PACIFIC JOURNAL OF MATHEMATICS
Vol. 34, No. 2, 1970

THE SOLUTION OF A DECISION PROBLEM FOR SEVERAL CLASSES OF RINGS

H. SIMMONS

This paper is concerned with the solution of certain decision problems for classes of associative commutative rings. We consider several such classes defined by restricting the nature of the rings, e.g., by specifying the characteristic. If $\mathscr{K}$ is any of these classes we consider the problem of deciding which universal sentences are true in (all members of) $\mathscr{K}$. We show that this problem is recursively solvable.

In § 1 we define our terminology, give a precise description of the problem, and state the main theorem. In § 2 we make certain reductions of the problem. Basically we show that it is sufficient to be able to solve linear equations over polynomial domains. In §'s 3 and 4 we show that these linear equations can be solved.

The techniques used in this paper can also be used to show that the word problem for commutative semigroups is solvable.

1. Introduction.

Throughout this paper we deal with rings which are both associative and commutative. Thus, from now on, 'ring' will mean 'associative commutative ring'.

By a ring we mean a structure $(A, +, \cdot, -, 0)$ which satisfies the usual axioms for rings. Let $\mathscr{R}$ be the class of rings. Associated with $\mathscr{R}$ there is the obvious first order language $\mathscr{L}$. This language has logical symbols $\neg$, $\vee$, &, $\rightarrow$, $\forall$, $\exists$, $=$, and extra-logical symbols $+$, $\times$, $-$, $\mathbf{0}$, and the the usual punctuation symbols. (It is not necessary to include '$-$' in the type of $\mathscr{R}$ and '$-$' in the language $\mathscr{L}$, however it is convenient to do so.)

By a ring with identity we mean a structure $(A, +, \cdot, -, 0, 1)$ which satisfies the usual axioms. (We assume that these axioms imply that 0,1 are distinct.) Let $\mathscr{R}(1)$ be the class of rings with identity. Associated with $\mathscr{R}(1)$ there is the obvious first order language $\mathscr{L}(1)$. This is like $\mathscr{L}$ except that it has another extra-logical symbol **1**. (Among the axioms for $\mathscr{R}(1)$ will be the sentence $\neg(\mathbf{0} = \mathbf{1})$.)

We use 'term', 'atomic formula', 'formula', 'sentence', etc. in the usual way to describe certain entities of $\mathscr{L}$ and $\mathscr{L}(1)$. However, since we have two languages we sometimes have to be more precise and say '$\mathscr{L}$-term', '$\mathscr{L}(1)$-formula', '$\mathscr{L}$-sentence', etc. Notice that every $\mathscr{L}$-term, $\mathscr{L}$-formula, $\mathscr{L}$-sentence, etc. is also an $\mathscr{L}(1)$-term, $\mathscr{L}(1)$-formula, $\mathscr{L}(1)$-sentence, etc.

It is convenient to introduce into $\mathscr{L}(1)$ the abbreviations **2**, **3**, **4**, 5, $\cdots$, for $1 + 1$, $2 + 1$, $3 + 1$, $4 + 1$, $\cdots$ respectively.

For each integer $c \geqq 2$ let $\mathscr{R}_c$ be the subclass of $\mathscr{R}$ of rings whose characteristics divide c. Similarly we define $\mathscr{R}_c(1)$. Thus $\mathscr{R}_c(1)$ is the class of rings with identity which satisfy the $\mathscr{L}(1)$-sentence $c = 0$. Let $\mathscr{R}_c'$, $\mathscr{R}_c'(1)$ be the subclasses of $\mathscr{R}_c$, $\mathscr{R}_c(1)$ of rings of characteristic exactly c. Thus each member of $\mathscr{R}_c'(1)$ satisfies

$$\neg(1 = 0) \& \neg(2 = 0) \& \cdots \& \neg(d = 0) \& (c = 0)$$

where $d = c - 1$. Notice that $\mathscr{R}_c' \subseteqq \mathscr{R}_c \subseteqq \mathscr{R}$ and

