\uparrow & & \uparrow{\scriptstyle\gamma_1} \\ \Omega_\gamma & \xrightarrow{d} & \Gamma_1 \end{array}$$

this statement is clear from the inductive definition of D.

Now if $D(t) = p_t$ then $v(t) = D(t)(\underline{a}_1,\ldots,\underline{a}_m) = p_t(\underline{a}_1,\ldots,\underline{a}_m)$. The function g calculating a label for $t(\underline{a}_1,\ldots,\underline{a}_m)$ in Ω_β is the tracking map of the procedure of decomposing a term t to its polynomial form $D(t)$ and directly evaluating that polynomial form on the generators in E^n. Here is this procedure exactly.

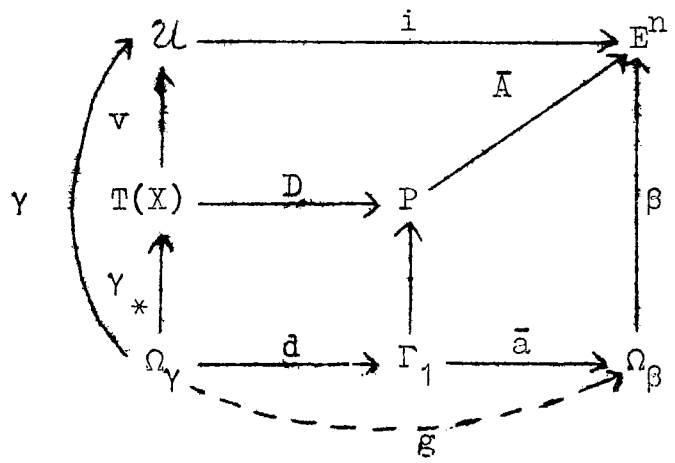
The evaluating action of $C[X_1,..,X_{mn}]$ on E is computable as it is part of the action of $E[X_1,\ldots,X_{mn}]$ on E (lemma 1.2). From e define a general process $A : P\times E^n\times\ldots\times E^n \to E^n$ by

$$A(p_1,\ldots,p_n,\underline{x}_1,\ldots,\underline{x}_m) = (e(p_1,\underline{x}_1,\ldots,\underline{x}_m),\ldots,e(p_n,\underline{x}_1,\ldots,\underline{x}_m))$$

and let it be recursively tracked by a, so that the following diagram commutes, $P\times E^n\times\ldots\times E^n \xrightarrow{A} E^n$. Now apply this

$$\begin{array}{ccc} \uparrow{\scriptstyle \gamma_1\times\beta^m} & & \uparrow{\scriptstyle \beta} \\ \Gamma_1\times\Omega_\beta^m & \xrightarrow{a} & \Omega_\beta \end{array}$$

A over P on the m-tuple $(\underline{a}_1,\ldots,\underline{a}_m)$: write this restriction $\bar{A}$ and let it be computed by $\bar{a}$. To complete the argument, take $g = \bar{a}d$ and, to see that this proves the Basic Lemma, consider $\bar{A}D\gamma_*$ in the following diagram



By the upper route, $\bar{A}D\gamma_*(n) = p_{\gamma_*(n)}(\underline{a}_1,\ldots,\underline{a}_m)$

$= v\gamma_*(n)$

$= \gamma(n)$.

By the lower route, $\bar{A}D\gamma_*(n) = \bar{A}\gamma_1 d(n)$

$= \beta\bar{a}d(n)$

$= \beta g(n)$

So $\gamma = \beta g$ and the theorem is proved.

Q.E.D.

To obtain the stronger statement of the Affine Theorem, wherein arbitrary polynomials are allowed to define the operations of the structure $\mathcal{U}$, consider the stage in the proof at which E is constructed. Since $\mathcal{U}$ is finitary at most a finite number of elements of F will appear in the collection of polynomials used for its operations, these coefficients may be included along with the coordinates of the generators in extending C to the computable affine space required to enclose $\mathcal{U}$.

And from the Affine Theorem may be deduced a possibly more useful, though equivalent, result in which the field F is replaced by a commutative integral domain R . To see this is to notice that if $\mathcal{U}$ is an affine system over R then it is an affine system over the quotient field Q of R (precisely: $\mathcal{U} \subset R^n \subset Q^n$ and operations polynomial over R are polynomial over Q) so the Affine Theorem applies to show computability. The ring of real-valued analytic functions on an open subset of $\mathbb{R}^n$ is an integral domain whose quotient field is not encountered naturally (contrast this with the complex case however). Actually something much stronger is true by significantly more complicated

constructions: any finitely generated affine system over an arbitrary commutative ring is computable (see [26]).

Let us illustrate the Affine Theorem with some applications.

First, structures made from matrices over fields are going to be affine: if $\mathcal{U}$ consists of $n \times n$ matrices with entries from F then $\mathcal{U}$ lies within F^{n^2} so providing the operations involved are polynomial over F - for example, operations polynomial over $M(n,F)$ - then finitely generated substructures of $\mathcal{U}$ will be computable. In particular: any finitely generated ring, group or semigroup which is linear, in the sense that it may be faithfully represented in some $M(n,F)$, is computable. Doubtless the reader can compose his or her own examples of matric structures.

Secondly, indeed canonically, there are the natural affine systems of Algebraic Geometry. For F a field an algebraic group G over F can be defined to be a group whose domain $G \subset F^n$, for some $n > 0$, is the set of zeros of a finite collection of polynomials over F (precisely: there exist $p_1,\ldots,p_k \in F[X_1,\ldots,X_n]$ such that $G = \{\underline{x} \in F^n : p_i(\underline{x}) = 0$ for $1 \leq i \leq k\}$) and whose operations are definable by polynomials over F. We may generalize this familiar concept to indefinite structures by adding the hypothesis that the domains of our affine systems be such closed sets, and declare all structures algebraic in the sense of Algebraic Geometry are locally computable. Note that the condition is a strong one at least in the group case where every algebraic group can be shown to be linear, see [8, p.63]. These and some further simple ideas from Algebraic Geometry appear in examples of the next section, a

most suitable reference is Shafarevich's book [22].

We have two applications to be considered more carefully, the sources of their "affineness" are, for the first, the fact that the structures considered are in essence made from polynomials and, for the second, that they are directly derived from finite dimensional linear spaces.

