SYSTEMS OF LINEAR CONGRUENCES, AND LEFT-ASSOCIATIVITY OF MATRICES, WHOSE ELEMENTS ARE INTEGERS FROM AN ALGEBRA

Thesis for the Degree of Ph. D.

MICHIGAN STATE COLLEGE

Alton Thomas Butson

1955

This is to certify that the

thesis entitled

Systems of linear congruences,
and left-associativity of matrices,
whose elements are integers from an algebra.

presented by

Alton Thomas Butson

has been accepted towards fulfillment
of the requirements for

Ph. D. degree in Mathematics

B. M. Stewart
Major professor

Date May 6, 1955

VITA

Alton Thomas Butson

candidate for the degree of

Doctor of Philosophy

Final examination, May 6, 1955, 2:00 P. M., in Room 310, Physics Mathematics Building

Dissertation: Systems of Linear Congruences, and Left-Associativity of Matrices, Whose Elements are Integers from an Algebra

Outline of Studies

Major subject: Mathematics (algebra)
Minor subjects: Mathematics (analysis, statistics, topology)

Biographical Items

Born, February 18, 1926, Lancaster, Pennsylvania

Undergraduate Studies, Franklin & Marshall College, 1946-1950

Graduate Studies, Michigan State College, 1950-1951, continued 1951-1955

Experience: Graduate Assistant, 1950-1953, Graduate Teaching Assistant, 1953-1954, Instructor, 1954-1955, Michigan State College

Member of Phi Beta Kappa, Phi Kappa Phi, Associate member of the Society of the Sigma Xi, American Mathematical Society, Mathematical Association of America

SYSTEMS OF LINEAR CONGRUENCES, AND LEFT-ASSOCIATIVITY OF MATRICES, WHOSE ELEMENTS ARE INTEGERS FROM AN ALGEBRA

By

ALTON THOMAS BUTSON

A THESIS

Submitted to the School of Graduate Studies of Michigan State College of Agriculture and Applied Science in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1955

[redacted]

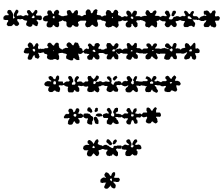
T512

[illegible]

ACKNOWLEDGMENTS

The author wishes to express his sincere thanks to Professor B. M. Stewart, under whose constant supervision and unfailing interest this investigation was undertaken and to whom the results are herewith dedicated. Grateful acknowledgment is also due many others in the Mathematics Department for their kind help and encouragement.

The writer also extends his sincere thanks to his wife whose cooperation and encouragement helped make this thesis possible.



SYSTEMS OF LINEAR CONGRUENCES, AND LEFT-ASSOCIATIVITY OF MATRICES, WHOSE ELEMENTS ARE INTEGERS FROM AN ALGEBRA

By

Alton Thomas Butson

AN ABSTRACT

Submitted to the School of Graduate Studies of Michigan State College of Agriculture and Applied Science in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

Year 1955

Approved B. M. Stewart

ABSTRACT

A major part of this thesis is devoted to the problem of solving a system of linear equations or a system of linear congruences whose elements are integers from an algebra. By means of regular representations each of these systems is replaced by an equivalent system whose elements are in a principal ideal ring. A system of equations is replaced by a system of linear equations of a classical type whose solution is known. A system of congruences is replaced by a system of linear congruences whose elements are actually matrices over a principal ideal ring. This latter system is solved by a procedure analogous to that employed in the classical case. Necessary and sufficient conditions are obtained for the existence of a solution whose elements are integers of the algebra. These conditions are in terms of elements of the principal ideal ring. This problem is completely solved - the main tool used being the regular representations.

Each matrix A whose elements are integers from an algebra has as a reduced regular representation a matrix s(A) whose elements are in a principal ideal ring. The remainder of the thesis is concerned with the possibility that a necessary and sufficient condition that A and B be

left-associates is that s(A) and s(B) have the same Hermite form. The condition is a necessary one and will be shown sufficient when A and B are not divisors of 0. A problem for further research is whether the condition is sufficient when A and B are divisors of 0.

TABLE OF CONTENTS

SYSTEMS OF LINEAR CONGRUENCES, AND LEFT-ASSOCIATIVITY OF MATRICES, WHOSE ELEMENTS ARE INTEGERS FROM AN ALGEBRA

1. Introduction. The problem of solving a system of linear equations or a system of linear congruences whose elements are in a principal ideal ring has been solved very neatly and completely a long time ago by H. J. S. Smith [8,9]. A major part of this thesis is devoted to extending these results to systems whose elements are integers from an algebra. The modus operandi is to replace by means of the regular representations the system whose elements are integers from an algebra by an equivalent system whose elements are in a principal ideal ring. A system of equations is replaced by a system of linear equations of the type solved by Smith. A system of congruences is replaced by a system of linear congruences whose elements including the moduli are actually matrices over a principal ideal ring. This latter system is solved by a procedure analogous to that used by Smith in solving an ordinary system of congruences. Necessary and sufficient conditions are obtained for the existence of a solution whose elements are integers from the algebra. These conditions are in terms of the invariant factors of the coefficient matrix and the augmented matrix of the corresponding system in the

principal ideal ring. This problem of solving a system whose elements are integers from an algebra is completely resolved - the main tool used being the regular representations.

B. M. Stewart [12] determined a necessary and sufficient condition that two matrices A and B whose elements are integers of an algebraic field be left-associates, i.e., that there exists a unimodular matrix P whose elements are also integers of the algebraic field such that $PA=B$. The condition is that A^E and B^E have the same Hermite form, where A^E and B^E are the matrices in the rational domain obtained by replacing each element of A and B, respectively, by its second regular representation. The remainder of this thesis is concerned with an attempt to extend this result to matrices A^* and B^* whose elements are integers from an algebra. A reduced regular representation of A^* is the matrix $s(A^*)$ whose elements are in a principal ideal ring; consequently, the Hermite form of $s(A^*)$ is well-defined. The condition that $s(A^*)$ and $s(B^*)$ have the same Hermite form is a necessary one for A^* and B^* to be left-associates, and it will be shown sufficient when A^* and B^* are not divisors of 0. The method used will suggest how a future investigation might proceed either to obtain a complete proof or to construct a negative example.

2. Canonical Forms. In this section the Hermite and the Smith canonical forms for matrices with elements in a principal ideal ring will be described. The following brief summary will recall the position that the principal ideal ring occupies with respect to other related algebraic varieties.

A ring is a mathematical system composed of more than one element, an equals relation, and two operations, + and ×, under which the set of elements is closed. With respect to the operation +, the elements form an Abelian group with 0 as an identity. The operation × is associative, and distributive with respect to the operation +. The operation × may or may not have an identity element 1, may or may not provide inverses, may or may not be commutative, and may or may not possess divisors of 0.

A domain of integrity is a commutative ring without divisors of 0. A principal ideal ring is a domain of integrity which has an identity element 1, and in which every two elements not both 0 have a greatest common divisor representable linearly in terms of the elements; further, there is a chain condition that if in the sequence

$$a_1, a_2, a_3, \ldots$$

every number is a proper divisor of the preceding, there

are but a finite number of a's in the sequence. A field is a principal ideal ring in which the elements other than 0 form an Abelian group with respect to the operation $\times$.

Familiar examples of a field and a principal ideal ring are the rational field $\mathfrak{Ra}$ and the rational integral domain $[\mathfrak{Ra}]$ respectively.

Let $\mathfrak{P}$ be a principal ideal ring with elements a,b,...; and denote by $\mathfrak{M}(n,p;\mathfrak{P})$ the set of all n-by-p matrices

$$A=(a_{rs}),\ B=(b_{rs}),\ldots \quad (r=1,2,\ldots,n;\ s=1,2,\ldots,p)$$

with elements in $\mathfrak{P}$. A matrix P of $\mathfrak{M}(n,n;\mathfrak{P})$ is called unimodular if there exists a matrix Q in $\mathfrak{M}(n,n;\mathfrak{P})$ such that $QP=I_n$ ($I_n=(\delta_{rs})$, where $\delta_{rs}=1$ if $r=s$, and $\delta_{rs}=0$ if $r\neq s$). In terms of determinants this implies that $\det(Q)\det(P)=1$, hence $\det(P)$ is a unit of $\mathfrak{P}$. Therefore P^I (the inverse of P) is in $\mathfrak{M}(n,n;\mathfrak{P})$; since $P^IP=PP^I=I_n$ it follows that $Q=P^I$ and that Q is also unimodular.

If there exists a unimodular matrix P such that $PA=B$, then B is said to be a left-associate of A. This relation is an equivalence relation; hence A and B may be said to be left-associated without ambiguity of meaning.

The following lemma was first stated by C. Hermite for non-singular matrices with rational integral elements, a fact suggesting the term "Hermite form". However,

MacDuffee provided an additional construction in the case of singular matrices which gives a unique form in all cases [4].

Lemma 2.1. A matrix A in $\mathfrak{M}(n,p;\mathfrak{P})$ is the left-associate of a matrix H having 0's above the main diagonal, each diagonal element lying in a prescribed system of non-associates, and each element below the main diagonal lying in a prescribed residue system modulo the diagonal element above it (where $a \equiv b \bmod 0$ implies $a = b$). If a diagonal element be 0, all the elements of its row can be made 0. This form H is unique.

The Hermite form H of a matrix A is determined by two sets of transformations.

First one operates on A column by column from right to left to determine the diagonal elements of H. This is essentially a process of finding unimodular matrices which will transform a given column vector with elements $a_1,\ldots,a_j$ into the column vector $0,\ldots 0,h$ where the ideal $(a_1,\ldots,a_j)$ is the principal ideal (h). This step can be performed theoretically in any principal ideal ring, and can be accomplished by elementary transformations in a Euclidean ring [6,Th.22.3] -- for example, in $[\mathfrak{Ra}]$.

Thus if A is in $\mathfrak{M}(n,n;\mathfrak{P})$ (this is no restriction since any rectangular matrix can be squared by adding

either rows or columns of 0's) and has the n-th column not all 0, A may be transformed so that column n consists entirely of 0's except for $h_{nn} \neq 0$. In the new matrix exclude the row n from consideration and transform so that column n-1 consists entirely of 0's except possibly for $h_{n-1,n-1}$.

But if column n of A is all 0, take $h_{nn}=0$; then in working with column n-1 include the row n in the consideration so that the transformed matrix may have $h_{n,n-1}=0$. By continued inclusion of the row n in the subsequent finding of all diagonal elements all the elements of row n of H may be made 0.

The column-by-column application of these steps gives the diagonal elements of H, gives 0's above the main diagonal, and rows of 0's whenever the corresponding diagonal element is 0.

Secondly, one operates column-by-column from right to left to reduce the elements below the main diagonal modulo the diagonal element above. This may be done by elementary transformations that do not affect the properties attained by the first set of operations. Note that in case a diagonal element is 0, the elements below must be left just as they happen to appear whenever the second set of operations has been completed on the other columns of the matrix.

For example, let A have elements in $[\mathfrak{R}a]$, where the residue system may be prescribed to be 0 and the set of positive integers less than the modulus. A succession of transformations from A to H is shown together with the unimodular matrix P such that PA=H.

$$A=\begin{pmatrix}6&2&10\\3&9&45\\1&3&15\end{pmatrix}\to\begin{pmatrix}6&2&10\\3&9&45\\-5&1&5\end{pmatrix}\to\begin{pmatrix}16&0&0\\48&0&0\\-5&1&5\end{pmatrix}\to\begin{pmatrix}16&0&0\\0&0&0\\11&1&5\end{pmatrix}=H,\quad P=\begin{pmatrix}3&0&-2\\0&1&-3\\2&0&-1\end{pmatrix}.$$

To prove the uniqueness of the Hermite form, assume that H can be the left-associate of another Hermite form H', i.e., that there exists a unimodular G such that GH=H'. The properties of the Hermite form are restrictive enough to require that H=H', whereas G is revealed as the most general unimodular matrix leaving H unaltered when used as a left factor. The exact structure of G is as follows: Let $h_{ii}\neq 0$ for $i=s_1,s_2,\ldots,s_r$; let $h_{ii}=0$ for $i=t_1,t_2,\ldots,t_{n-r}$. Then the matrix G has as its columns $s_1,s_2,..,s_r$ the unit vectors $(\delta_{js_1}),(\delta_{js_2}),\ldots,(\delta_{js_r})$; while the columns $t_1,t_2,\ldots,t_{n-r}$ are arbitrary, except that the matrix G_{11} formed by deleting rows and columns $s_1,s_2,\ldots,s_r$ from G must be unimodular. Here r is the rank of the matrix H. In particular, if H is non-singular, then $G=I_n$.

The other canonical form due to H. J. S. Smith [6,Th.26.2] is described in the following lemma.

Lemma 2.2. For any matrix A in $\mathfrak{M}(n,p;\mathfrak{P})$ there exist unimodular matrices U in $\mathfrak{M}(n,n;\mathfrak{P})$ and V in $\mathfrak{M}(p,p;\mathfrak{P})$ such that $UAV=E$ has zero elements everywhere except in the main diagonal where there may appear non-zero elements $e_1,e_2,\ldots,e_r$, (which are called invariant factors and which are uniquely determined up to associates in $\mathfrak{P}$), having the property that e_i divides e_{i+1} and either $r\leqq p\leqq n$ or $r\leqq n<p$.

If A is of rank r, the rows and columns can be shifted by elementary transformations so that the minor determinant of order r in the upper left corner is $\neq 0$. Then as in the proof of Lemma 2.1, the element in the (1,1)-position can be made $\neq 0$ and a g.c.d. of the elements of the first column. The elements of the first column below the first row can then be made 0's by elementary transformations on the rows. If the element which now stands in the (1,1)-position divides every other element of the first row, these other elements can all be made 0's by elementary transformations on the columns so as not to disturb the first column of 0's. If they are not all divisible by this element a_{11}, then a_{11} can be replaced by the g.c.d. of the elements of the first row, and this g.c.d.

will contain fewer prime factors than a_{11}. The process is now repeated until an element in the (1,1)-position is obtained which divides every other element of the first row and every other element of the first column. Since every number of $\mathfrak{P}$ is factorable into a finite number of primes, this stage is reached in a finite number of steps.

By working with the last n-1 rows and last p-1 columns, then with the last n-2 rows and last p-2 columns etc., A can be reduced to the form

$$\begin{pmatrix} D & 0 \\ 0 & M \end{pmatrix}, \text{ where } D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_r \end{pmatrix}, \text{ and } d_1 \neq 0.$$

Now $M=0$, for if one element of M were not 0, it could be shifted into the (r+1,r+1)-position, and A would have a non-vanishing minor determinant of order r+1.

By adding column 2, column 3,..., column r to column 1, D is made to assume the form

$$\begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ d_2 & d_2 & 0 & \dots & 0 \\ d_3 & 0 & d_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ d_r & 0 & 0 & \dots & d_r \end{pmatrix}.$$

As in

K whi

of d_1

homog

eleme

the d

where

divid

elem

A =

As in the proof of Lemma 2.1, there is a unimodular matrix K which, used as a left factor, replaces d_1 by the g.c.d. of $d_1,d_2,\ldots,d_r$. The new matrix KD has every element a homogeneous linear combination of $d_1,d_2,\ldots,d_r$, so each element of KD is divisible by the new d_1. Again reduce to the diagonal form

$$\begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r \end{pmatrix}$$

where now d_1 divides $d_2,d_3,\ldots,d_r$. Continue until d_i divides d_{i+1}, $i = 1,2,\ldots,r-1$.