$$\mathscr{R}_c'(1) \subseteqq \mathscr{R}_c(1) \subseteqq \mathscr{R}(1) .$$

Let $\mathscr{R}_0$, $\mathscr{R}_0(1)$ be the subclasses of $\mathscr{R}$, $\mathscr{R}(1)$ of rings which satisfy all the sentences

$$(\forall x)[x + \cdots m \text{ times} \cdots + x = 0 \rightarrow x = 0]$$

for $m \geqq 1$. We say these rings are torsion free (since their additive groups are torsion free). Also let $\mathscr{R}_0'$, $\mathscr{R}_0'(1)$ be the subclasses of $\mathscr{R}$, $\mathscr{R}(1)$ of rings of characteristic zero. Notice that $\mathscr{R}_0 \subseteqq \mathscr{R}_0' \subseteqq \mathscr{R}$ and $\mathscr{R}_0(1) \subseteqq \mathscr{R}_0'(1) \subseteqq \mathscr{R}(1)$.

Let $\mathscr{K}$ be any of the above defined classes of rings. Let $T(\mathscr{K})$ be the elementary theory of $\mathscr{K}$ (i.e., the set of sentences which are true in all members of $\mathscr{K}$). From the works of Tarski, Rabin, Eršov it easily follows that $T(\mathscr{K})$ is undecidable (i.e., not recursive). For details see [1]. We are going to show that a certain subset $U(\mathscr{K})$ of $T(\mathscr{K})$ is recursive.

A universal sentence is a sentence in prenex normal form containing no existential quantifiers.

For each class $\mathscr{K}$ of rings let $U(\mathscr{K})$ be the set of universal sentences which hold in all members of $\mathscr{K}$. Thus $U(\mathscr{K}) \subseteqq T(\mathscr{K})$. In this paper we prove the following theorem.

MAIN THEOREM. *Let $\mathscr{K}$ be any of the following subclasses of $\mathscr{R}$:*

$$\mathscr{R},\ \mathscr{R}_c,\ \mathscr{R}_0,\ \mathscr{R}_c',\ \mathscr{R}_0'$$

for $c \geqq 2$, and let $\mathscr{K}(1)$ be the corresponding subclass of $\mathscr{R}(1)$. Then

(a) *$U(\mathscr{K})$ is recursive,*

(b) *$U(\mathscr{K}(1))$ is recursive if $\mathscr{K} \neq \mathscr{R}_0'$.*

Three remarks about this theorem:

(1) The theorem gives us no information about $U(\mathscr{R}_0'(1))$.

(2) The methods we use show that most of the above sets

are primitive recursive. In fact only $U(\mathscr{R}(1))$, $U(\mathscr{R})$, $U(\mathscr{R}_0')$ are not shown to be primitive recursive.

(3) The corresponding results for fields and integral domains follows from the decidability of the theory of algebraically closed fields.

2. Some preliminary reductions. In this section we show that for the main theorem to be true it is sufficient to be able to solve linear equations over certain polynomial domains. We do this by making several reductions of the problems, most of which are fairly standard.

Sections 3 and 4 and the last part of this section are devoted to proving the following theorem.

THEOREM 1. *The following sets of* $\mathscr{L}(1)$*-sentences are recursive:*
(i) $U(\mathscr{R}(1))$.
(ii) $U(\mathscr{R}_0(1))$.
(iii) $U(\mathscr{R}_c(1))$ *for any integer* $c \geqq 2$.

Once we have Theorem 1 the remainder of the main theorem is fairly easy. We use the following lemma.