By way of preparation for the first example (and for an example of section four) consider that the polynomial ring $F[X_1,\ldots,X_n]$ can be readily identified with a subset of a countably infinite cartesian product of F with itself by thinking of $F[X_1,\ldots,X_n]$ as a vector space over F with the countable basis comprising of all the monomials in the X_i. On restricting attention to a subcollection of polynomials bounded by a fixed degree an identification with a finite dimensional affine structure can be made: let $F_k[X_1,\ldots,X_n]$ be the set of all elements of $F[X_1,\ldots,X_n]$ of degree $\leq k$ we can identify $F_k[X_1,\ldots,X_n]$ with an F^N where $N = \binom{n+k}{k}+1$. Our application belongs to the local analysis of differentiable mappings; for the material that follows we rely on Levine [11].

Let $C^k(n)$ denote the set of all k-times continuously differentiable mappings $f:\mathbb{R}^n \to \mathbb{R}^n$ which fix the origin, that is $f(\underline{0}) = \underline{0}$. Mappings $f,g \in C^k(n)$ are said to be <u>equivalent to order k at 0</u> if their partial derivatives of order $\leq k$ coincide at $\underline{0}$; this relation between functions is an equivalence relation and its equivalence classes are called <u>k-jets</u>. A k-jet is an invariant way of referring to a Taylor series. We denote by $J^k(n)$ the set of all k-jets of the C^k functions fixing $\underline{0}$. Clearly an element of $J^k(n)$ can be identified

with the Taylor expansion of any of its representative maps upto and including the k-th partial derivatives. So $J^k(n) = \mathbb{R}^{n(N-1)}$.

Now the operation of composition of mappings makes $C^k(n)$ into a semigroup with identity and this structure for $C^k(n)$ is imitated in the k-jet space $J^k(n)$ by defining $[g]\cdot[f] = [g\circ f]$. Concretely, the Chain Rule for differentiation expresses the partial derivatives of $g\circ f$ as polynomial functions of the partial derivatives of g and those of f : the jet space $J^k(n)$ is trivially isomorphic to an affine space with a polynomial operation. By the Affine Theorem we have that the semigroup of k-jets of C^k mappings $\mathbb{R}^n \to \mathbb{R}^n$ fixing 0 is locally computable. Furthermore it may be observed that the subgroup $L^k(n)$ of $J^k(n)$ consisting of the invertible k-jets is a locally computable group. For negative theorems about $C^k(n)$ see [26].

Turning to the final example, let V be a vector space over the field F. If V possesses a product of vectors which is compatible with the linearity of V then V together with this product is called a linear algebra, precisely a bilinear map $[\ ,\ ] : V\times V \to V$ is required to act as the product. Note that V together with vector addition and such a product constitute a ring, which is not necessarily associative, as the bilinearity of $[\ ,]$ entails the ring distribution laws. Actually linear algebras are classified by means of the properties of their ring structures, for example the alternate, division, Jordan, Lie algebras, see [21].

Assume V is a linear algebra of finite dimension n as a vector space, let $\underline{e}_1,\ldots,\underline{e}_n$ be a basis for V and consider the product of two elements $\underline{x},\underline{y}$ of V. If $\underline{x} = \sum_{i=1}^{n} x_i\underline{e}_i$ and

$\underline{y} = \sum_{i=1}^{n} y_i \underline{e}_i$ then using the linearity of $[\ ,\ ]$ we may write $[\underline{x},\underline{y}] = \sum_{i,j=1}^{n} x_i y_j [\underline{e}_i, \underline{e}_j]$ and are led to consider the n^2 products of the basis elements. In terms of the given basis we derive n^2 expressions, therefore: $[\underline{e}_i, \underline{e}_j] = \sum_{k=1}^{n} \lambda_k^{ij} \underline{e}_k$ and upon substituting these into the expression for the product we find that $[\underline{x},\underline{y}] = \sum_{i,j,k=1}^{n} x_i y_j \lambda_k^{ij} \underline{e}_k$.

The definition of the product in a linear algebra of dimension n is determined by n^3 scalars, the so called structure constants of the algebra. On making the affine identification of V with F^n, an affine ring is obtained: the k-th coordinate function of $[\ ,\ ]$ is the polynomial $p_k(X_1,\ldots,X_n,Y_1,\ldots,Y_n) = \sum_{i,j,k=1}^{n} \lambda_k^{ij} X_i Y_j$; that addition is polynomial is obvious.

We may conclude that the ring structure of any finite dimensional linear algebra over a field is locally computable.

3. The Definability Theorem for $\mathbb{C}^n$

The Affine Theorem asserts that algebraic systems derived directly from the algebra of a field are combinatorially simple. Obviously, the most general operations which may be defined on a set $A \subset F^n$ in terms of the field structure of F are not the polynomials. A far more complicated class can be obtained from the polynomial functions together with the machinery of first-order logic, more general still are those obtained from second-order logic or from infinitary formulae. (One need only think of the use of power series in defining the operations of Lie groups.)

It is a valid and interesting problem to examine precisely this connection between the logical complexity of the operations of the structure $\mathcal{U} \subset F^n$ and the combinatorial complexity of its algebra to find companion, perhaps negative, results which fix a boundary for the structure of the operations beyond which $\mathcal{U}$ is no longer computable. The first-order expressions of field theory fall into a natural hierarchy of quantification analogous to the arithmetic hierarchy classifying expressions into <u>universal</u> (Π_1), <u>diophantine</u> (Σ_1), <u>Skolem</u> (Π_2) and so on, see § 7 of Mal'cev's book [15] for example.

So it is that the Definability Theorems to be proved are solutions to this problem in its most important cases, those of complex and real affine systems. I have decided to adopt a definite point of view toward these particular results and that is to harmonise them with basic conceptions in Algebraic Geometry: this is the most fruitful way of understanding the theorems and is compatible with other material to appear in due course. (An alternate would be to emphasise the model-theoretic point of view which underlies this work on fields.)

An <u>elementary</u> or <u>first-order algebraic expression</u> of field theory is a formula of a first-order logical language with equality equipped with the two binary function symbols $+$, $\cdot$ the two unary operation symbols $-$, $^{-1}$ and the constant symbols 0 , 1 .

Let F be a field and $A \subset F^n$. A map $f : A \to F$ is <u>elementary algebraic</u> iff the relation $f(\underline{x}) = y$ is definable as an elementary algebraic expression, that is, there is an elementary algebraic expression E of $n+1$ free variables such that $f(\underline{x}) = y$ iff $E(\underline{x},y)$ holds on $A \times F$.