We illustrate this procedure with a matrix A with elements in $[\mathcal{R}a]$, and give the unimodular matrices U and V.

$$A = \begin{pmatrix} 2 & 4 & 13 \\ 0 & 6 & 3 \\ 0 & 0 & 6 \\ 0 & 0 & 2 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & -2 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = E$$

$$U = \begin{pmatrix} 0 & 1 & 0 & -1 & -1 \\ 1 & -1 & 0 & -5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -3 & 0 \\ 0 & -2 & 0 & 3 & 3 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & -2 \end{pmatrix}.$$

3. Linear Equations in $\mathfrak{P}$. Using matric notation a new exposition of Smith's material is given in this and the immediately succeeding section. The results are easier to state and the proofs are greatly simplified through the use of Lemma 2.2.

The coefficients, constants, and moduli in the equations and congruences of sections 3, 4, and 5 are assumed to be in a specified principal ideal ring $\mathfrak{P}$, such as the rational domain. For the system of p linear equations in n unknowns represented by

$$\sum_{i=1}^{n} x_i a_{ij} = k_j, \qquad j = 1,2,\ldots,p;$$

we will use the matric notation

$$XA = K, \tag{3.1}$$

where X is 1-by-n, A is in $\mathfrak{M}(n,p;\mathfrak{P})$, and K is in $\mathfrak{M}(1,p;\mathfrak{P})$. We wish to determine when (3.1) has a solution X in $\mathfrak{M}(1,n;\mathfrak{P})$, to find how many solutions there may be, and to give a method for actually obtaining the solution.

By Lemma 2.2 there exist unimodular matrices U in $\mathfrak{M}(n,n;\mathfrak{P})$ and V in $\mathfrak{M}(p,p;\mathfrak{P})$ such that $UAV = E$ is the Smith normal form with invariant factors $e_1, e_2, \ldots, e_r$, where e_i divides e_{i+1} and either $r \leqq p \leqq n$ or $r \leqq n < p$.

Hence the system (3.1) may be replaced by the equivalent system $(XU^I)(UAV)=KV$, so that by setting $Y=XU^I$ and $C=KV$ we arrive at

$$YE=C. \tag{3.2}$$

The system (3.2) is so simple that we can immediately conclude that necessary and sufficient conditions for its solvability are as follows:

$$\begin{aligned} &e_i \text{ must divide } c_i, && i=1,2,\ldots,r; \\ &c_i=0, && i>r. \end{aligned} \tag{3.3}$$

If we define $A'=\begin{pmatrix}A\\K\end{pmatrix}$ as the augmented matrix of (3.1), then using the conventional block notation we have

$$\begin{pmatrix}U & 0\\ 0 & 1\end{pmatrix} A'V=\begin{pmatrix}E\\C\end{pmatrix};$$

so that a further transformation by unimodular matrices U' in $\mathfrak{M}(n+1,n+1;\mathfrak{P})$ and V' in $\mathfrak{M}(p,p;\mathfrak{P})$ will take A' into its Smith normal form, say $U'\begin{pmatrix}E\\C\end{pmatrix}V'=E'$, which is in $\mathfrak{M}(n+1,p;\mathfrak{P})$ with the invariant factors $e'_1,e'_2,\ldots$. If we use the block notation and write

$$\begin{pmatrix}E\\C\end{pmatrix}=\begin{pmatrix}E_1 & 0\\ 0 & 0\\ C_1 & C_2\end{pmatrix},$$

it is

satis

Conve

and

in t

Perf

$$\text{where } E_1 = \begin{pmatrix} e_1 & 0 & \dots & 0 \\ 0 & e_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_r \end{pmatrix},$$

$$C_1 = (c_1, c_2, \dots, c_r), \text{ and } C_2 = (c_{r+1}, c_{r+2}, \dots, c_p),$$

it is quite obvious that if the conditions (3.3) are satisfied the Smith normal form of A' is

$$E' = \begin{pmatrix} E_1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Conversely, if we assume that the Smith normal form of A' is

$$E' = \begin{pmatrix} E_1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

and let X and Y be the inverses of U' and V' respectively, in block notation we have

$$\begin{pmatrix} E_1 & 0 \\ 0 & 0 \\ C_1 & C_2 \end{pmatrix} = \begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ X_{31} & X_{32} & X_{33} \end{pmatrix} \begin{pmatrix} E_1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix}.$$

Performing the block multiplication on the right we obtain

$E_1 = X_{11}E_1Y_{11}$, $C_1 = X_{31}E_1Y_{11}$, $C_2 = X_{31}E_1Y_{12}$, and
$X_{11}E_1Y_{12} = X_{21}E_1Y_{11} = X_{21}E_1Y_{12} = 0$.

From the first of these equations and a well known theorem concerning determinants we have

$$\det(E_1) = \det(X_{11})\det(E_1)\det(Y_{11});$$

which implies, since E_1 is non-singular, that $\det(X_{11})\det(Y_{11}) = 1$. Now X_{11} and Y_{11} are in $\mathfrak{M}(r,r;\mathfrak{P})$, so $\det(X_{11})$ and $\det(Y_{11})$ are in $\mathfrak{P}$. Hence $\det(X_{11})$ and $\det(Y_{11})$ are units of $\mathfrak{P}$ and X_{11} and Y_{11} are unimodular, so that X_{11}^{I} and Y_{11}^{I} are in $\mathfrak{M}(r,r;\mathfrak{P})$. From the first of the above equations we obtain $E_1Y_{11} = X_{11}^{I}E_1$, which we substitute into the second to yield

$$C_1 = X_{31}X_{11}^{I}E_1.$$

Since X_{11} is unimodular and E_1 is non-singular, it follows from $X_{11}E_1Y_{12} = 0$ that Y_{12} must be 0; and, consequently that

$$C_2 = 0.$$

Hence the conditions (3.3) are satisfied.

If we now agree that <u>all</u> the elements in the main diagonal of E and E' are to be denoted by e_i and e'_i, respectively, and observe when $p \leqq n$ that E and E' have p elements in the main diagonal, and when $n < p$ that E has n,

and E' has $n+1$ elements in the main diagonal, then depending on the relative size of n and p, the conditions (3.3) may be replaced by the equivalent conditions:

(3.4) $p \leqq n$: $e_i = e'_i$, $i = 1,2,\ldots,p$;

(3.4') $n < p$: $e_i = e'_i$, $i = 1,2,\ldots,n$; and

$e'_{n+1} = 0$.

Supposing that these necessary and sufficient conditions are satisfied, we return to (3.2) and see that the first r of the y's are determined uniquely by $y_i = c_i/e_i$, while the remaining n-r of the y's are arbitrary. The complete solution of (3.1) is then given by $X = YU$ and involves n-r parameters; but it is not necessarily the unique expression for the general solution, since the matrices U and V are not unique.

4.

congrue

$$\sum_{i=1}^{n}$$

we will

(4.1)

A matrix

only if

(4.2)

Two solu

if and o

system

(4.1')

of p line

4. Linear Congruences in $\mathfrak{P}$. For the system of linear congruences represented by

$$\sum_{i=1}^{n} x_i b_{ij} \equiv g_j \bmod (m_j), \qquad j=1,2,\ldots,p;$$

we will use the matric notation

$$(4.1) \qquad XB \equiv G \bmod M', \text{ where } M' = \begin{pmatrix} m_1 & 0 & \ldots & 0 \\ 0 & m_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & m_p \end{pmatrix}.$$

A matrix X in $\mathfrak{M}(1,n;\mathfrak{P})$ will be a solution of (4.1) if and only if there exists a matrix T in $\mathfrak{M}(1,p;\mathfrak{P})$ such that

$$(4.2) \qquad XB + TM' = G.$$

Two solutions X and X' of (4.1) will be called congruent if and only if $X \equiv X' \bmod m_j I_n$, for $j=1,2,\ldots,p$. Another system

$$(4.1') \qquad ZA \equiv K \bmod N', \text{ where } N' = \begin{pmatrix} n_1 & 0 & \ldots & 0 \\ 0 & n_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & n_p \end{pmatrix},$$

of p linear congruences in n unknowns will be called

equivalent to the system (4.1) if and only if there exists a unimodular matrix Q in $\mathfrak{M}(n,n;\mathfrak{P})$ such that: if X_1 is a solution of (4.1), then $Z_1=X_1Q$ is a solution of (4.1'); if Z_2 is a solution of (4.1'), then $X_2=Z_2Q^I$ is a solution of (4.1); if X_1 and X_2 are congruent solutions of (4.1), then Z_1 and Z_2 are congruent solutions of (4.1'); and if Z_1 and Z_2 are congruent solutions of (4.1'), then X_1 and X_2 are congruent solutions of (4.1).

If $m=[m_1,m_2,\ldots,m_p]$ is the least common multiple of the m_j, and R is a diagonal matrix whose elements r_j are such that $m=m_jr_j$, multiplication of the system (4.1) on the right by R gives a system

(4.3) $\qquad XA\equiv K \bmod M_p,$

where $A=BR$, $K=GR$, and $M_p=mI_p$. This system is equivalent to (4.1) since in the above definition we can choose $Q=I_n$; and if $X\equiv X' \bmod m_jI_n$, $j=1,2,\ldots,p$, that $X\equiv X' \bmod M_n$, and conversely, follows from the properties of the least common multiple.

We shall now determine necessary and sufficient conditions for the solvability of (4.3), the number of incongruent solutions, and a method of obtaining the solution.

The system (4.3) of congruences has a solution X

in $\mathfrak{M}(1,n;\mathfrak{P})$ if and only if there exists a matrix T in $\mathfrak{M}(1,p;\mathfrak{P})$ such that

$$(4.4) \qquad XA+TM_p=K,$$

which is an equivalent system of $p_1=p$ equations in $n_1=n+p$ unknowns. Since $p_1<n_1$, we apply the test (3.4) which requires us to compute the invariant factors of $\begin{pmatrix}A\\M_p\end{pmatrix}$ and $\begin{pmatrix}A'\\M_p\end{pmatrix}$. Fortunately this task is easy because of the form of M_p. Following an argument which is more direct than that used by Smith we write

$$\begin{pmatrix}U & 0\\ 0 & V^I\end{pmatrix}\begin{pmatrix}A\\M_p\end{pmatrix}V=\begin{pmatrix}E\\M_p\end{pmatrix}.$$

Because e_i divides e_{i+1}, we see that no further rearrangement of columns is necessary and that the i-th invariant factor of $\begin{pmatrix}A\\M_p\end{pmatrix}$ is either (e_i,m) when $i\leqq p\leqq n$, or is m when $n<i\leqq p$.

Similarly, for $\begin{pmatrix}A'\\M_p\end{pmatrix}$ the i-th invariant factor is (e'_i,m) when $i\leqq p\leqq n$; but when $n<p$, the (n+1)-st invariant factor is (e'_{n+1},m); and when $n+1<i\leqq p$, the i-th invariant factor is m.

Hence the test (3.4) shows that the necessary and sufficient conditions for the solution of (4.3) (and, moreover, of (4.1)) are as follows:

(4.5)

(4.5')

We note t

$a'_{n+1} \equiv 0$

As

equivale

$y = X^{-1}$, c

matrix),

(4.6)

which ca

(4.7)

If

matrix T

$X_1 U^{-1} E V^{-1} +$

multiply

see that

is a sol

show the

two comp

W in

right by

(4.5) $p \leq n$: $(e_i, m) = (e'_i, m)$, $i = 1, 2, \ldots, p$;

(4.5') $n < p$: $(e_i, m) = (e'_i, m)$, $i = 1, 2, \ldots, n$; and
$m = (e'_{n+1}, m)$.

We note that the final condition in (4.5') may be written $e'_{n+1} \equiv 0 \bmod m$, in close analogy with (3.4').

As in section 3, we replace the system (4.4) by the equivalent system $(XU^I)UAV + TM_pV = KV$, so that by setting $Y = XU^I$, $C = KV$, and $T' = TV$, ($M_pV = VM_p$ since M_p is a scalar matrix), we obtain

(4.6) $$YE + T'M_p = C,$$

which can be written as the following system of congruences,

(4.7) $$YE \equiv C \bmod M_p.$$

If X_1 is a solution of (4.3), then there exists a matrix T_1 such that $X_1A + T_1M_p = K$. Since $A = U^IEV^I$ we have $X_1U^IEV^I + T_1M_p = K$; and letting $Y_1 = X_1U^I$, $T'_1 = T_1V$, and multiplying on the right by V we obtain $Y_1E + T'_1M_p = C$ and see that Y_1 is a solution of (4.7). If we assume that Y_1 is a solution of (4.7) we can reverse the above steps to show that $X_1 = Y_1U$ is a solution of (4.3). If X_1 and X_2 are two congruent solutions of (4.3) there must exist a matrix W in $\mathfrak{M}(1,n;\mathfrak{P})$ such that $X_1 - X_2 = WM_n$. Multiplying on the right by U^I we have $X_1U^I - X_2U^I = WU^IM_n$. This last equation

shows that $Y_1 = X_1 U^I$ and $Y_2 = X_2 U^I$ are congruent solutions of (4.7). If we let Y_1 and Y_2 be congruent solutions of (4.7) and reverse the preceding steps we easily obtain that X_1 and X_2 are congruent solutions of (4.3). This establishes the equivalence of the systems (4.3) and (4.7).

From (4.7) we see that the first r of the y's are determined by congruences of the form $y_i e_i \equiv c_i \bmod m$. From properties of $\mathfrak{P}$ we know there are as many solutions y_i which are incongruent mod m as there are residue classes of $\mathfrak{P}$, mod (e_i, m). The remaining y's are arbitrary, so for each of these there are as many solutions incongruent mod m as there are residue classes of $\mathfrak{P}$, mod m. The general solution of (4.3) and of (4.1) is given explicitly by $X \equiv YU \bmod M_n$.

In particular, when $\mathfrak{P}$ is the domain of rational integers, the above considerations show that there are exactly

$$N = (e_1, m)(e_2, m)\ldots(e_r, m)m^{n-r}$$

distinct solutions of (4.1).

For an example we take $\mathfrak{P}$ to be the rational integers and consider the system

$$3x_1 + x_2 = 5,$$
$$5x_1 + 3x_2 = 1.$$

Using the notation of the preceding sections, we have

$$UAV = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = E,$$

$$KV = (5\ 1) \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix} = (5\ 14) = C,$$

$$U' \begin{pmatrix} E \\ C \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -5 & -3 & 1 \\ 10 & 7 & -2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 5 & 14 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} = E'.$$

Since $4 = e_2 \neq e'_2 = 2$, it follows from (3.4) that the system has no solution in rational integers.

Considering the same system mod M_2, we see from (4.5) that we must have $(1,m) = (1,m)$ and $(4,m) = (2,m)$. If $m \equiv 0 \bmod 4$, there are no solutions; if $m \equiv 1$ or $3 \bmod 4$, there will be $N = 1$ solution; and if $m \equiv 2 \bmod 4$, there will be $N = 2$ solutions.