LEMMA 2. *Let* $\mathscr{K}$ *be any of the above defined subclasses of* $\mathscr{R}$, *and let* $\mathscr{K}(1)$ *be the corresponding subclass of* $\mathscr{R}(1)$. *Let c be any integer* $\geqq 2$.
(a) *If* $U(\mathscr{K}(1))$ *is recursive then so is* $U(\mathscr{K})$.
(b) *If* $U(\mathscr{R})$ *is recursive then so is* $U(\mathscr{R}_0')$.
(c) *If* $U(\mathscr{R}_c(1))$ *is recursive then so is* $U(\mathscr{R}_c'(1))$.

To obtain the main theorem from Theorem 1 and Lemma 2 we use the following chains of implication.

$$
\begin{array}{ccccc}
 & & & & \mathscr{R}_0' \\
 & & & & \big\downarrow{\scriptstyle (b)} \\
\text{(i)} & \longrightarrow & \mathscr{R}(1) & \xrightarrow{(a)} & \mathscr{R} \\
\text{(ii)} & \longrightarrow & \mathscr{R}_0(1) & \xrightarrow{(a)} & \mathscr{R}_0 \\
\text{(iii)} & \longrightarrow & \mathscr{R}_c(1) & \xrightarrow{(a)} & \mathscr{R}_c \\
 & & \big\downarrow{\scriptstyle (c)} & & \\
 & & \mathscr{R}_c'(1) & \xrightarrow{(a)} & \mathscr{R}_c'
\end{array}
$$

Proof of Lemma 2. (a) Let σ be any universal $\mathscr{L}$-sentence. Since every member of $\mathscr{K}(1)$ is a (reduct of a) member of $\mathscr{K}$ we have

$$\mathscr{K} \models \sigma \Rightarrow \mathscr{K}(1) \models \sigma \,.$$

It is well known that every member of $\mathscr{K}$ can be embedded in a member of $\mathscr{K}(1)$. Thus, since universal sentences are preserved under passage to substructure, we have

$$\mathscr{K}(1) \models \sigma \Rightarrow \mathscr{K} \models \sigma \,.$$

Hence, for any universal $\mathscr{L}$-sentence σ,

$$\sigma \in U(\mathscr{K}) \Leftrightarrow \sigma \in U(\mathscr{K}(1)) \,,$$

which gives (a).

(b) Every ring can be embedded in a ring of zero characteristic, hence (b) follows in the same way as (a).

(c) Let α be the quantifier-free $\mathscr{L}(1)$-sentence

$$\mathbf{1} \neq \mathbf{0} \,\&\, \cdots \,\&\, \boldsymbol{d} \neq \mathbf{0}$$

where $d = c - 1$. Let σ be any universal $\mathscr{L}(1)$-sentence. Then

$$\mathscr{R}_c'(1) \models \sigma \Leftrightarrow \mathscr{R}_c(1) \models \alpha \rightarrow \sigma \,.$$

Thus, since $\alpha \rightarrow \sigma$ is (equivalent to) a universal sentence, we get (c).

In order to extend the main theorem to include the class $\mathscr{K} = \mathscr{R}_0'(1)$ it would be sufficient to extend Lemma 2 by adding the implication

(d) If $U(\mathscr{R}(1))$ is recursive then so is $U(\mathscr{R}_0'(1))$,

and prove this by the method of proof of (b). However this will not work since there are rings with identity which cannot be embedded in rings with identity of characteristic zero. (Such an embedding must preserve the indentity.)

Another way to extend the main theorem would be to add

(e) If $U(\mathscr{R}_0(1))$ is recursive then so is $U(\mathscr{R}_0'(1))$,

to Lemma 2. This could be proved by the method of proof of (c), i.e., we describe an effective method which, for each universal sentence σ, produces a universal sentence σ' such that

$$\mathscr{R}_0'(1) \models \sigma \Leftrightarrow \mathscr{R}_0(1) \models \sigma' \,.$$

However I do not know how to construct such a σ'.

We must now prove Theorem 1. To do this we first use a result of McKinsey [3].