Consider some examples. For $F = \mathbb{C}$ or $\mathbb{R}$ the members of $\mathbb{Z}[X_1,\ldots,X_n]$ are elementary algebraic and so are those of $\mathbb{Q}[X_1,\ldots,X_n]$ since they may be rationalised; for example, $p(X_1,X_2,X_3) = \frac{1}{4}X_1^4 + \frac{1}{2}X_2X_1^2 + X_3X_1$ is definable through $x_1^4 + 2x_2x_1^2 + 4x_3x_1 = 4y$.

More generally a map $f : A \subset F^n \to F^m$ is <u>elementary algebraic</u> iff it is definable in the same fashion by an elementary expression of $n+m$ free variables, in particular such a mapping is elementary algebraic iff the coordinate functions $f_1,\ldots,f_m : A \to F$ into which f decomposes are elementary algebraic.

A familiar example is the following. Let C be the prime subfield of F and $r_1,\ldots,r_m \in C(X_1,\ldots,X_n)$ the field of rational functions in n indeterminates over C; let $A \subset F^n$ be such that the denominators of the r_i do not take the value 0 on A. The function $f(X) = (r_1(X),\ldots,r_m(X))$ is elementary algebraic.

Let us also distinguish for the purposes of illustration, and later application, the <u>elementary algebraic subsets</u> of an affine space, obviously $A \subset F^n$ is elementary algebraic iff there is an elementary algebraic expression E of n free variables such that $\underline{x} \in A$ iff $E(\underline{x})$ holds.

Examples of such sets abound. For F a field and C its prime subfield the root spaces of polynomials $p \in C[X_1,\ldots,X_n]$, that is, sets $\{\underline{x} : p(\underline{x}) = 0\}$; their finite unions and intersections; because of the Hilbert Basis Theorem, all those closed subsets of F^n of the Zariski topology which are defined over C are elementary algebraic (such sets form a topology in their own right, the <u>C-Zariski topology</u>). By applying negation, all the open subsets of F^n defined over C are elementary algebraic. Existential quantification adds

the image of an elementary algebraic set under projection: if $A \subset F^{n+m}$ is elementary algebraic defined by $E(\underline{x},\underline{y})$ and P projects F^{n+m} to F^n by deleting the last m coordinates then of course $P(A) = \{\underline{x} \in F^n : (\exists \underline{y})E(\underline{x},\underline{y})\}$ is elementary algebraic.

Let us define a group G within F^n to be an <u>elementary algebraic group</u> if its domain and operations are elementary algebraic; algebraic groups over F defined over the prime subfield C are elementary algebraic, the Classical Matrix Groups are obvious examples.

Now the conjuacy relation in an elementary algebraic group is an elementary algebraic relation: the statement that $\underline{a},\underline{b} \in G$ are conjugate is definable as

$$Conj_G(\underline{a},\underline{b}) \text{ iff } (\underline{a},\underline{b} \in G) \ \& \ (\exists \underline{c} \in G)(\underline{a} = \underline{c}.\underline{b}.\underline{c}^{-1})$$

More generally, we have the relation for $X \subset G$ of X-conjugacy: $\underline{a},\underline{b}$ are conjugate in G by an element of X is definable as

$$Conj_{G,X}(\underline{a},\underline{b}) \text{ iff } (\underline{a},\underline{b} \in G) \ \& \ (\exists \underline{c} \in X)(\underline{a} = \underline{c}.\underline{b}.\underline{c}^{-1})$$

and which is elementary algebraic if X is.

In the case of the complex numbers the elementary algebraic expressions may assume a particularly simple form:

<u>Theorem of Elimination of Quantifiers for Algebraically Closed Fields</u>

Let F be an algebraically closed field. Given any elementary algebraic expression of field theory, say E of n free variables, there exists a sequence of polynomials from $C[X_1,\ldots,X_n]$ say $p_1,q_1,\ldots,p_s,q_s$ such that $E(x)$ holds in F iff

$$\bigvee_{i=1}^{s}\{p_i(X) = 0 \ \& \ q_i(X) \neq 0\}.$$

And furthermore the path from any expression to an appropriate collection of polynomials is effective.

This was discovered by Tarski [23]. The removal of all quantifiers making up E, the reduction of E to the simple algebraic processes of F, is possible (it seems) because of the rich structure of an algebraically closed field in possessing enough elements to solve all equations. A useful reference on quantifier elimination is chapter four of Kreisel and Krivine's book [9].

Let us remark that for F algebraically closed the elementary algebraic subsets of F^n are precisely finite unions of the intersections of pairs of open and closed C-subsets, the so called constructible subsets of F^n in the C-Zariski topology. And that the X-conjugacy problem for an elementary algebraic group G becomes polynomial if X is elementary algebraic.

These necessary preliminaries completed we apply Tarski's theorem to prove the following.

3.1 Definability Theorem for an Algebraically Closed Field

Let F be an algebraically closed field and let $\mathcal{U}$ be an algebraic system whose domain A is a subset of F^n and whose operations $\sigma_1,\ldots,\sigma_k$ and relations $R_1,\ldots,R_s$ are elementary algebraic on F^n. If $\mathcal{U}$ is finitely generated then $\mathcal{U}$ is computable and its relations are decidable.

Let $\{\underline{a}_1,\ldots,\underline{a}_m\} \subset A \subset F^n$ generate $\mathcal{U}$ and let γ be the standard coordinatisation of $\mathcal{U}$ so determined. Again we are to prove $\equiv_\gamma$ is recursive. The strategy is precisely that of the Affine Theorem but a large number of technical modifications are necessary. First consider what Tarski's theorem is to provide.

The term $t(X_1,\ldots,X_m) \in T(X)$ can be thought of as an m-argument operation on A as the σ_i are defined over A and, as such

a function, t is elementary algebraic built inductively from the σ_i and the indeterminates: from t we can effectively find an elementary algebraic expression E_t of $mn+n$ free variables which defines it

$$t(X) = Y \text{ iff } E_t(x,y)$$

(each indeterminate X_i employs n indeterminates $x_{i1},\ldots,x_{in}$ of the language of fields). By the elimination of quantifiers its definition can be effectively simplified to a polynomial condition

$$t(X) = Y \text{ iff } \bigvee_{i=1}^{s_t} \{p_i(X,Y) = 0 \ \& \ q_i(X,Y) \neq 0\}.$$

In particular $t(X) = Y$ is definable throughout F^n by polynomials in $mn+n$ indeterminates whose coefficients are elements of the prime subfield C.