Thus if $m = 10$, we solve $y_1 \equiv 5$, $4y_2 \equiv 14$, for $y_1 \equiv 5$, $y_2 \equiv 1$; and $y_1 \equiv 5$, $y_2 \equiv 6$. Then from $X = YU$, we compute $x_1 \equiv 1$, $x_2 \equiv 2$; and $x_1 \equiv 6$, $x_2 \equiv 7$, respectively.

5. A Mixed System in $\mathfrak{P}$. We are now going to exhibit a procedure for solving a mixed system of equations and congruences in $\mathfrak{P}$. This was not considered by Smith but we shall have occasion to refer to it in the sequel, and it is included at this point since the system is in a principal ideal ring.

In the matric notation of the preceding sections

(5.1) $XA_1 = K_1$ and

(5.1') $XA_2 \equiv K_2 \bmod M_{p_2}$,

where X is 1-by-n, A_1 is in $\mathfrak{M}(n,p_1;\mathfrak{P})$, A_2 is in $\mathfrak{M}(n,p_2;\mathfrak{P})$, K_1 is in $\mathfrak{M}(1,p_1;\mathfrak{P})$, K_2 is in $\mathfrak{M}(1,p_2;\mathfrak{P})$, and $M_{p_2} = mI_{p_2}$, represent, respectively, a system of p_1 equations in n unknowns of the type (3.1) and a system of p_2 congruences in n unknowns of the type (4.3). Since we are concerned to find all solutions common to both systems we regard the former as a system of congruences each mod 0, and letting $p = p_1 + p_2$, $A = (A_1\ A_2)$, $K = (K_1\ K_2)$, and $\overline{M} = (0\ M_{p_2})$ we can write

(5.2) $XA \equiv K \bmod \overline{M}$.

This system will have a solution if and only if there exists a matrix T in $\mathfrak{M}(1,p_2;\mathfrak{P})$ satisfying

(5.3) $XA + T\overline{M} = K$,

which is a system of p equations in $n+p_2$ unknowns. We apply the test (3.4) to the coefficient matrix $\left(\frac{A}{M}\right)$ and the augmented matrix $\left(\frac{A'}{M}\right)$ to determine whether or not (5.3) has a solution. Due to the form of $\overline{M}$ the invariant factors are not as simply expressed as in section 4.

Assuming the conditions of (3.4) are met we proceed to determine the common solutions of (5.1) and (5.1'). Letting $U_1A_1V_1=E_1$ with rank r_1, $Y=XU_1^I$, and $C_1=K_1V_1$, and proceeding as in section 3 we find that $y_1,y_2,\ldots,y_{r_1}$ are uniquely determined, $y_{r_1+1},y_{r_1+2},\ldots,y_n$ are arbitrary, and $X=YU_1$ is the general solution of (5.1). We set $Y'=(y_1,y_2,\ldots,y_{r_1})$, $Y''=(y_{r_1+1},y_{r_1+2},\ldots,y_n)$, and $U_1=\begin{pmatrix}U_1'\\U_1''\end{pmatrix}$, where U_1' has r_1 rows; and since X is to be also a solution of (5.1') we now consider

$$YU_1A_2\equiv K_2 \bmod M_{p_2}.$$

Since $y_1,y_2,\ldots,y_{r_1}$ are uniquely determined, we let $A_2''=U_1''A_2$ and $K_2''=K_2-Y'U_1'A_2$ and write

$$Y''A_2''\equiv K_2'' \bmod M_{p_2}, \tag{5.4}$$

which is a system of p_2 congruences in $n-r_1$ unknowns of the type (4.3). Letting $U_2A_2''V_2=E_2$ with rank r_2 and invariant factors e_i, $Z=Y''U_2^I$, and $C_2=K_2''V_2$ we proceed as in section 4 and find that $z_1,z_2,\ldots,z_{r_2}$ are determined by congruences

of the type $z_i e_i \equiv c_i \bmod m$, $z_{r_2+1}, z_{r_2+2}, \ldots, z_{n-r_1}$ are arbitrary and $Y'' \equiv ZU_2 \bmod M_{p_2}$ is the general solution of (5.4). Then the general solution of (5.1) and (5.1') is given by $X = (Y'U_1' + Y''U_1'')$ where $Y'' \equiv ZU_2 \bmod M_{p_2}$.

Since (5.4) is a system of congruences of the type (4.3), the discussion in section 4 concerning the number of incongruent solutions of (4.3) can be applied directly to (5.4). In particular, if $\mathfrak{P}$ is $[\mathfrak{Ra}]$, we note that the number of incongruent solutions of (5.4) is

$$N = (e_1, m)(e_2, m)\ldots(e_{r_2}, m)\, m^{n-r_1-r_2}.$$

We now agree that two common solutions $\bar{X}$ and X of (5.1) and (5.1') are to be considered congruent when

(5.5) $\qquad \bar{X} \equiv X \bmod M_n.$

Let $X = Y'U_1' + Y''U_1''$ and $\bar{X} = Y'U_1' + \bar{Y}''U_1''$ be two congruent solutions of (5.1) and (5.1'). Then there must exist a T in $\mathfrak{M}(1,n;\mathfrak{P})$ so that

(5.6) $\qquad TM_n = \bar{X} - X = \bar{Y}''U_1'' - Y''U_1''.$

Let $U_1^{\,I} = (L_1\ L_2)$ so that $U_1''L_2 = I_{n-r_1}$. Then multiplication of (5.6) on the right by L_2 gives

$$\bar{Y}'' - Y'' = TM_nL_2 = TL_2M_{n-r_1} = WM_{n-r_1},$$

where $W=TL_2$ is in $\mathfrak{M}(1,n-r_1;\mathfrak{P})$, which implies that $\overline{Y}''$ and Y'' are congruent solutions of (5.4). Conversely, if we assume that $\overline{Y}''$ and Y'' are congruent solutions of (5.4), then there exists a matrix W in $\mathfrak{M}(1,n-r_1,\mathfrak{P})$ so that

$$(5.7) \qquad \overline{Y}'' - Y'' = WM_{n-r_1}.$$

Multiplication of (5.7) on the right by U'' gives

$$\overline{Y}''U'' - Y''U'' = WM_{n-r_1}U'' = WU''M_n = TM_n$$

where $T=WU''$ is in $\mathfrak{M}(1,n;\mathfrak{P})$. Then

$$TM_n = \overline{Y}''U'' - Y''U'' = (Y'U_1' + \overline{Y}''U'') - (Y'U_1' + Y''U'') = \overline{X} - X,$$

and $\overline{X}$ and X are congruent solutions of (5.1) and (5.1'). Hence the number of incongruent solutions of (5.1) and (5.1') is the same as the number of incongruent solutions of (5.4).

As an example, we consider (5.2) when

$$X=(x_1\ x_2\ x_3),\ A=\begin{pmatrix}2 & 26 & 4\\ 0 & 6 & 6\\ 0 & 12 & 0\end{pmatrix},$$

$$K=(4\ 8\ 8),\ \text{and}\ \overline{M}=\begin{pmatrix}0 & 4 & 0\\ 0 & 0 & 4\end{pmatrix}.$$

Since the invariant factors of $\begin{pmatrix}A\\ \overline{M}\end{pmatrix}$ are $e_1=2$, $e_2=2$, $e_3=4$

and of $\left(\frac{A'}{M}\right)$ are $e'_1=2$, $e'_2=2$, $e'_3=4$ we are assured that solutions exist. Since (5.1) is $2x_1=4$ we have immediately $(2\ x_2\ x_3)$ is the general solution. For this to be also a solution of (5.1') requires

$$(2\ x_2\ x_3)\begin{pmatrix}26 & 4\\ 6 & 6\\ 12 & 0\end{pmatrix} \equiv (8\ 8) \bmod \begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix},$$

which gives $6x_2+12x_3\equiv 0 \bmod 4$, $6x_2\equiv 0 \bmod 4$. Hence we have $x_2\equiv 0 \bmod 2$ and x_3 is arbitrary, and the general common solution is given by

$$x_1=2,$$
$$x_2\equiv 0 \bmod 2,$$
$$x_3 \text{ arbitrary.}$$

We remark that there are $N=2\cdot 4=8$ incongruent solutions.

6. Integral Elements and Regular Representations. Our immediate goal is the extension of Smith's results to a mathematical system more general than a principal ideal ring. In this section this system is defined, and, following the terminology of MacDuffee [5], it is called a "set of integral elements". Also, the first and second regular representations of an integral element are described; and an intertwining relationship between the two which will be extremely useful is observed.

An algebra $\mathfrak{A}$ over a field $\mathfrak{F}$ is a mathematical system composed of more than one element, an equals relation, and three operations, $+$, $\times$, and $\circ$, under which the set of elements is closed. The operation $\circ$, called scalar multiplication, may be performed on any number a of $\mathfrak{F}$ and any element α of $\mathfrak{A}$ to produce a unique element $a\circ\alpha$, called the scalar product, which for simplicity we write as $a\alpha$. It is assumed to satisfy $a\alpha=\alpha a$, $a(b\alpha)=(ab)\alpha$, $(a\alpha)(b\beta)=(ab)(\alpha\beta)$, $(a+b)\alpha=a\alpha+b\alpha$, and $a(\alpha+\beta)=a\alpha+a\beta$. The operation $+$, called addition, is commutative and associative. The operation $\times$, called multiplication, is assumed to satisfy $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$, $(\beta+\gamma)\alpha=\beta\alpha+\gamma\alpha$. If multiplication is associative, $\mathfrak{A}$ is called an associative algebra. If $\mathfrak{A}$ contains an element ϵ such that $\alpha\epsilon=\epsilon\alpha=\alpha$ for all α in $\mathfrak{A}$, then ϵ is

called a modulus.

We now let $\mathfrak{A}$ be an associative algebra, with a modulus ϵ, defined over a field $\mathfrak{F}$; and we assume that $\mathfrak{P}$ is a principal ideal ring contained in $\mathfrak{F}$. Then each element of a set $\mathfrak{S}$ of elements of $\mathfrak{A}$ will be called an integral element if the set has the following three properties:

C(closure): the set is closed under addition, subtraction, and multiplication;

U(unity): the set contains the modulus ϵ;

B(finite basis): the set contains elements $\epsilon_1=\epsilon,\epsilon_2,\ldots,\epsilon_k$ such that every element of the set is expressed uniquely in the form $\sum a_i\epsilon_i$, where each a_i is in $\mathfrak{P}$.

As an example we may take $k=1$ and obtain as $\mathfrak{S}$ the ring $\mathfrak{P}$ itself. Again when $\mathfrak{F}$ is the rational field and $\mathfrak{P}$ the rational domain, we see that $\mathfrak{S}$ is a set of integral elements (but not necessarily a maximal set) in the sense of L. E. Dickson [1].

If $\alpha=\sum_{i=1}^{k} a_i\epsilon_i$ is any element of $\mathfrak{S}$, by properties C and B there must exist elements r_{tj} and s_{jt} of $\mathfrak{P}$ such that

$$\alpha\epsilon_j = (\sum a_i\epsilon_i)\epsilon_j = \sum r_{tj}\epsilon_t, \qquad j=1,2,\ldots,k;$$
$$\epsilon_j\alpha = \epsilon_j(\sum a_i\epsilon_i) = \sum s_{jt}\epsilon_t, \qquad j=1,2,\ldots,k.$$

Hence with each α in $\mathfrak{S}$ there are associated matrices $R(\alpha)=(r_{tj})$ and $S(\alpha)=(s_{jt})$ in $\mathfrak{M}(k,k;\mathfrak{P})$.

If E^* indicates the 1-by-k matrix with elements $\epsilon_1,\epsilon_2,\ldots,\epsilon_k$, then in matric notation we have

$$(6.1) \qquad \alpha E^* = E^* R(\alpha), \qquad E^{*T}\alpha = S(\alpha)E^{*T}.$$

Since $\epsilon_1=\epsilon$, the first column of $R(\alpha)$ and the first row of $S(\alpha)$ consist of precisely the elements $a_1,a_2,\ldots,a_k$. Then from property B it follows that the correspondences defined by (6.1) are both one-to-one. Since

$$E^{*T}(\alpha+\beta) = E^{*T}\alpha + E^{*T}\beta = S(\alpha)E^{*T} + S(\beta)E^{*T} = (S(\alpha)+S(\beta))E^{*T},$$
$$E^{*T}(\alpha\beta) = (E^{*T}\alpha)\beta = (S(\alpha)E^{*T})\beta = S(\alpha)(E^{*T}\beta)$$
$$= S(\alpha)(S(\beta)E^{*T}) = (S(\alpha)S(\beta))E^{*T},$$

and since the second correspondence in (6.1) is one-to-one it follows that $S(\alpha+\beta)=S(\alpha)+S(\beta)$ and $S(\alpha\beta)=S(\alpha)S(\beta)$. In an analogous manner it is easily shown that the first correspondence in (6.1) is also preserved under both addition and multiplication. Hence the matrices $R(\alpha)$ and the matrices $S(\alpha)$ provide isomorphic representations for $\mathfrak{S}$, well-known, respectively, as the first and second regular representations.

If α and β are in $\mathfrak{S}$, we may use (6.1) and the fact that elements of $\mathfrak{P}$ commute with elements of $\mathfrak{S}$ to write

$$\begin{aligned} R^T(\alpha)S(\beta)E^{*T} &= R^T(\alpha)E^{*T}\beta = (E^*R(\alpha))^T\beta = (\alpha E^*)^T\beta = (\alpha I_k)E^{*T}\beta \\ &= (\alpha I_k)S(\beta)E^{*T} = S(\beta)(\alpha I_k)E^{*T} = S(\beta)(\alpha E^*)^T \\ &= S(\beta)(E^*R(\alpha))^T = S(\beta)R^T(\alpha)E^{*T}; \end{aligned}$$

then from property B, it follows that, [5],

$$R^T(\alpha)S(\beta) = S(\beta)R^T(\alpha).$$

In particular, letting $A=(a_1,a_2,\ldots,a_k)$ and $B=(b_1,b_2,\ldots,b_k)$ be the first rows of $R^T(\alpha)$ and $S(\beta)$, respectively, we obtain the useful relation

$$AS(\beta) = BR^T(\alpha). \tag{6.2}$$

7. Systems of Linear Equations over $\mathfrak{S}$. We are now going to extend the material in section 3, and we consider the following system of p linear equations in n unknowns:

$$(7.1) \qquad \sum_{i=1}^{n} \alpha_{ij} \chi_i \beta_{ij} = \kappa_j, \qquad j=1,2,\ldots,p;$$

where the α_{ij}, β_{ij}, and κ_j are given elements of $\mathfrak{S}$. Since $\mathfrak{S}$ is not necessarily commutative, note that coefficients are allowed on both sides of the unknowns. We are concerned to establish necessary and sufficient conditions that (7.1) have solutions $\chi=(\chi_1,\chi_2,\ldots,\chi_n)$ in $\mathfrak{M}(1,n;\mathfrak{S})$.