A conditional sentence is a sentence of the shape

$$(\forall x_1, \cdots, x_n)[f_1 = 0 \,\&\, \cdots \,\&\, f_r = 0 \rightarrow f = 0]$$

where $f_1, \cdots, f_r, f$ are terms in the variables $x_1, \cdots, x_n$. For each class of rings with identity, $\mathscr{K}(1)$, let $C(\mathscr{K}(1))$ be the set of conditional sentences which hold in $\mathscr{K}(1)$. We will eventually prove the following theorem.

THEOREM 3. *The following sets of* $\mathscr{L}(1)$*-sentences are recursive.*
(i) $C(\mathscr{R}(1))$.
(ii) $C(\mathscr{R}_0(1))$.
(iii) $C(\mathscr{R}_c(1))$ *for any integer* $c \geqq 2$.

Once we have proved Theorem 3 we can obtain Theorem 1 using the following lemma.

LEMMA 4. *Let* $\mathscr{K}(1)$ *be any of* $\mathscr{R}(1)$, $\mathscr{R}_0(1)$, $\mathscr{R}_c(1)$ *for* $c \geqq 2$. *If* $C(\mathscr{K}(1))$ *is recursive then so is* $U(\mathscr{K}(1))$.

Proof. Let σ be any universal $\mathscr{L}(1)$-sentence. σ is logically equivalent to a sentence of the shape

$$(\forall x_1, \cdots, x_n)[D_1 \,\&\, \cdots \,\&\, D_m]$$

where each D_i is a disjunction of literals (i.e., atomic formulas or negations of atomic formulas). For each $1 \leqq i \leqq m$ let σ_i be the sentence

$$(\forall x_1, \cdots, x_n) D_i \; .$$

Clearly we have

$$\mathscr{K}(1) \models \sigma \Leftrightarrow \mathscr{K}(1) \models \sigma_1 \text{ and } \cdots \text{ and } \mathscr{K}(1) \models \sigma_m \; .$$

Using the constants $0, 1$, and the abbreviations $2, 3, \cdots$, we can write each term of σ_i as a "polynomial" in the variables $x_1, \cdots, x_n$ with coefficients from $0, 1, 2, \cdots$. Also, since '$-$' occurs in $\mathscr{L}(1)$, each atomic formula can be written as $f = 0$ for some "polynomial" f. Thus each σ_i can be rephrased in the shape

$$(\forall x_1, \cdots, x_n)[f_1 \neq 0 \vee \cdots \vee f_r \neq 0 \vee g_1 = 0 \vee \cdots \vee g_s = 0]$$

where $f_1, \cdots, g_s$ are "polynomials". We may assume that $r \geqq 1$ and $s \geqq 1$, for if not we introduce a new formula $0 \neq 0$ or $1 = 0$.

For $1 \leqq j \leqq s$ let σ_{ij} be the sentence

$$(\forall x_1, \cdots, x_n)[f_1 = 0 \,\&\, \cdots \,\&\, f_r = 0 \rightarrow g_j = 0] \; .$$

Clearly we can obtain the σ_{ij} from σ in a recursive fashion. Thus the proof is completed by using the following lemma.

LEMMA 5. *With* $\mathscr{K}(1), \sigma_i, \sigma_{ij}$ *as above*

$$\mathscr{K}(1) \models \sigma_i \Leftrightarrow \mathscr{K}(1) \models \sigma_{i1} \text{ or } \cdots \text{ or } \mathscr{K}(1) \models \sigma_{is} .$$

Lemma 5 is proved in McKinsey [3, Th. 1, p. 66]. It should be pointed out that Lemma 5 depends on the fact that $\mathscr{R}(1)$, $\mathscr{R}_0(1)$ and $\mathscr{R}_c(1)$ are closed under (finite) direct products.