Now this means that for $\underline{a} = (\underline{a}_1,\ldots,\underline{a}_m)$ the relation $t(\underline{a}) = Y$, which arises on substituting $X = \underline{a}$, is defined by a polynomial condition involving elements of C and certain other elements namely those making up the generators $\underline{a}$. We desire a computable structure within which all the possible polynomial conditions arising from all the terms can be tested because this will enable each relation $t(\underline{a}) = Y$ to be enumerated and the unique solution computed if it lies within the structure.

The situation is that of theorem 2.2: we desire a computable affine space E^n into which $\mathcal{U}$ may be effectively embedded. Indeed, we shall prove that such an E^n exists, computable under say β, and that

3.2 Basic Lemma There exists a recursive function $g : \Omega_\gamma \to \Omega_\beta$ such that $\gamma = \beta g$.

whence the theorem will follow exactly as 2.4 follows from 2.3.

Before setting about the construction of the E^n, let us tidy the path from a term to its polynomial definition in the language of fields.

Let $\mathcal{E}$ denote the set of all elementary algebraic expressions and let P denote the set of all conceivable polynomial conditions. These sets are quite clearly constructive and we assume them computably numbered by $\gamma_1 : \Gamma_1 \to \mathcal{E}$ and $\gamma_2 : \Gamma_2 \to P$. Note that P is the set of all finite sequences of even length of elements of $C[X_1,\ldots,X_{mn+n}]$.

We may express the effectiveness of unpacking a term t to its elementary algebraic expression E_t in $\mathcal{E}$ by saying there exists a recursive function $w_1 : \Omega_\gamma \to \Gamma_1$ tracking $u(t) = E_t$, so that the diagram

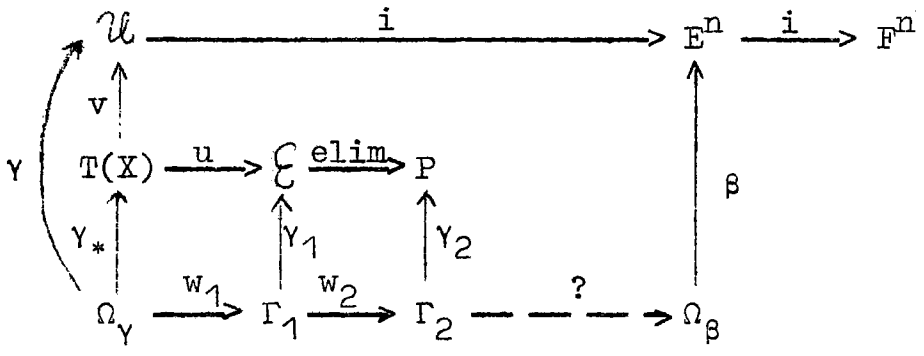
$$\begin{array}{ccc} T(X) & \xrightarrow{u} & \mathcal{E} \\ \uparrow{\scriptstyle \gamma_*} & & \uparrow{\scriptstyle \gamma_1} \\ \Omega_\gamma & \xrightarrow{w_1} & \Gamma_1 \end{array}$$

commutes.

And we may express the effectiveness of Tarski's procedure for eliminating quantifiers from E_t to obtain the polynomial condition p_t by saying there exists a recursive function $w_2 : \Gamma_1 \to \Gamma_2$ tracking $\mathrm{elim}(E_t) = p_t$, so that

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\mathrm{elim}} & P \\ \uparrow{\scriptstyle \gamma_1} & & \uparrow{\scriptstyle \gamma_2} \\ \Gamma_1 & \xrightarrow{w_2} & \Gamma_2 \end{array}$$

commutes. Given the existence of E^n the Basic Lemma requires us to close the gap:



Consider the operations of $\mathcal{U}$ more intimately, we must make a number of preliminary constructions. A is a subset of F^n and if σ is an r-ary operation of $\mathcal{U}$ then it decomposes into n coordinate functions $\sigma^1,\ldots,\sigma^n : A^r \to F$, functions essentially $F^{nr} \to F$.

Let $\underline{x}_1,\ldots,\underline{x}_s \in F^{nr}$. By $C(\underline{x}_1,\ldots,\underline{x}_s)$ we denote the finite extension of C given by $C(\{x_{ij}^k : 1 \leq i \leq r,\ 1 \leq j \leq n,\ 1 \leq k \leq s\})$ where x_{ij}^k is the j-th coordinate of the i-th n-tuple making up $\underline{x}_k$. By $\overline{C(\underline{x}_1,\ldots,\underline{x}_s)}$ we denote the algebraic closure of $C(\underline{x}_1,\ldots,\underline{x}_s)$.

3.3 Lemma For any $\underline{x}_1,\ldots,\underline{x}_s \in F^{nr}$, $\overline{C(\underline{x}_1,\ldots,\underline{x}_s)}$ is a computable subfield of F.

Proof: A finite extension of the prime field C is computable (lemma 1.3) and the algebraic closure of a computable field is computable (lemma 1.4). $\overline{C(\underline{x}_1,\ldots,\underline{x}_s)}$ is a subfield of F because F is algebraically closed.

Q.E.D.

Here is the computable affine space. Take E to be the algebraic closure of the prime subfield extended by all the mn elements of F making up the generators. If E is computable under α, let E^n be computable under $\beta = \alpha^n$. The first task is to prove $A \subset E^n$; the following lemma is a technical device.

3.4 Lemma Let σ be an r-ary operation of $\mathcal{U}$. If $\underline{a} \in A^r$ then $\sigma(\underline{a}) \in \overline{C(\underline{a})}^n$.

Proof: The definability of σ as an elementary algebraic expression is the definability of its n coordinate functions σ^i as elementary algebraic expressions:

$\sigma^i(X) = Y$ iff $E^i(x,y)$ for an appropriate formula of $nr+1$ free variables;

iff $\bigvee_{j=1}^{s_i} \{p_j(X,Y) = 0 \ \&\ q_j(X,Y) \neq 0\}$ by elimination.