If we assume that such solutions exist, we may write $\chi_i=\sum x_{ij}\epsilon_j$, where the x_{ij} are in $\mathfrak{P}$, and define $X_i=(x_{i1},x_{i2},\ldots,x_{ik})$. Supposing $\kappa_j=\sum k_{ji}\epsilon_i$, we define $K_j=(k_{j1},k_{j2},\ldots,k_{jk})$. We define A_{ij} to be the first row of $S(\alpha_{ij})$. Then (6.2) and (7.1) imply that

$$K_j E^{*T}=\sum A_{ij}E^{*T}\chi_i\beta_{ij}=\sum A_{ij}S(\chi_i)S(\beta_{ij})E^{*T}$$
$$=\sum X_i R^T(\alpha_{ij})S(\beta_{ij})E^{*T}.$$

Hence property B implies that

$$K_j=\sum X_i R^T(\alpha_{ij})S(\beta_{ij}), \qquad j=1,2,\ldots,p.$$

We set $K=(K_1,K_2,\ldots,K_p)$, $X=(X_1,X_2,\ldots,X_n)$, and $A=(R^T(\alpha_{ij})S(\beta_{ij}))$, where K is in $\mathfrak{M}(1,pk;\mathfrak{P})$, X is in $\mathfrak{M}(1,nk;\mathfrak{P})$, and the "enlarged coefficient matrix" A is in $\mathfrak{M}(nk,pk;\mathfrak{P})$ and is made up of k-by-k blocks of which the one in the (i,j)-position is $R^T(\alpha_{ij})S(\beta_{ij})$. Then the equations obtained above may be written as the single matric equation

$$XA=K. \tag{7.2}$$

Except for the size of the matrices involved, (7.2) is precisely a system of the classical type (3.1) with kp equations in kn unknowns, with the elements involved all in $\mathfrak{P}$.

Conversely, if (7.2) has a solution X in $\mathfrak{P}$, we can retrace the steps above to obtain in $\mathfrak{S}$ a solution of (7.1).

Thus the problem of solving (7.1) in $\mathfrak{S}$ has been shown equivalent to solving (7.2) in $\mathfrak{P}$. Referring to (3.4) and (3.4') we can assert that if $e_1,e_2,\ldots$ are the invariant factors of A and if $e'_1,e'_2,\ldots$ are the invariant factors of the augmented matrix $\begin{pmatrix}A\\K\end{pmatrix}$, then necessary and sufficient conditions that the system (7.1) have a solution are that

$$p\leqq n:\quad e_i=e'_i,\qquad i=1,2,\ldots,kp; \tag{7.3}$$

$$n<p:\quad e_i=e'_i,\qquad i=1,2,\ldots,kn;\ \text{and}\quad e'_{kn+1}=0. \tag{7.3'}$$

Determining the number of solutions and the most general solution proceeds along the lines given in section 3. In these matters it is worth a word of caution that the rank of A need not be a multiple of k.

Letting $\mathfrak{F}$ be the rational field and $\mathfrak{P}$ the rational domain, we consider the algebra $\mathfrak{A}$ having as a basis $\epsilon_1=\epsilon,\epsilon_2,\epsilon_3$ with $\epsilon_2\epsilon_2=\epsilon_2$, $\epsilon_3\epsilon_2=\epsilon_3$, and $\epsilon_2\epsilon_3=\epsilon_3\epsilon_3=0$. If we take as $\mathfrak{S}$ the set of all $\alpha=a_1\epsilon_1+a_2\epsilon_2+a_3\epsilon_3$ where a_1, a_2, and a_3 are in $\mathfrak{P}$, we have a set of integral elements with the basis $\epsilon_1,\epsilon_2,\epsilon_3$. Using (6.1) we find

$$R^T(\alpha)=\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_1+a_2 & a_3 \\ 0 & 0 & a_1 \end{pmatrix}, \qquad S(\alpha)=\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_1+a_2 & 0 \\ 0 & 0 & a_1+a_2 \end{pmatrix}.$$

As an example, we study

$$\alpha X \beta = K,$$

when $\alpha=(3\ 3\ 1)E^{*T}$, $\beta=(1\ 5\ 2)E^{*T}$, and $K=(6\ 30\ 0)E^{*T}$; and find

$$A=R^T(\alpha)S(\beta)=\begin{pmatrix} 3 & 3 & 1 \\ 0 & 6 & 1 \\ 0 & 0 & 3 \end{pmatrix}\begin{pmatrix} 1 & 5 & 2 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}=\begin{pmatrix} 3 & 33 & 12 \\ 0 & 36 & 6 \\ 0 & 0 & 18 \end{pmatrix},$$

$$UAV=\begin{pmatrix}1&0&0\\0&1&0\\0&-3&1\end{pmatrix}\begin{pmatrix}3&33&12\\0&36&6\\0&0&18\end{pmatrix}\begin{pmatrix}1&-4&-13\\0&0&-1\\0&1&6\end{pmatrix}=\begin{pmatrix}3&0&0\\0&6&0\\0&0&108\end{pmatrix}=E,$$

$$KV=(6\ 30\ 0)\begin{pmatrix}1&-4&-13\\0&0&-1\\0&1&6\end{pmatrix}=(6\ -24\ -108)=C,$$

$$U'\begin{pmatrix}E\\C\end{pmatrix}V'=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\-2&4&1&1\end{pmatrix}\begin{pmatrix}3&0&0\\0&6&0\\0&0&108\\6&-24&-108\end{pmatrix}I_3=\begin{pmatrix}3&0&0\\0&6&0\\0&0&108\\0&0&0\end{pmatrix}=E'.$$

Since $e_i=e'_i, i=1,2,3$, a solution exists; and, moreover, since $r=p=3$ it is a unique solution. Since (3.2) is

$$(y_1\ y_2\ y_3)\begin{pmatrix}3&0&0\\0&6&0\\0&0&108\end{pmatrix}=(6\ -24\ -108),$$

we obtain $(y_1\ y_2\ y_3)=(2\ -4\ -1)$; and hence the desired solution in $\mathfrak{P}$ is

$$(x_1\ x_2\ x_3)=(2\ -4\ -1)\begin{pmatrix}1&0&0\\0&1&0\\0&-3&1\end{pmatrix}=(2\ -1\ -1).$$

So the unique solution in $\mathfrak{S}$ is $\chi=2\epsilon_1-\epsilon_2-\epsilon_3$.

We note that one type of matric equation, well-known in the literature, is included in the above discussion. Let the algebra $\mathfrak{A}$ be the total matric algebra $\mathfrak{M}(n,n;\mathfrak{F})$ and the set of integral elements $\mathfrak{S}$ be the total matric algebra $\mathfrak{M}(n,n;\mathfrak{P})$. The matrices Z_{ij} of $\mathfrak{M}(n,n;\mathfrak{P})$, where Z_{ij} has 1 in the (i,j)-position and 0's elsewhere, and $Z_{xy}Z_{ij}$ is 0 when $y\neq i$ and Z_{xj} when $y=i$, form a natural basis for $\mathfrak{M}(n,n;\mathfrak{P})$. If

$$E^* = (Z_{11},\ldots,Z_{1n};Z_{21},\ldots,Z_{2n};\ldots;Z_{n1},\ldots,Z_{nn}),$$

it follows from (6.1) and the relation $Z_{ij}B = \sum b_{jx}Z_{ix}$ that the typical element $\beta = \sum b_{ij}Z_{ij}$ in $\mathfrak{M}(n,n;\mathfrak{P})$, which we ordinarily represent as $B=(b_{ij})$, has the regular representations

$$R(\beta) = I_n \times B, \qquad S(\beta) = B \times I_n,$$

where $A\times B$ indicates the direct product matrix in $\mathfrak{M}(n^2,n^2;\mathfrak{P})$ whose (i,j)-block is Ab_{ij}. Then a linear equation like $\alpha\chi\beta=\gamma$ is replaced, according to the theory above for passing from (7.1) to (7.2), by an equation $X'D'=C'$, where

$$D' = R^T(\alpha)S(\beta) = (I_n\times A)^T(B\times I_n) = B\times A^T,$$

X' is 1-by-n^2 and is obtained from $X=(x_{ij})$ by taking row blocks, and C' is in $\mathfrak{M}(1,n^2;\mathfrak{P})$ and is obtained

from $C=(c_{ij})$ by taking row blocks. The general linear equation in one unknown $\sum \alpha_i \chi \beta_i = \gamma$ may be treated in the same manner, the enlarged coefficient matrix being

$$D^{M}=\sum B_i \cdot \chi A_i^{T}.$$

This is the nivellateur studied by Sylvester [13], however, only for the case $\mathfrak{P}=\mathfrak{F}$.

Similarly, the system of equations (7.1) may be generalized to allow each unknown to appear in a finite number of summands in each equation; the technique for passing to (7.2) remains the same, except each component block of the enlarged coefficient matrix will now be a sum of matrices of the type $R^{T}(\alpha_{ij})S(\beta_{ij})$.

If $\mathfrak{A}$ is a non-commutative field and (7.1) is a one-sided system, then if a solution of (7.1) exists in $\mathfrak{A}$ it can be found by an elimination process somewhat analogous to that employed in the classical case -- i.e., in solving a linear system over a commutative field. This result is due to Ore [7], who, by introducing a new definition of determinants in a non-commutative field, determined that elimination between linear systems can be performed in all rings for which a quotient field can exist. If a ring has a quotient field, however, it must contain no divisors of 0. Since $\mathfrak{S}$ may contain divisors

of 0 and (7.1) may be two-sided, the results in this section can be employed to solve linear systems that could not be solved by the elimination process of Ore. Moreover, our results determine whether the solution is in $\mathfrak{S}$ itself, not just in some suitable extension of $\mathfrak{S}$.

8. Minimal Bases for Ideals in $\mathfrak{S}$. In the usual manner the left ideal $\mathfrak{M}$ generated by $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_t$, a given set of elements of $\mathfrak{S}$, is defined to be the set of elements

$$\sum_{i=1}^{t} \nu_i \mathfrak{S}_i$$

obtained by allowing the left-multipliers ν_i to vary independently over all of $\mathfrak{S}$. A minimal basis for the ideal $\mathfrak{M}$ is by definition a set of elements $\mu_1, \mu_2, \ldots, \mu_s$ such that an element of $\mathfrak{S}$ is in the ideal $\mathfrak{M}$ if and only if it can be represented in the form

$$\sum_{i=1}^{s} c_i \mu_i$$

where the c_i are in $\mathfrak{P}$; and this representation is to be unique.

An argument by MacDuffee [3] shows that if H is the uniquely determined left-Hermite form, described in Lemma 2.1, of the matrix

$$S = \begin{pmatrix} s(\mathfrak{S}_1) \\ s(\mathfrak{S}_2) \\ \cdots \\ s(\mathfrak{S}_t) \end{pmatrix},$$

then the non-zero rows H_i of H determine a minimal basis for $\mathfrak{M}$, having $s \leqq k$, by the relation $\mu_i = H_i E^{*T}$. The notation which we have been using makes it simple to reproduce the proof.

Let U be a unimodular matrix in $\mathfrak{M}(kt,kt;\mathfrak{P})$ such that $US = H$. Let $V = U^I$, so that $S = VH$. If the i-th row of U is divided into 1-by-k blocks U_{ij}, then

$$\mu_i = H_i E^{*T} = \sum U_{ij} S(\xi_j) E^{*T} = \sum U_{ij} E^{*T} \xi_j = \sum \nu_{ij} \xi_j,$$

where $\nu_{ij} = U_{ij} E^{*T}$ is in $\mathfrak{S}$; hence μ_i is in the ideal $\mathfrak{M}$, and so are all $\sum c_i \mu_i$.

Conversely, given any element $\nu = \sum \nu_i \xi_i$ in the ideal, we have $\nu_i = \sum n_{ij} \epsilon_j$ and if we define $N_i = (n_{i1}, n_{i2}, \ldots, n_{ik})$ we can write $\nu_i = N_i E^{*T}$. Hence

$$\nu = \sum N_i E^{*T} \xi_i = \sum N_i S(\xi_i) E^{*T} = NSE^{*T} = NVHE^{*T} = \sum c_i \mu_i$$

where N is in $\mathfrak{M}(1,kt;\mathfrak{P})$ and is made up of the 1-by-k blocks N_i, and where c_i is the element in the i-th column of NV. Since c_i is in $\mathfrak{P}$, a representation of the desired type for ν has been found. The uniqueness of the representation follows from the independence of the non-zero rows in the canonical left-Hermite form H.

In an analogous way we define the right-ideal generated by $\xi_1, \xi_2, \ldots, \xi_t$ to be the set of elements

$$\sum \mathfrak{S}_i \eta_i$$

obtained by allowing the right-multipliers η_i to vary independently over $\mathfrak{S}$. In this case a minimal basis can be found by computing the left-Hermite form D of the matrix

$$R = \begin{pmatrix} R^T(\mathfrak{S}_1) \\ R^T(\mathfrak{S}_2) \\ \cdots \\ R^T(\mathfrak{S}_t) \end{pmatrix}$$

in $\mathfrak{M}(kt,k;\mathfrak{P})$; for if $D_1, D_2, \ldots, D_r$ are the non-zero rows of D, necessarily with $r \leqq k$, the elements $\delta_j = D_j E^{*T}$ serve as a minimal basis.

By combining these operations we can find a minimal basis for the two-sided ideal generated by $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_t$, whose typical element is

$$\alpha = \sum_{i=1}^{t} \sum_{j=1}^{q_i} \nu_{ij} \mathfrak{S}_i \eta_{ij},$$

where the q_i are all finite. For we may first compute a minimal basis $\mu_1, \mu_2, \ldots, \mu_s$ for the left-ideal generated by $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_t$ and replace each $\nu_{ij} \mathfrak{S}_i$ by

$$\sum_{m=1}^{s} c_{ijm} \mu_m.$$

Then

$$\alpha = \sum_{m=1}^{s} \mu_m \eta_m$$

where

$$\eta_m = \sum_{i=1}^{t} \sum_{j=1}^{q_i} c_{ijm} \eta_{ij}.$$

Hence if, secondly, we compute a minimal basis $\delta_1, \delta_2, \ldots, \delta_r$ for the right ideal generated by $\mu_1, \mu_2, \ldots, \mu_s$ we will have arrived at a suitable minimal basis $\delta_1, \delta_2, \ldots, \delta_r$ for the two-sided ideal generated by $\varsigma_1, \varsigma_2, \ldots, \varsigma_t$.

However, not every matrix H in left-Hermite form represents a minimal basis for an ideal of $\mathfrak{S}$ [3].

For α and β in $\mathfrak{S}$, by the notation

$$\alpha \equiv \beta \bmod \mathfrak{M}$$

we mean that $\alpha - \beta$ is in the ideal $\mathfrak{M}$, and we say that α and β are in the same residue class mod $\mathfrak{M}$. For the next section, it is important to notice that, in general, it is only when the ideal $\mathfrak{M}$ is two-sided that multiplication of residue classes mod $\mathfrak{M}$ is well-defined.

As an example we take $\mathfrak{S}$ to be the set defined in section 7 and compute the minimal basis for the two-sided ideal generated by $\gamma = 4\epsilon_2 + 6\epsilon_3$.