The rest of the paper is devoted to proving Theorem 3. To do this we first translate the statement '$\sigma \in C(\mathscr{K}(1))$' (where σ is any conditional sentence and $\mathscr{K}(1)$ is any of $\mathscr{R}(1)$, $\mathscr{R}_0(1)$, $\mathscr{R}_c(1)$) into a statement concerning the membership of polynomial ideals. We will concentrate on one particular sentence,

$$\sigma \equiv (\forall x_1, \cdots, x_n)[f_1 = \mathbf{0} \,\&\, \cdots \,\&\, f_r = \mathbf{0} \rightarrow f = \mathbf{0}] ,$$

although this sentence can be arbitrarily chosen. The technique we use was used by Shepherdson in [4].

Let Z be the ring of integers, Q the field of rational numbers, and Z_c the ring of integer modulo c. With each of $f_1, \cdots, f_r, f$ we associate, in the obvious way, polynomials $F_1, \cdots, F_r, F$ of the polynomial domain $Z[X_1, \cdots, X_n]$. Thus

(i) $X_1, \cdots, X_n$ are associated with $x_1, \cdots, x_n$, respectively,

(ii) $0, 1, 2, \cdots$ are associated with $\mathbf{0}, \mathbf{1}, \mathbf{2}, \cdots$, respectively,

(iii) if G_1, G_2 are associated with g_1, g_2 then $G_1 + G_2, G_1 \cdot G_2, G_1 - G_2$ are associated with $g_1 + g_2, g_1 \times g_2, g_1 - g_2$, respectively. Let $\mathfrak{a}$ be the ideal generated by $F_1, \cdots, F_r$.

Although $F_1, \cdots, F_r, F$ are defined to be polynomials in $Z[X_1, \cdots, X_n]$ they can be construed as polynomials in $Q[X_1, \cdots, X_n]$ or $Z_c[X_1, \cdots, X_n]$. In the same way $\mathfrak{a}$ can be construed as an ideal of $Q[X_1, \cdots, X_n]$ or $Z_c[X_1, \cdots, X_n]$. We will use the phrases 'over Z', 'over Q', 'over Z_c', to indicate the polynomial domain we are considering.

The following theorem completes our translation of the problem.

THEOREM 4. *With* $\sigma, F, \mathfrak{a}$ *defined as above,*

(i) $\sigma \in C(\mathscr{R}(1)) \Leftrightarrow F \in \mathfrak{a}$, *over* Z,

(ii) $\sigma \in C(\mathscr{R}_0(1)) \Leftrightarrow F \in \mathfrak{a}$, *over* Q,

(iii) $\sigma \in C(\mathscr{R}_c(1)) \Leftrightarrow F \in \mathfrak{a}$, *over* Z_c.

Proof. Since the proofs of (i), (ii), and (iii) are similar we will prove only (iii), and sketch the proof of (ii).

Consider first the implication $\Leftarrow$ of (iii). If $F \in \mathfrak{a}$, over Z_c then, for some polynomials $G_1, \cdots, G_r$,

$$F = G_1F_1 + \cdots + G_rF_r ,$$

over Z_c. Let $G_1, \cdots, G_r$ be associated with the terms $g_1, \cdots, g_r$, so that

$$f = (g_1 \times f_1) + \cdots + (g_r \times f_r)$$

holds in $\mathscr{R}_c(1)$. The implication is now clear, for if

$$f_1 = \mathbf{0} \ \& \cdots \& f_r = \mathbf{0}$$

holds in some $R \in \mathscr{R}_c(1)$, then automatically $f = \mathbf{0}$ holds in R.

To prove the implication $\Rightarrow$ of (iii) suppose $\sigma \in C(\mathscr{R}_c(1))$ and consider the ring $R = Z_c[X_1, \cdots, X_n]/\mathfrak{a}$. Clearly $R \in \mathscr{R}_c(1)$, and so σ holds in R. Now consider the elements $x_1 = X_1/\mathfrak{a}, \cdots, x_n = X_n/\mathfrak{a}$ of R, and with these elements form $f_1, \cdots, f_r, f$. The elements of R so formed are, in fact, $F_1/\mathfrak{a}, \cdots, F_r/\mathfrak{a}, F/\mathfrak{a}$ respectively. Since $F_1 \in \mathfrak{a}, \cdots, F_r \in \mathfrak{a}$ we have

$$f_1 = \mathbf{0} \ \& \cdots \& f_r = \mathbf{0}$$

holds in R, and so (since R satisfies σ) we have $f = \mathbf{0}$ holds in R. Thus $F \in \mathfrak{a}$, as required.