Now consider $\sigma^i(\underline{a})$ for any $\underline{a} \in A^r$. If $\sigma^i(\underline{a}) = b_i$ then from the polynomial condition we know that $p_j(\underline{a},b_i) = 0$ for at least one of the polynomials. We rewrite this equation as $p_j(\underline{a})(b_i) = 0$ thinking of $p_j(\underline{a})(Y)$ as a polynomial over $C(\underline{a})$. Thus b_i is a root of such a polynomial and must be algebraic over $C(\underline{a})$; thus each coordinate of $\sigma(\underline{a})$ lies in $\overline{C(\underline{a})}$.

Q.E.D.

3.5 Lemma $A \subset E^n$.

Proof: As with lemma 2.5 we show that for each $t \in T(X)$, $v(t) \in E^n$ by induction on term length.

Basis. The generators of $\mathcal{U}$ lie in E^n by construction so the terms of length zero all map into E^n.

Induction Step. Assume that all terms of length $< l$ map into E^n under v, let t be any term of length l. Breaking t down into its component subterms write $t = \sigma(t_1,\ldots,t_r)$ say. Now since v is a homomorphism $v(t) = \sigma(vt_1,\ldots,vt_r)$ and let $vt_i = \underline{z}_i$ for $1 \leq i \leq r$ and let $\underline{z} = (\underline{z}_1,\ldots,\underline{z}_r) \in A^r$. By the induction hypothesis $\underline{z} \in E^{nr}$ and so $\overline{C(\underline{z})}^n \subset E^n$ since E is algebraically closed. By lemma 3.4, $\sigma(\underline{z}) \in \overline{C(\underline{z})}^n$, and $\sigma(\underline{z}) \in E^n$.

By induction, all the t map under v into E^n.

Q.E.D.

We must set up the machinery which is to test the polynomial conditions obtained from quantifier elimination on the generators $\underline{a}_1,\ldots,\underline{a}_m$ in E^n: it is easy to apply this procedure to define g of the Basic Lemma.

The path from the term t to its polynomial definition p_t is

constructive, tracked by $w_2 w_1$. At

$$t(X) = Y \text{ iff } p_t(X,Y) \equiv \bigvee_{i=1}^{s_t} \{p_i(X,Y) = 0 \ \& \ q_i(X,Y) \neq 0\}$$

we insert $\underline{a} = (\underline{a}_1,\ldots,\underline{a}_m)$ for X and pass over to

$$t(\underline{a}) = Y \text{ iff } \bigvee_{i=1}^{s_t} \{p_i(\underline{a})(Y) = 0 \ \& \ q_i(\underline{a})(Y) \neq 0\}.$$

We arrive at a condition involving $2s_t$ polynomials from the ring $E[Y]$ of all n argument polynomials with coefficients in E. To test on a given $\underline{y} \in E^n$ whether or not $t(\underline{a}) = \underline{y}$ is to undertake to calculate at most $2s_t$ polynomials for the value $\underline{y}$ and test the answers for equality or inequality with 0: there will exist for each t one and only one $\underline{y} \in E^n$ for which the condition will be satisfied. The precise mechanism is provided by the algebra of polynomials over E and is constructive.

Let us collect together all the E-polynomial conditions we might need: let P_2 denote the set of all finite sequences of polynomials from $E[Y]$ which have even length. From the computable coordinatisation α of E construct computable coordinate systems for $E[Y]$ and then $\mathrm{FinSeq}(E[Y])$ say θ and $\bar{\theta}$ respectively. It is completely clear (from our remarks on Sets in section one) that P_2 is a computable subset of $\mathrm{FinSeq}(E[Y])$ and for convenience of notation let it have coordinate system $\gamma_3 = \bar{\theta}$ restricted to $\Gamma_3 = \bar{\theta}^{-1}(P_2)$. The passage from P to P_2 we denote sub, $\mathrm{sub}(p_1(X,Y),\ldots,p_s(X,Y)) = (p_1(\underline{a})(Y),\ldots,p_s(\underline{a})(Y))$; it is constructive: there exists a recursive function $w_3 : \Gamma_2 \to \Gamma_3$ which commutes the diagram

$$\begin{array}{ccc} P & \xrightarrow{\mathrm{sub}} & P_2 \\ {\scriptstyle\gamma_2}\uparrow & & \uparrow{\scriptstyle\gamma_3} \\ \Gamma_2 & \xrightarrow{w_3} & \Gamma_3 \end{array}.$$

Now there is an action $A : \mathrm{FinSeq}(E[Y]) \times E^n \to \mathrm{FinSeq}(E)$ defined by $A(p_1,\ldots,p_s;\underline{y}) = (p_1(\underline{y}),\ldots,p_s(\underline{y}))$ and it is constructive. From α construct a computable coding of $\mathrm{FinSeq}(E)$ say $\bar{\alpha}$; the action A is defined directly from the computable action e of $E[Y]$ on E^n (lemma 1.2) and for it can be constructed a recursive tracking function $a : \Omega_{\bar{\theta}} \times \Omega_\beta \to \Omega_{\bar{\alpha}}$. Apply this action to P_2. Let $\mathrm{FinSeq}_2(E)$ be the set of all finite sequences of elements of E of even length computable under $\bar{\alpha}$ restricted to $\Omega_{2\bar{\alpha}}$, say.

3.6 Lemma The restriction $A : P_2 \times E^n \to \mathrm{FinSeq}_2(E)$ is computable tracked by $\bar{a} : \Gamma_3 \times \Omega_\beta \to \Omega_{2\bar{\alpha}}$.

We are endeavouring to demonstrate

3.7 Lemma The characteristic map $\chi : P_2 \times E^n \to \{0,1\}$ defined by

$$\chi(p_1,q_1,\ldots,p_s,q_s;\underline{y}) = 0 \quad \text{if} \quad \bigvee_{i=1}^{s} \{p_i(\underline{y}) = 0 \;\&\; q_i(\underline{y}) \neq 0\}$$

$$= 1 \quad \text{otherwise};$$

is computable.

This is achieved by lemma 3.6 together with

3.8 Lemma The checking function $c : \mathrm{FinSeq}_2(E) \to \{0,1\}$ defined by

$$c(x_1,y_1,\ldots,x_s,y_s) = 0 \quad \text{if} \quad \bigvee_{i=1}^{s} \{x_i = 0 \;\&\; y_i \neq 0\}$$

$$= 1 \quad \text{otherwise};$$

is computable.