Since $S(\gamma) = \begin{pmatrix} 0 & 4 & 6 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ has the Hermite form $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

we note that a basis for the left ideal $(\gamma]$ is $\mu_1 = 4\epsilon_2$,

$\mu_2 = 2\epsilon_3$. Next we find $\begin{pmatrix} R^T(\mu_1) \\ R^T(\mu_2) \end{pmatrix} = \begin{pmatrix} 0 & 4 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ has the

Hermite form $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, and conclude that the desired

basis is $\delta_1 = 4\epsilon_2$, $\delta_2 = 2\epsilon_3$.

9. Systems of Linear Congruences Modulo Ideals over $\mathfrak{S}$.

With the necessary preliminary remarks concerning ideals and minimal bases stated in section 8, we are now ready to consider over $\mathfrak{S}$ the following system of p linear congruences, modulo ideals of $\mathfrak{S}$, in n unknowns:

$$(9.1) \qquad \sum_{i=1}^{n} \alpha_{ij} \chi_i \beta_{ij} \equiv \kappa_j \bmod \mathfrak{M}_j, \qquad j = 1,2,\ldots,p.$$

We will assume as explained in section 8 that for the ideal $\mathfrak{M}_j$ whether it be left, right, or two-sided, a minimal basis of s_j elements has been found, say $\mu_{1j}, \mu_{2j}, \ldots, \mu_{s_j j}$, given by $\mu_{ij} = H_{ij} E^{*T}$ where the H_{ij} are non-zero rows of a left-Hermite matrix in $\mathfrak{M}(k,k;\mathfrak{P})$. We let H_j be the matrix in $\mathfrak{M}(s_j,k;\mathfrak{P})$ with rows H_{ij} (this H_j is what is sometimes called the "echelon row form").

Then $\chi_1, \chi_2, \ldots, \chi_n$ is a solution of (9.1) in $\mathfrak{M}(1,n;\mathfrak{S})$ if and only if there exist elements t_{ij} in $\mathfrak{P}$ satisfying

$$(9.2) \qquad \sum_{i=1}^{n} \alpha_{ij} \chi_i \beta_{ij} + \sum_{i=1}^{s_j} t_{ij} \mu_{ij} = \kappa_j, \quad j = 1,2,\ldots,p.$$

Supposing that $\chi_1, \chi_2, \ldots, \chi_n$ is a solution of (9.1), that all the ideals $\mathfrak{M}_j$ are two-sided, and that

(9.3) $\qquad \chi'_i \equiv \chi_i \bmod \mathfrak{M}_j, \qquad i=1,2,\ldots,n;\ j=1,2,\ldots,p;$

then $\chi'_1, \chi'_2, \ldots, \chi'_n$ also solves (9.1). But if one or more of the ideals $\mathfrak{M}_j$ is one-sided, (9.3) is no longer sufficient to guarantee that $\chi'_1, \chi'_2, \ldots, \chi'_n$ is a solution of (9.1). Having given these words of caution, we now define sets of solutions of (9.1) which satisfy (9.3) to be congruent sets. Two solutions of (9.1) which do not satisfy (9.3) are called incongruent.

As in section 7 we let $\chi_i = X_i E^{*T}$, $\kappa_j = K_j E^{*T}$, A_{ij} be the first row of $S(\alpha_{ij})$, and T_j be the matrix $(t_{1j}, t_{2j}, \ldots, t_{s_j j})$ in $\mathfrak{M}(1, s_j; \mathfrak{P})$. Then (6.2) and (9.2) imply that

$$\begin{aligned} K_j E^{*T} &= \sum A_{ij} E^{*T} \chi_i \beta_{ij} + T_j H_j E^{*T} \\ &= \sum A_{ij} S(\chi_i) S(\beta_{ij}) E^{*T} + T_j H_j E^{*T} \\ &= \sum X_i R^T(\alpha_{ij}) S(\beta_{ij}) E^{*T} + T_j H_j E^{*T}. \end{aligned}$$

Hence property B implies that

(9.4) $\qquad K_j = \sum X_i R^T(\alpha_{ij}) S(\beta_{ij}) + T_j H_j, \qquad j=1,2,\ldots,p.$

We set $K=(K_1, K_2, \ldots, K_p)$, $X=(X_1, X_2, \ldots, X_n)$, $T=(T_1, T_2, \ldots, T_p)$, $A=(R^T(\alpha_{ij}) S(\beta_{ij}))$, and $H = H_1 \dot{+} H_2 \dot{+} \ldots \dot{+} H_p$, where $A \dot{+} B$ denotes the direct sum matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. Then the equations (9.4) can be

written as the single matric equation

(9.5) $XA+TH=K.$

We now write

(9.6) $XA\equiv K \bmod H,$

and agree that $X=(X_1,X_2,\ldots,X_n)$ is a solution of (9.6) if and only if there exists a matrix T in $\mathfrak{M}(1,s;\mathfrak{P})$ satisfying (9.5), where $s=\sum s_j$. Following the development of section 4 we call two solutions X and X' of (9.6) congruent if and only if

(9.7) $X'\equiv X \bmod (H_j,I_n), \qquad j=1,2,\ldots,p.$

Two solutions of (9.6) which do not satisfy (9.7) are called incongruent.

Now if $\chi_1, \chi_2,\ldots, \chi_n$ is a solution of (9.1), and $\chi_i=X_iE^{*T}$, then $X=(X_1,X_2,\ldots,X_n)$ is a solution of (9.6). Conversely, if $X=(X_1,X_2,\ldots,X_n)$ is a solution of (9.6), since the steps leading from (9.1) to (9.6) are reversible, it follows that $\chi_1, \chi_2,\ldots, \chi_n$ is a solution of (9.1). Letting $\chi_1, \chi_2,\ldots, \chi_n$ and $\chi'_1, \chi'_2,\ldots, \chi'_n$ be two congruent solutions of (9.1), (9.3) requires the existence of elements w_{rj} in $\mathfrak{P}$ such that

$$\chi'_i - \chi_i = \sum_{r=1}^{s_j} w_{rj}\mu_{rj},$$

which can be written as

$$X'_i E^{*T} - X_i E^{*T} = \sum w_{rj} H_{rj} E^{*T}.$$

Letting $W_j = (w_{1j}, w_{2j}, \ldots, w_{s_j j})$, from property B we have

$$X'_i - X_i = W_j H_j, \qquad i = 1,2,\ldots,n; \qquad j = 1,2,\ldots,p;$$

which, by (9.7), means that X and X' are congruent solutions of (9.6). Since these steps are reversible, we can conclude that the problem of solving the system of congruences (9.1) in $\mathfrak{S}$ is resolved if we solve the system of congruences (9.6) in $\mathfrak{P}$.

Since the system of congruences (9.6) is equivalent to the system of equations (9.5), we write (9.5) in the form $(X\ T)\begin{pmatrix} A \\ H \end{pmatrix} = K$, which is a system of pk equations in nk + s unknowns. If $pk \leqq nk + s$, we apply (3.4) to obtain the necessary and sufficient conditions

$$(9.8) \qquad e_i\begin{pmatrix} A \\ H \end{pmatrix} = e_i\begin{pmatrix} A \\ K \\ H \end{pmatrix}, \qquad i = 1,2,\ldots,pk.$$

If $nk + s < pk$, we apply (3.4') to obtain the necessary and sufficient conditions

$$(9.8') \qquad e_i\begin{pmatrix} A \\ H \end{pmatrix} = e_i\begin{pmatrix} A \\ K \\ H \end{pmatrix}, \qquad i = 1,2,\ldots nk+s; \text{ and}$$

$$e_i\begin{pmatrix} A \\ K \\ H \end{pmatrix} = 0 \text{ for } i = nk+s+1.$$

Thus (9.8) and (9.8') represent necessary and sufficient conditions for the solution of (9.6), and of (9.1).

The solution of (9.6) may be obtained by solving the system of equations (9.5) by the method of section 3; and for each solution (X T) of (9.5) so obtained, X will be a solution of (9.6). This procedure, however, involves the additional parameters t_{ij}; so we now describe an alternative method which does not involve the t_{ij} and is analogous to the procedure of section 4.

Let P_j be a unimodular matrix in $\mathfrak{M}(s_j,s_j,\mathfrak{P})$ and Q_j be a unimodular matrix in $\mathfrak{M}(k,k;\mathfrak{P})$ such that $P_jH_jQ_j = D_j$ is the Smith normal form of H_j. Since H_j has rank $s_j \leqq k$, D_j has the form

$$\begin{pmatrix} d_{1j} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_{2j} & \ldots & 0 & 0 & \ldots & 0 \\ \ldots\ldots & & & & \ldots\ldots & & \\ 0 & 0 & \ldots & d_{s_j j} & 0 & \ldots & 0 \end{pmatrix}.$$

Let m be the l.c.m. of d_{ij}, $i=1,2,\ldots,s_j$, $j=1,2,\ldots,p$;

and let $m = d_{ij}r_{ij}$. Denote by R_j the non-singular diagonal matrix in $\mathfrak{M}(k,k;\mathfrak{P})$ whose i-th diagonal element is r_{ij} for $i \leqq s_j$, and 1 for $s_j < i \leqq k$. Then D_jR_j has the form $(M_{s_j}\ 0)$, where $M_{s_j} = mI_{s_j}$. Letting $P = P_1 \dot{+} P_2 \dot{+} \ldots \dot{+} P_p$, $Q = Q_1 \dot{+} Q_2 \dot{+} \ldots \dot{+} Q_p$, $D = D_1 \dot{+} D_2 \dot{+} \ldots \dot{+} D_p$, and $R' = R_1 \dot{+} R_2 \dot{+} \ldots \dot{+} R_p$; we note that P and Q are unimodular, and $PHQ = D$. We let $R = R'G$ where G is a permutation matrix so that DR has the form $(M_s\ 0)$ where $M_s = mI_s$. Multiplication of the system of equations (9.5) on the right by QR gives

$$XAQR + TP^{I}PHQR = KQR;$$

so that by setting $\bar{A} = AQR$, $\bar{T} = TP^{I}$, $\bar{K} = KQR$, and $\bar{M} = PHQR = DR = (M_s\ 0)$ we have

$$X\bar{A} + \bar{T}\bar{M} = \bar{K}. \tag{9.9}$$

We now write

$$X\bar{A} \equiv \bar{K} \bmod \bar{M}; \tag{9.10}$$

and, as usual, we agree that (9.10) has a solution X if and only if there exists a matrix $\bar{T}$ in $\mathfrak{M}(1,s;\mathfrak{P})$ satisfying (9.9). The system (9.10) is a mixed system of kp-s equations and s congruences of precisely the type considered in section 5, and may be solved by the method described in that section.

Since the steps leading from (9.6) to (9.10) are reversible, it follows that any solution of (9.6) is a solution of (9.10), and conversely. However, as will be illustrated by examples, two solutions X' and X may be congruent solutions of one system and incongruent solutions of the other.

In the particular case when $s_j = k$, $j = 1,2,\ldots,p$, $D_jR_j = M_k = mI_k$, $\overline{M} = DR = M_{kp} = mI_{kp}$ and (9.10) is a system of kp congruences of the type (4.3). Since D_j and R_j are diagonal matrices it follows that $D_jR_j = R_jD_j$. Also $M_kQ_j^I = Q_j^IM_k$ since M_k is a scalar matrix. It now follows from $M_k = D_jR_j = R_jD_j = R_jP_jH_jQ_j$ that $Q_j^IM_k = R_jP_jH_j$. If now X' and X are congruent solutions of (9.10) it is necessary that a matrix T in $\mathfrak{M}(1,kn;\mathfrak{P})$ exists such that

$$X' - X = TM_{kn},$$

where $M_{kn} = mI_{kn}$. Then

$$\begin{aligned} X' - X &= TM_{kn} \\ &= T(M_k \times I_n) \\ &= T(Q_j \times I_n)(Q_j^I \times I_n)(M_k \times I_n) \\ &= T(Q_j \times I_n)(Q_j^IM_k \times I_n) \\ &= T(Q_j \times I_n)(R_jP_jH_j \times I_n) \\ &= T(Q_j \times I_n)(R_jP_j \times I_n)(H_j \times I_n) \\ &= T(Q_jR_jP_j \times I_n)(H_j \times I_n). \end{aligned}$$

Denoting $T(Q_j R_j P_j \times I_n)$ which is in $\mathfrak{M}(1,kn;\mathfrak{P})$ by W_j, we have

$$X' - X = W_j(H_j \times I_n), \qquad j = 1,2,\ldots,p;$$

which are precisely the conditions (9.7) that X' and X be congruent solutions of (9.6). Hence when $s = kp$ all the desired incongruent solutions of (9.6) are found among the incongruent solutions of (9.10). However, the two systems are not equivalent, because two incongruent solutions of (9.10) may be congruent solutions of (9.6). We remark that when $\mathfrak{P} = [\mathfrak{R}a]$, if the rank of $\bar{A}$ is r and $U\bar{A}V = E$ is the Smith form of $\bar{A}$ with invariant factors e_i, then the number $\bar{N}$ of incongruent solutions of (9.6) is such that $\bar{N} \leqq (e_1,m)(e_2,m)\ldots(e_r,m)m^{kn-r}$. When $s < kp$, it is even possible that two congruent solutions of (9.10) are incongruent solutions of (9.6).

We observe that the conditions (9.7) for two solutions X' and X of (9.6) to be congruent imply that $X' - X$ is a common left multiple of the $H_j \times I_n$. By repeated application of the method described in [11] there is a constructive way of finding H_L, the l.c.l.m. of $H_1, H_2, \ldots, H_p$. Then $H_L \times I_n$ is the l.c.l.m. of $H_1 \times I_n, H_2 \times I_n, \ldots, H_p \times I_n$; and, if H_L is in say $\mathfrak{M}(s_L,k;\mathfrak{P})$, the conditions (9.7) are equivalent to the existence of a matrix W in $\mathfrak{M}(1,ns_L;\mathfrak{P})$

such that

$$(9.11) \qquad X' - X = W(H_L \cdot \times I_n).$$

Then for any two particular solutions X' and X, (9.11) is a system of equations of the type (3.1). Hence to determine if X' and X are congruent we may apply (3.4) and (3.4') to obtain conditions expressed in terms of the invariant factors of $(H_L \cdot \times I_n)$ and $\begin{pmatrix} H_L \cdot \times I_n \\ X' - X \end{pmatrix}$.

We take $\mathfrak{S}$ to be the same set of integral elements described in section 7, and as the first example study

$$(9.12) \qquad \alpha \times \beta \equiv \kappa \bmod (\gamma]$$

$$(9.13) \qquad \alpha \times \beta \equiv \kappa \bmod [\gamma),$$

when $\alpha = (3\ 3\ 1)E^{*T}$, $\beta = (1\ 5\ 2)E^{*T}$, $\kappa = (0\ 0\ 2)E^{*T}$, $\gamma = (6\ 2\ 12)E^{*T}$, and where $(\gamma]$ and $[\gamma)$ indicate, respectively, the left and right ideals generated by γ.