Now for the implication $\Leftarrow$ of (ii). If $F \in \mathfrak{a}$, over Q then

$$F = H_1F_1 + \cdots + H_rF_r$$

where $H_1, \cdots, H_r$ are polynomials with rational coefficients. Hence

$$dF = G_1F_1 + \cdots + G_rF_r$$

for some integer d and integral polynomials $G_1, \cdots, G_r$. Thus $\mathbf{d} \times f = \mathbf{0}$ holds in $\mathscr{R}_0(1)$. But each member of $\mathscr{R}_0(1)$ is torsion free, hence $f = \mathbf{0}$ holds in $\mathscr{R}_0(1)$.

For the implication $\Rightarrow$ of (ii) we consider the torsion free ring $R = Q[X_1, \cdots, X_n]/\mathfrak{a}$ and argue as above.

This completes the translation. To complete the proof of Theorem 3 (and hence the main theorem) we must show how to test membership of polynomial ideals.

3. The solution of linear equations over polynomial domains. Let $F_1, \cdots, F_r, F$ be polynomials in $D[X_1, \cdots, X_n]$, where D is any of $Z, Q, Z_c, c \geqq 2$. We must consider the solution of equations of the form

$$F_1\alpha_1 + \cdots + F_r\alpha_r = F \tag{3.1}$$

and

$$F_1\alpha_1 + \cdots + F_r\alpha_r = 0 , \tag{3.2}$$

where $\alpha_1, \cdots, \alpha_r$ are unknown polynomials of $D[X_1, \cdots, X_n]$. As in the previous section we will assume where possible that all polynomials are written as polynomials in $Z[X_1, \cdots, X_n]$, and, where necessary, we will use the phrases 'over Z', 'over Q', 'over Z_c' to indicate how they should be interpreted.

With equations like (3.1) the problem is first to test whether or not a solution $\alpha_1, \cdots, \alpha_r$ exists, and then to find such a solution if one exists. With equations like (3.2) the problem is to find a complete solution, i.e., a finite matrix $[G_{ij}: 1 \leqq i \leqq r, 1 \leqq j \leqq s]$ of polynomials such that $\alpha_1, \cdots, \alpha_r$ satisfies (3.2) if and only if

$$\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_r\end{pmatrix} = [G_{ij}] \begin{pmatrix}\beta_1 \\ \vdots \\ \beta_s\end{pmatrix}$$

for some polynomials $\beta_1, \cdots, \beta_s$. Of course, these solution procedures must be carried out in a recursive fashion.

Let $\mathfrak{a}$ be the ideal over D generated by $F_1, \cdots, F_r$. Notice that as soon as we can test the solvability of (3.1), we can test whether or not $F \in \mathfrak{a}$; hence we have a proof of Theorem 3 for the corresponding class of rings.

For each polynomial G we denote the degree of G by ∂G. Also we let $d = \partial F$, $q = \max(\partial F_1, \cdots, \partial F_r)$.

Methods of solving equations like (3.1), (3.2) have been considered by Hermann in [2]. We state the following results of that paper.

LEMMA 5. *There are recursive functions* $m_1(\cdot, \cdot, \cdot,)$ *and* $m_2(\cdot, \cdot)$ *such that if D is a field then*:

(i) *Equation* (3.1) *has a solution over D if and only if it has a solution $\alpha_1, \cdots, \alpha_r$ such that $\partial\alpha_i \leqq m_1(d, q, n)$ for each i.*

(ii) *Equation* (3.2) *has a complete solution $[G_{ij}]$ over D such that $\partial G_{ij} \leqq m_2(q, n)$ for each i, j.*

The proof of (i) is contained in Satz 2 of [2], and the proof of (ii) is contained in Satz 3 of [2]. Both of these proofs are an intricate use of the division algorithm for polynomial domains.