Proof: Define $\bar{c} : \Omega_{2\bar{\alpha}} \to \{0,1\}$ by

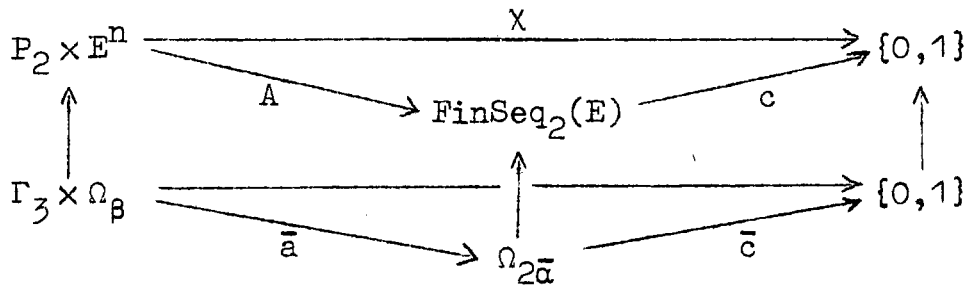
$$\bar{c}(n_1,m_1,\ldots,n_s,m_s) = 0 \quad \text{if} \quad \bigvee_{i=1}^{s} \{n_i \equiv_\alpha 0 \;\&\; m_i \not\equiv_\alpha 0\}$$

$$= 1 \quad \text{otherwise};$$

$\bar{c}$ clearly tracks c and is recursive since $\equiv_\alpha$ is.

Q.E.D.

Now χ in lemma 3.7 can be recursively tracked by $w = \bar{c}\,\bar{a}$:



Given t, we effectively enumerate E^n to discover that $\underline{y}$ such that $t(\underline{a}) = \underline{y}$. This is implemented by the function

$$g(n) = (\mu m \in \Omega_\beta)[w(w_3 w_2 w_1(n), m) = 0]$$

which establishes the Basic Lemma.

Finally we must show that the relations of $\mathcal{U}$ are decidable. Let R be an r-ary relation of $\mathcal{U}$, since it is elementary algebraic we have

$$R(X_1,\ldots,X_r) \quad \text{iff} \quad \bigvee_{i=1}^{s_R} \{p_i(X) = 0 \ \& \ q_i(X) \neq 0\}$$

for some polynomials from the ring $C[X]$ in nr indeterminates. It must be shown that the set $\gamma^{-1}R = \{(n_1,\ldots,n_r) : \gamma^r(n_1,\ldots,n_r) \in R\}$ is recursive. We proceed as follows: given $(n_1,\ldots,n_r)$ we compute their β labels as elements of E^n using g, so $(n_1,\ldots,n_r) \in \gamma^{-1}R$. Over E^n we apply and test the polynomial definition of R. To implement this requires new machinery analogous to the action A of lemma 3.6, new because we are now calculating polynomials in nr variables in place of mn. Given such equipment and using the same notations, $(n_1,\ldots,n_r) \in \gamma^{-1}R$ iff $\bar{c}\,\bar{a}(n_1,\ldots,n_r) = 0$ will do in proving the appropriate analogue of lemma 3.7.

This completes the proof of the theorem.

Q.E.D.

In particular: finitely generated algebraic systems made from complex numbers using the field algebra of $\mathbb{C}$ together with first-order logic are computable.

Here is a more sophisticated corollary.

3.9 Theorem Let H be an elementary algebraic group over the algebraically closed field F, say $H \subset F^n$. Let G be a finitely generated subgroup of H. Then G is computable and the following variant of the conjugacy problem for G is effectively soluble: if $X \subset H$ is an elementary algebraic set then to determine for arbitrary $g_1, g_2 \in G$ whether or not g_1 and g_2 are conjugate in H by an element of X.

Proof: Quite clearly G is a finitely generated affine system and the relation of X-conjugacy is elementary algebraic.

Q.E.D.

So let H be a closed subgroup of $GL(n,F)$ defined over the prime subfield C of F, by definition a rational algebraic subgroup of $GL(n,F)$. And let G be any finitely generated subgroup of H. If X is a C-defined algebraic subset of $GL(n,F)$ - such as H or $GL(n,F)$ itself - then the X-conjugacy problem of G is effectively soluble. Concentrating on the C-Zariski topology defined on F^{n^2}, note that the topological closure of G in H is a subgroup of H. Taking X to be this rational closure of G we deduce

3.10 Corollary Let H be a rational subgroup of $GL(n,F)$. For any finitely generated subgroup G of H there exists a rational subgroup K of H such that

G is dense in K (in the C-topology) and the conjugacy problem of G with respect to K is effectively decidable.

In contrast C.F. Miller, III has shown the existence of finitely generated subgroups of $GL(n,\mathbb{Z})$ with unsolvable (ordinary) conjugacy problem, [16, p. 42]. (The reader may find chapters two and twelve of [8] useful for an exposition of these ideas about algebraic groups.)

4. The Definability Theorem for $\mathbb{R}^n$

The effective elimination of quantifiers from the elementary algebraic expressions over an algebraically closed field derives from what is the most well known result of this kind: Tarski's seminal discovery of the effective elimination of quantifiers from the language of elementary geometry which supports his proof of the decidability of the elementary theory of Euclidean Geometry, see Tarski's [23]. This result is now more usually understood in an algebraic setting since the algebra of elementary geometry has been found to be represented in that of the real closed fields, see [24]. The fundamental geometric concept of order finds its algebraic expression in a real closed field which sustains one and only one sensible ordering and which may be defined $x < y$ iff $(\exists z)(z \neq 0 \ \& \ x+z^2 = y)$. By augmenting the syntax of our language for field theory by the symbol $<$ we obtain a larger class of expressions, the language of fields with orderings; over a real closed field these two languages define the same class of sets, of course. Tarski's work leads to the following simplification:

Theorem of Elimination of Quantifiers for Real Closed Fields

> Let F be a real closed field. Given any elementary algebraic expression of field theory with orderings, say E of n free variables, there exists a sequence of polynomials from $C[X_1,\ldots,X_n]$ say $p_1,q_1,\ldots,p_s,q_s$ such that $E(x)$ holds in F iff $\bigvee_{i=1}^{s}\{p_i(X) = 0 \ \& \ q_i(X) > 0\}$.
>
> And furthermore the path from any expression to an appropriate collection of polynomials is effective.