We compute:

$$R^T(\alpha)S(\beta) = \begin{pmatrix} 3 & 3 & 1 \\ 0 & 6 & 1 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 5 & 2 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 33 & 12 \\ 0 & 36 & 6 \\ 0 & 0 & 18 \end{pmatrix} = A;$$

$$UAV = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 33 & 12 \\ 0 & 36 & 6 \\ 0 & 0 & 18 \end{pmatrix} \begin{pmatrix} 1 & -4 & -13 \\ 0 & 0 & -1 \\ 0 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 108 \end{pmatrix} = E;$$

$$KV=(0\ 0\ 2)\begin{pmatrix}1 & -4 & -13\\ 0 & 0 & -1\\ 0 & 1 & 6\end{pmatrix}=(0\ 2\ 12)=C;$$

$$S(\gamma)=\begin{pmatrix}6 & 2 & 12\\ 0 & 8 & 0\\ 0 & 0 & 8\end{pmatrix}\ ;\ R^{T}(\gamma)=\begin{pmatrix}6 & 2 & 12\\ 0 & 8 & 12\\ 0 & 0 & 6\end{pmatrix}\ ;$$

$$H=\begin{pmatrix}24 & 0 & 0\\ 12 & 4 & 0\\ 6 & 2 & 4\end{pmatrix}\ ,\ \text{the left-Hermite form of } S(\gamma);\ \text{and}$$

$$G=\begin{pmatrix}24 & 0 & 0\\ 6 & 2 & 0\\ 0 & 0 & 6\end{pmatrix}\ ,\ \text{the left-Hermite form of } R^{T}(\gamma).$$

Next, by the method of Lemma 2.2, we find the invariant factors of $\begin{pmatrix}A\\ H\end{pmatrix}$ are $e_1=1, e_2=2, e_3=12$; the invariant factors of $\begin{pmatrix}A'\\ H\end{pmatrix}$ are $e'_1=1, e'_2=2, e'_3=12$; and we conclude by (9.8) that solutions of (9.12) exist. Similarly we find the invariant factors of $\begin{pmatrix}A\\ G\end{pmatrix}$ are $e_1=1, e_2=6, e_3=12$; the invariant factors of $\begin{pmatrix}A'\\ G\end{pmatrix}$ are $e'_1=1, e'_2=2, e'_3=12$; and we conclude by (9.8) that there is no solution to (9.13).

The solution of (9.12) will now be obtained using the method and notation of this section. The system

(9.6) for this example is

$$(x_1\ x_2\ x_3)\begin{pmatrix}3 & 33 & 12\\ 0 & 36 & 6\\ 0 & 0 & 18\end{pmatrix} \equiv (0\ 0\ 2) \bmod \begin{pmatrix}24 & 0 & 0\\ 12 & 4 & 0\\ 6 & 2 & 4\end{pmatrix}.$$

Upon computing

$$PHQ = \begin{pmatrix}0 & 0 & 1\\ 0 & 1 & -2\\ 1 & 0 & 0\end{pmatrix}\begin{pmatrix}24 & 0 & 0\\ 12 & 4 & 0\\ 6 & 2 & 4\end{pmatrix}\begin{pmatrix}0 & 0 & 1\\ 1 & 2 & -3\\ 0 & -1 & 0\end{pmatrix} = \begin{pmatrix}2 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 24\end{pmatrix} = D,$$

$$R = \begin{pmatrix}12 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 1\end{pmatrix},$$

$$AQR = \begin{pmatrix}3 & 33 & 12\\ 0 & 36 & 6\\ 0 & 0 & 18\end{pmatrix}\begin{pmatrix}0 & 0 & 1\\ 1 & 2 & -3\\ 0 & -1 & 0\end{pmatrix}\begin{pmatrix}12 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}396 & 162 & -96\\ 432 & 198 & -108\\ 0 & -54 & 0\end{pmatrix} = \bar{A},$$

$$KQR = (0\ 0\ 2)\begin{pmatrix}0 & 0 & 1\\ 1 & 2 & -3\\ 0 & -1 & 0\end{pmatrix}\begin{pmatrix}12 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 1\end{pmatrix} = (0\ -6\ 0) = \bar{K},$$

$$DR = \begin{pmatrix}2 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 24\end{pmatrix}\begin{pmatrix}12 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}24 & 0 & 0\\ 0 & 24 & 0\\ 0 & 0 & 24\end{pmatrix} = \bar{M},$$

(9.10) for this example is found to be

$$(x_1\ x_2\ x_3)\begin{pmatrix} 396 & 162 & -96 \\ 432 & 198 & -108 \\ 0 & -54 & 0 \end{pmatrix} \equiv (0\ -6\ 0) \bmod \begin{pmatrix} 24 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & 24 \end{pmatrix},$$

a system of the type (4.3). Proceeding as in section 4 we find

$$U\bar{A}V = \begin{pmatrix} 1 & 1 & 7 \\ 3 & 4 & 25 \\ 0 & -3 & -11 \end{pmatrix}\begin{pmatrix} 396 & 162 & -96 \\ 432 & 198 & -108 \\ 0 & -54 & 0 \end{pmatrix}\begin{pmatrix} 2 & -3 & 8 \\ 1 & -2 & -6 \\ 8 & -12 & 33 \end{pmatrix} = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 36 & 0 \\ 0 & 0 & 324 \end{pmatrix} = \bar{E},$$

$$U^I = \begin{pmatrix} 31 & -10 & -3 \\ 33 & -11 & -4 \\ -9 & 3 & 1 \end{pmatrix},$$

$$\bar{K}V = (0\ -6\ 0)\begin{pmatrix} 2 & -3 & 8 \\ 1 & -2 & -6 \\ 8 & -12 & 33 \end{pmatrix} = (-6\ 12\ 36) = \bar{C};$$

and letting $Y = XU^I$ the system (4.7) is

$$(y_1\ y_2\ y_3)\begin{pmatrix} 6 & 0 & 0 \\ 0 & 36 & 0 \\ 0 & 0 & 324 \end{pmatrix} \equiv (-6\ 12\ 36) \bmod \begin{pmatrix} 24 & 0 & 0 \\ 0 & 24 & 0 \\ 0 & 0 & 24 \end{pmatrix}.$$

The incongruent solutions of this system are

$$y_1 = 3 + 4t_1, \qquad \text{where } t_1 = 0,1,\ldots,5;$$
$$y_2 = 1 + 2t_2, \qquad \text{where } t_2 = 0,1,\ldots,11;$$
$$y_3 = 1 + 2t_3, \qquad \text{where } t_3 = 0,1,\ldots,11;$$

and we note that there are $N = (6,24)(12,24)(12,24) = 6 \cdot 12 \cdot 12 = 864$ incongruent ones. The general solution $X = YU$ of (9.10) is given by

$$x_1 = y_1 + 3y_2$$
$$x_2 = y_1 + 4y_2 - 3y_3$$
$$x_3 = 7y_1 + 25y_2 - 11y_3,$$

which when expressed in terms of the parameters t_i yields

$$x_1 = 4t_1 + 6t_2 + 6$$
$$x_2 = 4t_1 + 8t_2 - 6t_3 + 4$$
$$x_3 = 28t_1 + 50t_2 - 22t_3 + 35$$

where $t_1 = 0,1,\ldots,5$; $t_2 = 0,1,\ldots,11$; and $t_3 = 0,1,\ldots,11$. Since $s = kp = 3$ all the desired incongruent solutions of (9.6) occur among these 864 incongruent solutions of (9.10). The conditions(9.11) for two solutions X' and X of (9.6) to be congruent are $X' - X = WH$, which implies that $(X' - X)QR = (WP^I)(PHQR)$ or $(X' - X)QR \equiv 0 \bmod \overline{M}$.

Since

$$QR = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & -3 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 12 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 12 & 6 & -3 \\ 0 & -3 & 0 \end{pmatrix},$$

we have

$$12(x'_2 - x_2) \equiv 0 \bmod 24$$
$$6(x'_2 - x_2) - 3(x'_3 - x_3) \equiv 0 \bmod 24$$
$$(x'_1 - x_1) - 3(x'_2 - x_2) \equiv 0 \bmod 24,$$

which requires

$$x'_1 - x_1 = 6q_1 \qquad q_1 \equiv q_2 \bmod 4$$
$$x'_2 - x_2 = 2q_2 \quad \text{and} \quad q_3 \equiv q_2 \bmod 2.$$
$$x'_3 - x_3 = 4q_3$$

Expressing these conditions in terms of the parameters t_i and t'_i gives

$$t'_1 \equiv t_1 \bmod 6$$
$$t'_2 - t_2 \equiv t'_3 - t_3 \bmod 4.$$

Hence for any choice of t_1, t_2, t_3 there is 1 way of choosing t'_1, 12 ways of choosing t'_2, 3 ways of choosing t'_3, and hence 36 ways of choosing t'_1, t'_2, t'_3 to obtain solutions $(x'_1\ x'_2\ x'_3)$ of (9.10) and (9.6) which are incongruent to $(x_1\ x_2\ x_3)$ for (9.10) but congruent to $(x_1\ x_2\ x_3)$ for (9.6). Hence the number of incongruent solutions of (9.6) is $\frac{864}{36} = 24$.

As an example we note when $t_1=t_2=t_3=t'_1=0$ and $t'_2=t'_3=1$, that the incongruent solutions (6 4 35) and (12 6 63) of (9.10) are congruent solutions of (9.6).

To illustrate the procedure when $s<kp$ we choose $\alpha=(2\ 0\ 1)E^{*T}$, $\beta=(1\ 2\ 5)E^{*T}$, $\kappa=(4\ 8\ 4)E^{*T}$, $\gamma=4\epsilon_2+6\epsilon_3$, and consider

$$(9.14)\qquad \alpha\chi\beta\equiv\kappa \bmod (\gamma),$$

where (γ) denotes the two-sided ideal generated by γ. In section 8 a basis for this ideal was found to be $\mu_1=4\epsilon_2$, $\mu_2=2\epsilon_3$, so that $H=\begin{pmatrix}0&4&0\\0&0&2\end{pmatrix}$. We compute

$$R^T(\alpha)S(\beta)=\begin{pmatrix}2&0&1\\0&2&1\\0&0&2\end{pmatrix}\begin{pmatrix}1&2&5\\0&3&0\\0&0&3\end{pmatrix}=\begin{pmatrix}2&4&13\\0&6&3\\0&0&6\end{pmatrix}=A,$$

and note that in section 2 the invariant factors of $\begin{pmatrix}A\\H\end{pmatrix}$ were found to be $e_1=1, e_2=2, e_3=4$. The invariant factors of $\begin{pmatrix}A'\\H\end{pmatrix}$ are $e'_1=1, e'_2=2, e'_3=4$, so solutions of (9.14) do exist; and to find them we proceed to solve (9.6) which is

$$(x_1\ x_2\ x_3)\begin{pmatrix}2&4&13\\0&6&3\\0&0&6\end{pmatrix}\equiv(4\ 8\ 4) \bmod \begin{pmatrix}0&4&0\\0&0&2\end{pmatrix}.$$

We compute

$$PHQ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} = D,$$

$$R = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad QR = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix},$$

$$DR = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} = \overline{M},$$

$$AQR = \begin{pmatrix} 2 & 4 & 13 \\ 0 & 6 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 26 & 4 & 2 \\ 6 & 6 & 0 \\ 12 & 0 & 0 \end{pmatrix} = \overline{A},$$

$$KQR = (4\ 8\ 4) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{pmatrix} = (8\ 8\ 4) = \overline{K},$$

and (9.10) is then

$$(x_1\ x_2\ x_3) \begin{pmatrix} 26 & 4 & 2 \\ 6 & 6 & 0 \\ 12 & 0 & 0 \end{pmatrix} \equiv (8\ 8\ 4) \bmod \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}.$$

This system was solved in section 5, and the 8 incongruent solutions are

$$x_1 = 2$$
$$x_2 = 0,2$$
$$x_3 = 0,1,2,3.$$

The condition (9.11) for two solutions of (9.6) to be congruent is $X' - X \equiv 0 \bmod H$, from which we obtain $(X' - X)QR \equiv 0 \bmod \overline{M}$. Simplifying this last relation yields

$$x'_1 = x_1$$
$$x'_2 \equiv x_2 \bmod 4$$
$$x'_3 \equiv x_3 \bmod 2$$

as the conditions that two solutions of (9.6) be congruent. If now $x'_1 = x_1, x'_2 \equiv x_2 \bmod 4$, and $x'_3 \equiv x_3 \bmod 4$, which are the conditions that X' and X be congruent solutions of (9.10), then certainly the above conditions are satisfied and X' and X are also congruent solutions of (9.6). So in this example also all the desired incongruent solutions are found among those of (9.10). The desired incongruent solutions are quite obviously (2 0 0), (2 0 1), (2 2 0) and (2 2 1).

In order to illustrate that two congruent solutions of (9.10) may actually be incongruent solutions of (9.6)

we consider

(9.15) $\chi\beta \equiv \kappa \bmod (\gamma)$

when $\beta=(0\ 1\ 1)E^{*T}$, $\kappa=(0\ 2\ 0)E^{*T}$, and $\gamma=(0\ 0\ 3)E^{*T}$. A basis for this two-sided ideal is $\mu_1=(0\ 0\ 3)E^{*T}$. It is easily seen that the conditions (9.8) are satisfied so that solutions do exist. The system (9.6) is

$$(x_1\ x_2\ x_3)\begin{pmatrix}0&1&1\\0&1&0\\0&0&1\end{pmatrix} \equiv (0\ 2\ 0) \bmod (0\ 0\ 3);$$

$$P=(1),\quad Q=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},\quad R=I_3,\quad \overline{A}=\begin{pmatrix}1&1&0\\0&1&0\\1&0&0\end{pmatrix},$$

$\overline{K}=(0\ 2\ 0)$, $\overline{M}=D=(3\ 0\ 0)$, and the system (9.10) is

$$(x_1\ x_2\ x_3)\begin{pmatrix}1&1&0\\0&1&0\\1&0&0\end{pmatrix} \equiv (0\ 2\ 0) \bmod (3\ 0\ 0).$$

The solution is quite obviously given by

$$x_1+x_2=2$$
$$x_1+x_3\equiv 0 \bmod 3.$$

Let us consider the two particular solutions (5 -3 4) and (8 -6 4). Since

$$(5\ -3\ 4) - (8\ -6\ 4) = (-3\ 3\ 0) = (-1\ 1\ 0) \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

these are congruent solutions of (9.10). For them to be congruent solutions of (9.6) would require the existence of a rational integer w such that

$$(5\ -3\ 4) - (8\ -6\ 4) = (-3\ 3\ 0) = w(0\ 0\ 3).$$

Quite obviously no such w exists, hence these are incongruent solutions of (9.6).

In order to illustrate the necessity of the caution employed in defining congruent solutions, we consider

$$(9.16) \qquad \chi\beta \equiv \kappa \bmod (\delta]$$

where $\beta = (0\ 0\ 1)E^{*T}$, $\kappa = (0\ 0\ 0)E^{*T}$, and $\delta = (6\ 2\ 12)E^{*T}$. Let $\chi_1 = (0\ 1\ 2)E^{*T}$ and $\chi_2 = (6\ 3\ 6)E^{*T}$. Since

$$(6\ 3\ 6) = (0\ 1\ 2) + (0\ 0\ 1) \begin{pmatrix} 24 & 0 & 0 \\ 12 & 4 & 0 \\ 6 & 2 & 4 \end{pmatrix}, \text{ where } H = \begin{pmatrix} 24 & 0 & 0 \\ 12 & 4 & 0 \\ 6 & 2 & 4 \end{pmatrix},$$

it follows that $\chi_2 \equiv \chi_1 \bmod (\delta]$. Since the solution of (9.16) is given by $x_1 \equiv 0 \bmod 8$ and x_2 and x_3 arbitrary, we note that χ_1 is a solution of (9.16) and χ_2 is not a solution of (9.16) even though it is congruent to χ_1.