This lemma gives us an effective method of solving (3.1), (3.2) over Q or Z_p (p prime). We use the method of "comparing coefficients". For instance, consider (3.1) over D. We replace each α by an arbitrary (i.e., with unspecified coefficients) polynomial of $D[X_1, \cdots, X_n]$ of degree $m_1(d, q, n)$. If we now compare coefficients of the various products of $X_1, \cdots, X_n$ we obtain a set of linear equations E with coefficients in D and unknowns ranging over D. This set E is solvable if and only if (3.1) is solvable over D. But E can be solved using the usual methods of linear algebra.

Thus, using the previous lemma and the method of comparing coefficients we get the following lemma.

LEMMA 6. *Let D be any of Q, Z_p, p prime. Equations like* (3.1), (3.2) *over D can be effectively solved.*

COROLLARY. *Theorem* 3 *holds for the classes* $\mathscr{R}_0(1)$, $\mathscr{R}_p(1)$, *p prime.*

To obtain the Theorem 3 for the class $\mathscr{R}_c(1)$, $c \geqq 2$ we must extend this last lemma. This we now do.

THEOREM 7. *Let D be any of Z_c, $c \geqq 2$. Equations like* (3.1), (3.2) *over D can be effectively solved.*

COROLLARY. *Theorem* 3 *holds for the classes* $\mathscr{R}_c(1)$, $c \geqq 2$.

Proof of theorem. We prove the theorem by induction on c. Suppose the result is known for $2, 3, 4, \cdots, c-1$. If c is prime then the result (for c) follows from the previous lemma. (The initial case $c = 2$ also follows from the previous lemma.) If c is not prime we can factorize $c = d_1 d_2$ where $p_1 < c$, $d_2 < c$.

Consider (3.2). First we solve (3.2) over Z_{d_1} to get the complete solution $[G_{ij}\colon 1 \leqq i \leqq r, 1 \leqq j \leqq s]$. (Remember that the G_{ij} are written as polynomials over Z.) For each $1 \leqq j \leqq s$ define G_j by

$$G_j = \frac{G_{1j}F_1 + \cdots + G_{rj}F_r}{d_1}$$

so that G_j is a polynomial over Z. We now solve the equation

$$G_1\beta_1 + \cdots + G_s\beta_s = 0$$

over Z_{d_2} to obtain the complete solution $[H_{ij}\colon 1 \leqq i \leqq s, 1 \leqq j \leqq t]$. It is now an easy matter to check that the product $[G_{ij}][H_{ij}]$ gives a complete solution of (3.2) over Z_c.

We use the same technique to solve (3.1) over Z_c. First we solve (3.1) over Z_{d_1} to get the solution $G_1', \cdots, G_r'$. Let $[G_{ij}]$ be the complete solution of (3.2) over Z_{d_1}. We define

$$G = \frac{F_1G_1' + \cdots + F_rG_r' - F}{d_1}$$

and $G_1, \cdots, G_s$ above. It is now easy to show that (3.1) has a solution over Z_c if and only if

$$G_1\beta_1 + \cdots + G_s\beta_s = G$$

has a solution over Z_{d_2}. Also any solution of this last equation gives a solution of (3.1).

4. The test for membership of ideals over Z. To complete the proof of the main theorem we must show how to test for membership of the ideal $\mathfrak{a} = (F_1, \cdots, F_r)$ over Z. To do this we consider an arbitrary polynomial F, and describe two effective procedures. The first procedure stops if and only if $F \in \mathfrak{a}$, and the second procedure stops if and only if $F \notin \mathfrak{a}$. Thus, using the two procedures simultaneously, we can test whether or not $F \in \mathfrak{a}$. (All the effective procedures we have used so far have been primitive recursive, however the procedure we give for testing membership of $\mathfrak{a}$ over Z is not primitive recursive.)