See Seidenberg's paper [20].

Following the proof of the Definability Theorem for Algebraically Closed Fields it is to be expected that an analogous result should hold for $\mathbb{R}^n$ and the real closed fields in general: that the simplification to polynomial conditions can be employed and effectively tested in some replacement structure for E. As will be demonstrated this is not possible.

The elementary algebraic expressions of fields with orderings distinguish special classes of mappings between affine spaces over ordered fields in the same way as the elementary algebraic expressions of field theory did. The elementary algebraic expressions of fields with orderings we shall call the <u>elementary</u> or <u>first-order geometric expressions</u> when and only when they refer to real closed fields. In such circumstances we may define the elementary geometric mappings and sets as we did for the elementary algebraic expressions. Thus we may state the obvious expected result for $\mathbb{R}^n$ as

> if $\mathcal{U}$ is a finitely generated algebraic system whose domain is a subset of $\mathbb{R}^n$ and whose operations and relations are elementary geometric then $\mathcal{U}$ is computable and its relations are decidable.

For a counterexample to this assertion consider the subfield of the real numbers generated by 1 and r where r is taken to be a non-computable real number. This field is $\mathbb{Q}(r)$ of course; it is computable, yet consider the ordering relation $<$ on $\mathbb{Q}(r)$ inherited from $\mathbb{R}$: $<$ is elementary geometric but it cannot be decidable since this would stand in direct contradiction of the fact that r is non-computable. It is easy to construct non-computable finitely generated structures. For material on computable real numbers consult Rice's paper [19].

Let us consider more exactly, then, the steps involved in attempting an apparently unremarkable adaptation of the proof of the last section. A computable structure R is required to replace E which would contain A and allow a Basic Lemma. E must be replaced because the polynomial conditions provided by the new elimination require a different form of testing, involving the non-algebraic notion of "positiveness": R must have an appropriate computable ordering to allow a replacement lemma 3.8. The correct R is clear: extend $\mathbb{Q}$ by all the real numbers making up the generators of $\mathcal{U}$ and take this extension field's real closure [28, p. 253]. For this field lemma 3.5 may be proved and the strategy preserved. The breakdown occurs in our inability to replace lemma 3.3, for the real closure of a computable field need not be computable, the correct R fails to guarantee the polynomial conditions are effectively testable. This is of some interest being a feature of the singular algebraic behaviour possible in the relationship between orderings in fields and their algebra; by examining the question directly we shall quickly discover the Definability Theorem for $\mathbb{R}^n$ and come to understand why this result is not unnatural.

Our example involving $\mathbb{Q}(r)$ demonstrates that in general the complexity of the ordering of a field may be independent of the complexity of its field structure. It is clear that this independence may disappear in an appropriately richer algebraic system which can accommodate the ordering properly, for example in the real closure of an ordered field wherein the ordering is uniquely definable in the field structure. Notice, then, that if F is real closed and computable its ordering is computable so we deduce immediately that the real closure of our $\mathbb{Q}(r)$ is <u>not</u> computable.

Here it is that the argument with R fails when the algebraic system includes non-computable real numbers.

The constructive relationship between ordered fields and their real closures has been the subject of papers by A.H. Lachlan and E.W. Madison [10, 12] and we may conclude the situation in $\mathbb{R}^n$ by citing their discoveries.

If F is a computable subfield of the real numbers with its ordering computable then F must be a proper subfield of the field of computable reals, if F is not such a subfield then no field containing F and extending its ordering may be computable, [10]. If F is a computable field with a computable ordering then its real closure is a computable field, [12].

To these facts we add that a finite extension of $\mathbb{Q}$ by computable real numbers is a computable field with a computable ordering; these results enable us to prove the following by means of the argument of the last section.

Definability Theorem for $\mathbb{R}^n$

Let $\mathcal{U}$ be an algebraic system whose domain A is a subset of $\mathbb{R}^n$ and whose operations $\sigma_1,\ldots,\sigma_k$ and relations $R_1,\ldots,R_s$ are elementary geometric on $\mathbb{R}^n$. If $\mathcal{U}$ is finitely generated by vectors involving computable real numbers only, then $\mathcal{U}$ is computable and its relations are decidable.

This last step involving finite extensions of $\mathbb{Q}$ we must leave to the reader to adapt from Rice's paper [19, p. 785]. A more thorough account of the relationship between fields and their orderings, in terms of one, many-one, and Turing degrees, is to be included in [26]. The papers [6,13,17] make interesting and necessary reading in this connection.

From this vantage point the theorem explains itself in the following way: first, orderings in fields are not part of the algebraic point of view towards a field. This is clear from van der Waerden's examples which introduce his exposition of the subject [28] and is underlined by attention to complexity - for example, by the fact that all the Turing degrees can be realised in the field orderings of computable fields, [26] - and this is quite simply because some orderings can escape the quintessential feature of the algebraic concept: that it does not involve the nature of the elements of the system. Turning to the Definability Theorems their similarity in simple algebraic terms is misleading: in $\mathbb{C}^n$ algebraic definability can be reduced to algebraic definability in the large (as it were), in $\mathbb{R}^n$ it can be reduced to the geometric structure of $\mathbb{R}$. The computable reals represent, in combinatorial terms, what is constructive about the geometry of $\mathbb{R}$.

We conclude with an illustration of an elementary geometric system.

Consider the Lie algebra $\mathbb{P}$ of all polynomial vector fields on $\mathbb{R}^n$. Typically $\underline{v} \in \mathbb{P}$ is an n-tuple of elements of $\mathbb{R}[X_1,\ldots,X_n]$ whence $\mathbb{P}$ can be identified with the n-fold sum of a vector space of countably infinite dimension over the reals. On considering vector fields of degree bounded by k (that is $\underline{v} = (v_1,\ldots,v_n)$ such that each v_i is of degree $\leq k$) we obtain a finite dimensional system $\mathbb{P}_k$ naturally identified with the n-fold sum of $\mathbb{R}^{\binom{n+k}{k}+1}$ and abbreviated $\mathbb{R}^N$. (Notice that the Lie product must be dropped since $\mathbb{P}_k$ is not a Lie subalgebra unless $k = 1$. Of course, we could employ the product together with truncation.) What is of interest is $\mathbb{P}_k$ as a relational structure. For example, among the many relations it supports is the N-ary relation $S(\underline{v})$ meaning