10. Matrices in $\mathfrak{M}(n,n;\mathfrak{S})$. In the foregoing sections we were able to solve a system of linear equations or linear congruences in $\mathfrak{S}$ by solving an equivalent system in $\mathfrak{P}$. This latter system was obtained directly through the use of the regular representations. B. M. Stewart in [12] made good use of the second regular representation of elements of an algebraic domain to solve the problem of characterizing left-associated matrices. A brief summary of this paper follows.

Let $\mathfrak{F}$ be an algebraic field of order k over the rational field $\mathfrak{Ra}$, and $[\mathfrak{F}]$ the corresponding algebraic domain. A matrix P of $\mathfrak{M}(n,n;[\mathfrak{F}])$ is called unimodular if there exists a matrix Q of $\mathfrak{M}(n,n;[\mathfrak{F}])$ such that $QP=I_n$; and two matrices A and B of $\mathfrak{M}(n,n;[\mathfrak{F}])$ are said to be left-associates in $\mathfrak{M}(n,n;[\mathfrak{F}])$ if there exists a unimodular matrix P of $\mathfrak{M}(n,n;[\mathfrak{F}])$ such that $PA=B$. This notion of left-associativity is an equivalence relation dividing the matrices of $\mathfrak{M}(n,n;[\mathfrak{F}])$ into mutually exclusive classes of left-associated matrices. The fundamental problem of the author was to determine necessary and sufficient conditions for this class division.

If the domain under consideration is a principal ideal ring, a necessary and sufficient condition that A and B be left-associates is that A and B have the same

Hermite canonical form; but for domains whose class number is greater than one, the presence of non-principal ideals prevents the direct solution of the problem by an Hermite form.

However, if each element of a matrix A of $\mathfrak{M}(n,n;[\mathfrak{F}])$ is replaced by its k-by-k second regular representation, there is produced an enlarged matrix A^E, of order kn-by-kn, to be sure, but with elements in the rational domain. Hence for A^E the Hermite form is well-defined and easily found. Stewart's main result was that a necessary and sufficient condition that matrices A and B of $\mathfrak{M}(n,n;[\mathfrak{F}])$ be left-associates in $\mathfrak{M}(n,n;[\mathfrak{F}])$ is that the corresponding enlarged matrices A^E and B^E be left-associates, i.e., that the enlarged matrices have the same Hermite form.

Since the main factor in obtaining this result was the use of the second regular representation, an attempt was made to establish this same theorem for matrices in $\mathfrak{M}(n,n;\mathfrak{S})$ and the partial results obtained are discussed in the remainder of this dissertation.

We recall from section 7 that the matrices Z_{ij}, form a basis for $\mathfrak{M}(n,n;\mathfrak{P})$ such that any matrix $A=(a_{ij})$ in $\mathfrak{M}(n,n;\mathfrak{P})$ can be written uniquely in the form $\sum_{i,j} a_{ij}Z_{ij}$, where a_{ij} is in $\mathfrak{P}$. We let $S^1(A)$ denote the

second regular representation of A, and recall that it has the simple form $S^1(A)=A\times I_n$, where $A\times B$ stands for the direct product matrix (Ab_{ij}) in $\mathfrak{M}(n^2,n^2;\mathfrak{P})$ whose (i,j)-block is Ab_{ij}. We also let $S^2(\alpha)$ denote the second regular representation, described in section 6, of any element α of $\mathfrak{S}$.

The direct product $\mathfrak{M}(n,n;\mathfrak{P})\times\mathfrak{S}$ has the basis

$$(z_{11},\epsilon_1),\ldots,(z_{1n},\epsilon_1),\ldots,(z_{n1},\epsilon_1),\ldots,(z_{nn},\epsilon_1);$$
$$(z_{11},\epsilon_2),\ldots,(z_{1n},\epsilon_2),\ldots,(z_{n1},\epsilon_2),\ldots,(z_{nn},\epsilon_2);$$
$$\ldots$$
$$(z_{11},\epsilon_k),\ldots,(z_{1n},\epsilon_k),\ldots,(z_{n1},\epsilon_k),\ldots,(z_{nn},\epsilon_k);$$

where (z_{ij},ϵ_t) denotes the matrix having ϵ_t in the (i,j)-position and 0's elsewhere,* and

$$(z_{rs},\epsilon_i)(z_{uv},\epsilon_j)=(z_{rs}z_{uv},\epsilon_i\epsilon_j).$$

If $A^*=(\alpha_{ij})$ is any matrix in $\mathfrak{M}(n,n;\mathfrak{S})$ with $\alpha_{ij}=\sum a_{ijt}\epsilon_t$, we write $A^*=\sum_{i,j,t} a_{ijt}(z_{ij},\epsilon_t)$ and conclude that $\mathfrak{M}(n,n;\mathfrak{S})$ is $\mathfrak{M}(n,n;\mathfrak{P})\times\mathfrak{S}$.

In order to obtain the second regular representation of A^* we note that $Z=Z_{11}+Z_{22}+\ldots+Z_{nn}$ is I_n and write

* and $(0,\epsilon_i)$ means matrix of zeros

$$(Z_{pq},\epsilon_r)A^* = (Z_{pq},\epsilon_r)\sum_{i,j,t} a_{ijt}(Z_{ij},\epsilon_t)$$

$$= (Z_{pq},\epsilon_r)\sum_{t} A_t(Z,\epsilon_t), \text{ where } A_t = \sum_{i,j} a_{ijt}(Z_{ij},\epsilon_1)$$

$$= (Z_{pq},\epsilon_1)\sum_{t} A_t(Z,\epsilon_r\epsilon_t)$$

$$= \sum_{t}\sum_{x} a_{qxt}(Z_{px},\epsilon_r\epsilon_t)$$

$$= \sum_{t}\sum_{y}\sum_{x} a_{qxt}c_{rty}(Z_{px},\epsilon_y),$$

where $\epsilon_r\epsilon_t = \sum c_{rty}\epsilon_y$. Arranging (Z_{pq},ϵ_r) and (Z_{px},ϵ_y) each in the order shown above (i.e., hold y and t constant and sum on x, then hold t constant and sum on y, and then sum on t) we find that a second regular representation of A^* is

$$S(A^*) = \sum_{t} S^1(A_t)\cdot\times S^2(\epsilon_t)$$

$$= \sum_{t} (A_t\cdot\times I_n)\cdot\times S^2(\epsilon_t),$$

a matrix in $\mathfrak{M}(kn^2,kn^2;\mathfrak{P})$. For our purposes the repetition in this representation is useless and we shall use

$$(10.1) \qquad s(A^*) = \sum_{t} A_t\cdot\times S^2(\epsilon_t),$$

a matrix in $\mathfrak{M}(kn,kn;\mathfrak{P})$ called the <u>reduced</u> regular

representation. This reduced representation is obviously isomorphic to $\mathfrak{M}(n,n;\mathfrak{S})$. Since the first row of $S^2(\epsilon_t)$ has a 1 in the t-th position and zeros elsewhere we see that the first row block of $s(A^*)$ consists of precisely $A_1, A_2, \ldots, A_k$, the coefficients involved when we write A^* in the form $A^* = \sum_t A_t(Z, \epsilon_t)$. Since the coefficients A_t are unique we see that the reduced regular representation $s(A^*)$ is completely determined by its first row block. From this observation follows immediately an extremely useful lemma.

Lemma 10.2. If X and Y are matrices in $\mathfrak{M}(kn,kn;\mathfrak{P})$ such that $Xs(A^*) = Y$, then there exist matrices X^* and Y^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $s(X^*)s(A^*) = s(Y^*)$; and $X^* = \sum_t X_t(Z, \epsilon_t)$, $Y^* = \sum_t Y_t(Z, \epsilon_t)$ where X_t and Y_t are the matrices in $\mathfrak{M}(n,n;\mathfrak{P})$ found by separating the first block of n rows of X and Y, respectively, into k blocks. We remark that when Y is in s-form, say $Y = s(B^*)$, since the reduced regular representation is completely determined by the first row block, $Y^* = B^*$ and hence $s(X^*)s(A^*) = s(B^*)$.

If we had considered $\mathfrak{M}(n,n;\mathfrak{S})$ from the alternative point of view, i.e., as $\mathfrak{S} \times \mathfrak{M}(n,n;\mathfrak{P})$, we would have obtained as a reduced regular representation of A^* the matrix $A^{*E} = (S^2(\alpha_{ij}))$ in $\mathfrak{M}(kn,kn;\mathfrak{P})$. When $\mathfrak{A} = \mathfrak{F}$, $\mathfrak{S} = [\mathfrak{F}]$ and $\mathfrak{P} = [\mathfrak{Ra}]$, A^{*E} is the matrix A^E used by

Stewart. However, by using $s(A^*)$, the results to follow can be stated more easily.

In order to compare these two reduced regular representations we consider $\mathfrak{M}(2,2;\mathfrak{S})$ when $\mathfrak{S}$ is the same set of integral elements described in section 7 and determine $s(A^*)$ and A^{*E} in this particular case. We use the above notation.

Let $A^*=\begin{pmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{pmatrix}$ and $\alpha_{ij}=a_{ij1}\epsilon_1+a_{ij2}\epsilon_2+a_{ij3}\epsilon_3$.

Then, since $S^2(\alpha_{ij})=\begin{pmatrix}a_{ij1} & a_{ij2} & a_{ij3}\\ 0 & a_{ij1}+a_{ij2} & 0\\ 0 & 0 & a_{ij1}+a_{ij2}\end{pmatrix}$, we have

$$A^{*E}=\begin{pmatrix}S^2(\alpha_{11}) & S^2(\alpha_{12})\\ S^2(\alpha_{21}) & S^2(\alpha_{22})\end{pmatrix}$$

$$=\left(\begin{array}{ccc|ccc} a_{111} & a_{112} & a_{113} & a_{121} & a_{122} & a_{123}\\ 0 & a_{111}+a_{112} & 0 & 0 & a_{121}+a_{122} & 0\\ 0 & 0 & a_{111}+a_{112} & 0 & 0 & a_{121}+a_{122}\\ \hline a_{211} & a_{212} & a_{213} & a_{221} & a_{222} & a_{223}\\ 0 & a_{211}+a_{212} & 0 & 0 & a_{221}+a_{222} & 0\\ 0 & 0 & a_{211}+a_{212} & 0 & 0 & a_{221}+a_{222}\end{array}\right).$$

Since $Z_{11}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$, $Z_{12}=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, $Z_{21}=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$, $Z_{22}=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$,

and $Z=Z_{11}+Z_{22}=I_2$, we write

$$A^* = A_1(Z,\epsilon_1) + A_2(Z,\epsilon_2) + A_3(Z,\epsilon_3),$$

where $A_t = \begin{pmatrix} a_{11t} & a_{12t} \\ a_{21t} & a_{22t} \end{pmatrix}$ and $(Z,\epsilon_t) = \begin{pmatrix} \epsilon_t & 0 \\ 0 & \epsilon_t \end{pmatrix}$.

Then we have

$$s(A^*) = A_1 \cdot\times s^2(\epsilon_1) + A_2 \cdot\times s^2(\epsilon_2) + A_3 \cdot\times s^2(\epsilon_3)$$

$$= \begin{pmatrix} A_1 & 0 & 0 \\ 0 & A_1 & 0 \\ 0 & 0 & A_1 \end{pmatrix} + \begin{pmatrix} 0 & A_2 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & A_2 \end{pmatrix} + \begin{pmatrix} 0 & 0 & A_3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} A_1 & A_2 & A_3 \\ 0 & A_1+A_2 & 0 \\ 0 & 0 & A_1+A_2 \end{pmatrix}$$

$$= \left(\begin{array}{cc|cc|cc} a_{111} & a_{121} & a_{112} & a_{122} & a_{113} & a_{123} \\ a_{211} & a_{221} & a_{212} & a_{222} & a_{213} & a_{223} \\ \hline 0 & 0 & a_{111}+a_{112} & a_{121}+a_{122} & 0 & 0 \\ 0 & 0 & a_{211}+a_{212} & a_{221}+a_{222} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & a_{111}+a_{112} & a_{121}+a_{122} \\ 0 & 0 & 0 & 0 & a_{211}+a_{212} & a_{221}+a_{222} \end{array}\right).$$

The relation between these two reduced regular representations is readily apparent when they are written in the form

$$s(A^*) = \sum_t A_t \cdot\times s^2(\epsilon_t), \qquad A^{*E} = \sum_t s^2(\epsilon_t) \cdot\times A_t.$$

11. Left-Associativity of Matrices in $\mathfrak{M}(n,n;\mathfrak{S})$. A matrix P^* in $\mathfrak{M}(n,n;\mathfrak{S})$ is said to be unimodular if there exists a Q^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $Q^*P^*=I_n$. Two matrices A^* and B^* in $\mathfrak{M}(n,n;\mathfrak{S})$ are called left-associates if there is a unimodular P^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $P^*A^*=B^*$. This notion is obviously an equivalence relation and hence divides the matrices of $\mathfrak{M}(n,n;\mathfrak{S})$ into mutually exclusive classes of left-associated matrices. We wish to compare the left-associativity of A^* and B^* in $\mathfrak{M}(n,n;\mathfrak{S})$ with the left-associativity of $s(A^*)$ and $s(B^*)$ in $\mathfrak{M}(kn,kn;\mathfrak{P})$, i.e., with the condition that $s(A^*)$ and $s(B^*)$ have the same Hermite form.

If $Q^*P^*=I_n$, then $s(Q^*)s(P^*)=s(I_n)=I_{kn}$ and $s(P^*)$ is unimodular with $s(Q^*)=[s(P^*)]^I$. Then $s(P^*)s(Q^*)=I_{kn}$ which implies that $P^*Q^*=I_n$; hence $Q^*=P^{*I}$ and $[s(P^*)]^I=s(P^{*I})$. Conversely, we assume that $s(P^*)$ is unimodular so that a Q exists in $\mathfrak{M}(kn,kn;\mathfrak{P})$ such that $Qs(P^*)=I_{kn}$. Since $I_{kn}=s(I_n)$, applying Lemma 10.2 yields, according to the remark immediately succeeding the lemma, a Q^* such that $s(Q^*)s(P^*)=s(I_n)$. Then $Q=[s(P^*)]^I=s(Q^*)$ and we conclude that Q is in s-form, and since $Q^*P^*=I_n$ that P^* is unimodular. Hence a necessary and sufficient condition that P^* be unimodular in $\mathfrak{M}(n,n;\mathfrak{S})$ is that $s(P^*)$ be unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$.