The first procedure is trivial; we enumerate all r-tuples $(G_1, \cdots, G_r)$ and for each such r-tuple we compute $F_1G_1 + \cdots + F_rG_r$. We stop when $F = F_1G_1 + \cdots + F_rG_r$.

The second procedure is more complicated. We will first describe it, and then explain its workings.

Stage -1. Is $F \in \mathfrak{a}$ over Q?
No-then $F \notin \mathfrak{a}$ over Z. STOP.
Yes-go to stage 0.

Stage 0. Find an integer m such that $mF \in \mathfrak{a}$ over Z.
Go to stage 1.

Stage 1. Is $F \in \mathfrak{a} + (m)$ over Z?
No-then $F \notin \mathfrak{a}$ over Z. STOP.
Yes-go to stage 2.

⋮

Stage s. Is $F \in \mathfrak{a} + (m^s)$ over Z?
No-then $F \in \mathfrak{a}$ over Z. STOP.
Yes-go to stage $s + 1$.

⋮

Lemma 6 shows that stages $-1, 0$ are effective, and Theorem 7 together with the equivalence

$$F \in \mathfrak{a} + (k) \text{ over } Z \Leftrightarrow F \in \mathfrak{a} \text{ over } Z_k$$

(for any integer k) show that the remaining stages are effective. If $F \in \mathfrak{a}$ over Z then $F \in \mathfrak{a}$ over Q and $F \in \mathfrak{a} + (k)$ over Z for all integers k, thus the procedure does not stop. We must show that the procedure does stop whenever $F \notin \mathfrak{a}$ over Z.

Suppose $F \notin \mathfrak{a}$ over Z. If $F \notin \mathfrak{a}$ over Q then the procedure stops at stage -1. If $F \in \mathfrak{a}$ over Q then we compute an integer m such that $mF \in \mathfrak{a}$ over Z, and we go to stage 1. Consider the ascending chain of ideals

$$\mathfrak{a} \subset \mathfrak{a} : (m) \subset \cdots \subset \mathfrak{a} : (m^i) \subset \cdots$$

where

$$\mathfrak{a} : (k) = \{G : kG \in \mathfrak{a} \text{ over } Z\} .$$

We know that $F \in \mathfrak{a} : (m^i)$ over Z for each $i \geqq 1$. Now $Z[X_1, \cdots, X_n]$ is noetherian hence the above ascending chain is finite. Thus there is an integer s such that

$$\mathfrak{a} : (m^s) = \mathfrak{a} : (m^{s+i})$$

for all $i \geqq 0$. With this s it is well known that

$$\mathfrak{a} = \mathfrak{a} : (m^s) \cap \mathfrak{a} + (m^s) .$$

Thus, since $F \in \mathfrak{a} : (m^s)$, we have

$$F \in \mathfrak{a} \Leftrightarrow F \in \mathfrak{a} + (m^s) .$$

But $F \notin \mathfrak{a}$, hence the procedure stops on or before stage s.

This completes the proof of the main theorem.

I would like to thank Professor J. C. Shepherdson who was my supervisor, John Cleave who read the first draft of this paper. I would also like to thank the referee for his comments on a previous draft of this paper.

References

1. Ju. L. Ersov et al., *Elementary theories*, Russian Math. Survey **20** (1965), 35-105.
2. G. Hermann, *Die Frage der Endlich Vielen Schritte der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736-788.
3. J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. S. L. **8** (1943), 61-76.
4. J. C. Shepherdson, *Inverses and zero divisors in matrix rings*, Proc. London Math. Soc. (3) **1** (1951), 71-85.

Received July 19, 1967, and in revised form September 22, 1969. The results in this paper were obtained while the author was a research student at the University of Bristol, and are contained in his Ph. D. thesis. The author would like to thank the Science Research Council for their support.

UNIVERSITY OF ABERDEEN