"$\underline{v}$ is stable at $\underline{0}$" and the 2N-ary relation $T(\underline{u},\underline{v})$ meaning "$\underline{u}$ and $\underline{v}$ are topologically equivalent", for these concepts the reader is recommended Arnold's book [1]. Clearly such relations are not prescribed in first-order terms. Let us concentrate on $S(\underline{v})$. From the point of view of the theory of differential equations, one is interested in obtaining algebraic criteria for stability, polynomial conditions of some kind or other. For $k=1$ such is known, it is the Routh test which is a condition on the coefficients of a linear vector field defined in terms of polynomials over $\mathbb{Q}$ and the order relation in $\mathbb{R}$; in particular it is elementary geometric, see [2, pp. 70-82]. We know directly from the Affine Theorem that the ring structure of $\mathbb{P}_1$ is locally computable. Providing one includes computable real numbers only then each such finitely generated subring has decidable stability problem. Actually it is possible to show that there exist finitely generated subrings with undecidable stability problem so the ordering condition is intrinsic to characterisations of stability even for small classes of linear vector fields [26].

To digress further let us note that extensions to complex linear systems of the algebraic criteria of Routh, as in the work of R.J. Duffin [5], cannot escape from involving orderings: the undecidable systems for $\mathbb{R}^n$ are automatically undecidable finitely generated affine systems in $\mathbb{C}^n$ so that the stability of a linear dynamical system on $\mathbb{C}^n$ is not first order definable over $\mathbb{C}$.

For $k>1$ let us observe that if there exists a k such that some finitely generated elementary geometric subsystem of $\mathbb{P}_k$ - involving computable reals only - has undecidable stability problem then one may conclude that the absence of an algebraic criterion is

dramatic in that the property cannot be elementary geometric. This question is open and has been recently posed by Arnold [3, p. 59].

There are a number of natural extensions of the theorems in this paper: first one may care to relax the condition that the affine systems be finitely generated. This can be done immediately for an algebraically closed field by scrutinising the construction of infinite field extensions, see Fröhlich and Shepherdson's [7]. Secondly, one may care to open up the problems for other fields and rings. Thirdly, there is the analysis of the model-theoretic properties which underlie the theorems; this problem I hope will be the subject of a paper of mine in due course.

References

[1] V.I. Arnold — Ordinary differential equations (Translated by R.A. Silverman.) M.I.T. Press, Cambridge, Massachusetts, 1973.

[2] R. Bellman & R. Kalaba (eds.) — Selected papers on mathematical trends in control theory Dover Publications, New York, 1964.

[3] F.E. Browder (ed.) — Mathematical developments arising from Hilbert's problems American Mathematical Society, Providence, Rhode Island, 1976.

[4] P.M. Cohn — Universal algebra Harper & Row, New York, 1965.

[5] R.J. Duffin — Algorithms for classical stability problems SIAM Review 11 (1969) pp. 196-213.

[6] Y.L. Ershov — Numbered fields pp. 31-34 of Logic, methodology and philosophy of science III, edited by B. van Rootselaar & J.F. Staal, North-Holland, Amsterdam, 1968.

[7] A. Fröhlich & J.C. Shepherdson — Effective procedures in field theory Philosophical Transactions Royal Society London (A) 248 (1956) pp. 407-432.

[8] J.E. Humphreys — Linear algebraic groups Springer-Verlag, New York, 1975.

[9] G. Kreisel & J.L. Krivine — Elements of mathematical logic North-Holland, Amsterdam, 1971.

[10] A.H. Lachlan & E.W. Madison — Computable fields and arithmetically definable ordered fields Proceedings American Mathematical Society, 24 (1970) pp. 803-807.

[11] H.I. Levine — Singularities of differentiable mappings
pp. 1-89 of Proceedings of Liverpool singularities - symposium 1, edited by C.T.C. Wall, Springer-Verlag, Berlin, 1971.

[12] E.W. Madison — A note on computable real fields
Journal Symbolic Logic 35 (1970) pp. 239-241.

[13] E.W. Madison — Some remarks on computable (non-Archimedean) ordered fields
Journal London Mathematical Society (2) 4 (1971) pp. 304-308.

[14] A.I. Mal'cev — Constructive algebras I
pp. 148-214 of The meta-mathematics of algebraic systems. Collected papers: 1936-1967 translated and edited by B.F. Wells, III, North-Holland, Amsterdam, 1971.

[15] A.I. Mal'cev — Algebraic systems
(Translated by B.D. Seckler & A.P. Doohovskoy.) Springer-Verlag, Berlin, 1973.

[16] C.F. Miller, III — On group-theoretic decision problems and their classification
Princeton University Press, Princeton, New Jersey, 1971.

[17] Y.N. Moschovakis — Notation systems and recursive ordered fields
Compositio Mathematica 17 (1965) pp. 40-71.

[18] M.O. Rabin — Computable algebra, general theory and the theory of computable fields
Transactions American Mathematical Society 95 (1960) pp. 341-360.

[19] H.G. Rice — Recursive real numbers
Proceedings American Mathematical Society 5 (1954) pp. 784-791.

[20] A. Seidenberg — A new decision method for elementary algebra
Annals Mathematics 60 (1954) pp. 365-374.

[21] R.D. Schafer — An introduction to non-associative algebras
Academic Press, New York, 1966.

[22] I.R. Shafarevich — Basic algebraic geometry
Springer-Verlag, Berlin, 1974.

[23] A. Tarski — A decision method for elementary algebra and geometry
University of California Press, Berkeley, 1951.

[24] A. Tarski — What is elementary geometry?
pp. 164-175 of The philosophy of mathematics, edited by J. Hintikka, Oxford University Press, London, 1969.

[25] J.V. Tucker — Computability as an algebraic property. Part one: general theory
Matematisk institutt, Universitetet i Oslo, Preprint Series, Oslo 1977.

[26] J.V. Tucker — Computability as an algebraic property. Part two: applications
Matematisk institutt, Universitetet i Oslo, Preprint Series, Oslo. In preparation.

[27] B.L. van der Waerden — Modern algebra I
(Translated by F. Blum)
Frederick Ungar, New York, 1949.

[28] B.L. van der Waerden — Algebra I
(Translated by F. Blum & J.R. Schulenberger)
Frederick Ungar, New York, 1970.