Now if A^* and B^* are left-associates in $\mathfrak{M}(n,n;\mathfrak{S})$ so that $P^*A^* = B^*$ for some P^* unimodular in $\mathfrak{M}(n,n;\mathfrak{S})$, it follows that $s(P^*)s(A^*) = s(B^*)$ and $s(P^*)$ is unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$. Hence $s(A^*)$ and $s(B^*)$ are left-associates; and, by Lemma 2.1, must have the same Hermite form. This establishes that:

A necessary condition that A^* and B^* be left-associates in $\mathfrak{M}(n,n;\mathfrak{S})$ is that $s(A^*)$ and $s(B^*)$ have the same Hermite form.

Let O_j denote the j-by-j matrix which consists entirely of 0's. If A^* is a proper divisor of 0, i.e., $A^* \neq O_n$ and there exists a $W^* \neq O_n$ in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $W^*A^* = O_n$, then $s(W^*)s(A^*) = s(O_n) = O_{kn}$ and $s(W^*) \neq O_{kn}$. Hence the rows of $s(A^*)$ are linearly dependent over $\mathfrak{P}$ and $s(A^*)$ is singular. Conversely, let us assume that $s(A^*)$ is singular. Then the rows of $s(A^*)$ are linearly dependent over $\mathfrak{P}$ and there exists a T_1 in $\mathfrak{M}(1,kn;\mathfrak{P})$ such that

$$T_1 s(A^*) = (0,0,\ldots,0)$$

and not all the elements of T_1 are 0. Letting T be the matrix in $\mathfrak{M}(kn,kn;\mathfrak{P})$ whose first row is T_1 and whose remaining elements are all 0's, we have

$$Ts(A^*) = O_{kn}.$$

We apply Lemma 10.2 to determine T^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $s(T^*)s(A^*)=s(0_n)$. Then $T^*A^*=0_n$ and $T^*\neq 0_n$ since T_1 contained elements other than 0. Hence a necessary and sufficient condition that A^* be a divisor of 0 is that $s(A^*)$ be singular.

Let us now assume that A^* and B^* are not divisors of 0, and are such that $s(A^*)$ and $s(B^*)$ have the same Hermite form H so that there exist matrices X and Y, unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$, such that $Xs(A^*)=H=Ys(B^*)$. Then $P=Y^IX$ is unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$ and $Ps(A^*)=s(B^*)$. Applying Lemma 10.2 to this relation determines, according to the remark immediately succeeding the lemma, a P^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $s(P^*)s(A^*)=s(B^*)$. Since $s(A^*)$ is non-singular, however, we have $P=s(B^*)\left[s(A^*)\right]^I=s(P^*)$ which means that P is in s-form. Since $s(P^*)=P$ is unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$, it follows, as we have shown earlier, that P^* is unimodular in $\mathfrak{M}(n,n;\mathfrak{S})$. Thus $P^*A^*=B^*$ with P^* unimodular, and we can now state the following theorem:

If A^* and B^* of $\mathfrak{M}(n,n;\mathfrak{S})$ are not divisors of 0, then a necessary and sufficient condition that they be left-associates in $\mathfrak{M}(n,n;\mathfrak{S})$ is that $s(A^*)$ and $s(B^*)$ be left-associates in $\mathfrak{M}(kn,kn;\mathfrak{P})$.

To illustrate we choose the same set $\mathfrak{M}(2,2;\mathfrak{S})$ that we used in section 10, and consider

$$A^* = \begin{pmatrix} 2\epsilon_1+\epsilon_2+2\epsilon_3 & -\epsilon_1+\epsilon_2+\epsilon_3 \\ \epsilon_1-\epsilon_2-3\epsilon_3 & \epsilon_1+\epsilon_2-2\epsilon_3 \end{pmatrix} \text{ and}$$

$$B^* = \begin{pmatrix} 7\epsilon_1-\epsilon_2 & -2\epsilon_1-4\epsilon_2+\epsilon_3 \\ 12\epsilon_1-21\epsilon_2+\epsilon_3 & -3\epsilon_1+11\epsilon_2+\epsilon_3 \end{pmatrix}.$$

Since $A_1 = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, $A_3 = \begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix}$,

and $B_1 = \begin{pmatrix} 7 & -2 \\ 12 & -3 \end{pmatrix}$, $B_2 = \begin{pmatrix} -1 & -4 \\ -21 & 11 \end{pmatrix}$, $B_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$,

from the expression for $s(A^*)$ derived in section 10 we find

$$s(A^*) = \begin{pmatrix} 2 & -1 & 1 & 1 & 2 & 1 \\ 1 & 1 & -1 & 1 & -3 & -2 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}, \text{ and}$$

$$s(B^*) = \begin{pmatrix} 7 & -2 & -1 & -4 & 0 & 1 \\ 12 & -3 & -21 & 11 & 1 & 1 \\ 0 & 0 & 6 & -6 & 0 & 0 \\ 0 & 0 & -9 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & -6 \\ 0 & 0 & 0 & 0 & -9 & 8 \end{pmatrix}.$$

We compute

$$Xs(A^*) = \begin{pmatrix} 6 & 6 & 0 & -6 & 2 & 3 \\ 0 & 6 & 2 & -3 & 6 & 6 \\ 0 & 2 & 1 & -1 & 2 & 2 \\ 0 & 3 & 1 & -1 & 3 & 3 \\ 2 & 2 & 0 & -2 & 1 & 1 \\ 3 & 3 & 0 & -3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 7 & -2 & -1 & -4 & 0 & 1 \\ 12 & -3 & -21 & 11 & 1 & 1 \\ 0 & 0 & 6 & -6 & 0 & 0 \\ 0 & 0 & -9 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & -6 \\ 0 & 0 & 0 & 0 & -9 & 8 \end{pmatrix}$$

$$= \begin{pmatrix} 18 & 0 & 0 & 0 & 0 & 0 \\ 6 & 6 & 0 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 & 0 \\ 3 & 3 & 0 & 1 & 0 & 0 \\ 6 & 0 & 0 & 0 & 1 & 0 \\ 9 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = H.$$

We discover that there exists a unimodular Y such that $Ys(B^*)=H$ and we compute

$$Y^I = \begin{pmatrix} 0 & 2 & -1 & -4 & 0 & 1 \\ 0 & 1 & -21 & 11 & 1 & 1 \\ 0 & 1 & 6 & -6 & 0 & 0 \\ 0 & -1 & -9 & 8 & 0 & 0 \\ 1 & 0 & 0 & 0 & 6 & -6 \\ -1 & 0 & 0 & 0 & -9 & 8 \end{pmatrix}.$$

Then

$$P = Y^I X = \begin{pmatrix} 3 & 1 & -1 & -4 & -1 & 0 \\ 5 & 2 & -8 & 2 & -1 & 0 \\ 0 & 0 & 2 & -3 & 0 & 0 \\ 0 & 0 & -3 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -3 \\ 0 & 0 & 0 & 0 & -3 & 4 \end{pmatrix}$$

and we note, as the theory predicted, that P is unimodular and in s-form.

We now obtain

$$P^* = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} \epsilon_1 & 0 \\ 0 & \epsilon_1 \end{pmatrix} + \begin{pmatrix} -1 & -4 \\ -8 & 2 \end{pmatrix}\begin{pmatrix} \epsilon_2 & 0 \\ 0 & \epsilon_2 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \epsilon_3 & 0 \\ 0 & \epsilon_3 \end{pmatrix}$$

$$= \begin{pmatrix} 3\epsilon_1 - \epsilon_2 - \epsilon_3 & \epsilon_1 - 4\epsilon_2 \\ 5\epsilon_1 - 8\epsilon_2 - \epsilon_3 & 2\epsilon_1 + 2\epsilon_2 \end{pmatrix},$$

which is the desired unimodular matrix such that $P^*A^* = B^*$.

If A^* and B^* are divisors of 0, and are such that $s(A^*)$ and $s(B^*)$ have the same Hermite form H, as before there exist matrices X and Y, unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$, such that $Xs(A^*) = H = Ys(B^*)$; and $P = Y^I X$ is unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$ and such that $Ps(A^*) = s(B^*)$. We also can apply Lemma 10.2 to determine from the first row block of P a matrix P^* in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $s(P^*)s(A^*) = s(B^*)$. However, as we shall show by means of an example, the matrix $s(P^*)$ so determined is not necessarily unimodular. Since $s(A^*)$ and $s(B^*)$ are singular, H is also; and the most general unimodular matrix G (described in Lemma 2.1) such that $GH = H$ is not I_{kn}. Since $Y^I GX$ is unimodular in $\mathfrak{M}(kn,kn;\mathfrak{P})$ and such that $Y^I GXs(A^*) = s(B^*)$, there is some freedom in the choice of the matrix P and hence of P^*. Whether or not G can be chosen so that $Y^I GX$ is in s-form has not been established.

If we let $Q=X^{I}Y$, then $Qs(B^{*})=s(A^{*})$; and applying Lemma 10.2 to this relation determines a Q^{*} in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $s(Q^{*})s(B^{*})=s(A^{*})$ and $s(Q^{*})$ is not necessarily unimodular. Hence, if A^{*} and B^{*} are divisors of 0 and such that $s(A^{*})$ and $s(B^{*})$ have the same Hermite form, then there exist matrices P^{*} and Q^{*} in $\mathfrak{M}(n,n;\mathfrak{S})$ such that $P^{*}A^{*}=B^{*}$ and $Q^{*}B^{*}=A^{*}$ -- i.e., A^{*} and B^{*} are mutually left-divisible. At this point, by referring to the result due to Steinitz [10] that mutual left-divisibility is equivalent to left-associativity for matrices in $\mathfrak{M}(n,n;[\mathfrak{F}])$, Stewart was able to establish his result where $[\mathfrak{F}]$ is an algebraic domain of classical type.

Some results about mutual left-divisibility implying left-associativity are given by Kaplansky [2], but they cannot be applied here for we have not restricted the algebra $\mathfrak{A}$ which contains $\mathfrak{S}$.

As an example we consider once more the same $\mathfrak{M}(2,2;\mathfrak{S})$ and study

$$A^{*}=\begin{pmatrix}2\epsilon_{2}+\epsilon_{3} & 0\\ 0 & 0\end{pmatrix}, \text{ and } B^{*}=\begin{pmatrix}2\epsilon_{2}+2\epsilon_{3} & 0\\ \epsilon_{3} & 0\end{pmatrix}.$$

We note that

$$A_{1}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, A_{2}=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}, A_{3}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, B_{1}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

$$B_2=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}, \text{ and } B_3=\begin{pmatrix}2 & 0\\ 1 & 0\end{pmatrix}; \text{ so that}$$

$$s(A^*)=\begin{pmatrix}0&0&2&0&1&0\\0&0&0&0&0&0\\0&0&2&0&0&0\\0&0&0&0&0&0\\0&0&0&0&2&0\\0&0&0&0&0&0\end{pmatrix} \text{ and } s(B^*)=\begin{pmatrix}0&0&2&0&2&0\\0&0&0&0&1&0\\0&0&2&0&0&0\\0&0&0&0&0&0\\0&0&0&0&2&0\\0&0&0&0&0&0\end{pmatrix}.$$

We compute

$$Xs(A^*)=\begin{pmatrix}-2&0&2&0&1&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\1&0&-1&0&0&0\\0&0&0&0&0&1\end{pmatrix}\begin{pmatrix}0&0&2&0&1&0\\0&0&0&0&0&0\\0&0&2&0&0&0\\0&0&0&0&0&0\\0&0&0&0&2&0\\0&0&0&0&0&0\end{pmatrix}$$

$$=\begin{pmatrix}0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&2&0&0&0\\0&0&0&0&0&0\\0&0&0&0&1&0\\0&0&0&0&0&0\end{pmatrix}=H,$$

We find a unimodular Y such that $Ys(B^*)=H$ and we compute

$$Y^I=\begin{pmatrix}1&0&1&0&2&0\\0&1&0&0&1&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&1&0&0&2&0\\0&0&0&0&0&1\end{pmatrix}.$$

Then

$$P = Y^{I}X = \begin{pmatrix} 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We note that P is unimodular but not in s-form. When we apply Lemma 10.2 to obtain the matrix in s-form determined by the first row block of P we find

$$s(P^{*}) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

which we easily see is <u>singular</u>. The matrix G mentioned above is

$$G = \begin{pmatrix} g_{11} & g_{12} & 0 & g_{14} & 0 & g_{16} \\ g_{21} & g_{22} & 0 & g_{24} & 0 & g_{26} \\ g_{31} & g_{32} & 1 & g_{34} & 0 & g_{36} \\ g_{41} & g_{42} & 0 & g_{44} & 0 & g_{46} \\ g_{51} & g_{52} & 0 & g_{54} & 1 & g_{56} \\ g_{61} & g_{62} & 0 & g_{64} & 0 & g_{66} \end{pmatrix}$$

where $\begin{pmatrix} g_{11} & g_{12} & g_{14} & g_{16} \\ g_{21} & g_{22} & g_{24} & g_{26} \\ g_{41} & g_{42} & g_{44} & g_{46} \\ g_{61} & g_{62} & g_{64} & g_{66} \end{pmatrix}$ is unimodular,

so in this particular example there is a great deal of freedom that we can exercise in choosing $P = Y^{I}GX$. However, due to the simplicity of $s(A^*)$ and $s(B^*)$, by direct observation we can find

$$s(P^*) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$ which is obviously

unimodular; and hence a unimodular matrix of the desired type is

$$P^* = \begin{pmatrix} \epsilon_2+\epsilon_3 & \epsilon_1 \\ \epsilon_1-\epsilon_2 & \epsilon_2 \end{pmatrix}.$$

12. Conclusion. The problem of solving a system of linear equations or a system of linear congruences whose elements are integers from an algebra has been completely solved. Concerning the left-associativity of matrices whose elements are integers from an algebra, it has been established that when A^* and B^* are not divisors of 0, a necessary and sufficient condition that they be left-associates is that $s(A^*)$ and $s(B^*)$ have the same Hermite form. Also, when A^* and B^* are divisors of 0, this condition is necessary. The problem remaining for further research is the determination whether, when A^* and B^* are divisors of 0, the fact that $s(A^*)$ and $s(B^*)$ have the same Hermite form is a sufficient condition that A^* and B^* be left-associates. Perhaps additional conditions concerning A^* and B^* must be added; but if this is not so the Hermite form of the reduced regular representations would certainly be an interesting and practical criterion for determining left-associated matrices whose elements are integers from an algebra.

BIBLIOGRAPHY

1. Dickson, L. E., Algebras and their arithmetics, (Chicago, 1923), Chapter X.

2. Kaplansky, I., Elementary divisors and modules, Trans. Amer. Math. Soc., 66(1949), 464-491.

3. MacDuffee, C. C., An introduction to the theory of ideals in linear associative algebras, Trans. Amer. Math. Soc., 31(1929), 71-90.

4. MacDuffee, C. C., Matrices with elements in a principal ideal ring, Bull. Amer. Math. Soc., 39(1933), 564-584.

5. MacDuffee, C. C., Modules and ideals in a Frobenius algebra, Monat. fur Math. und Physik, 48(1939), 293-313.

6. MacDuffee, C. C., Theory of Matrices, (Chelsea, 1946).

7. Ore, O., Linear equations in non-commutative fields, Annals of Math., 32(1931), 463-477.

8. Smith, H. J. S., On systems of linear indeterminate equations and congruences, Phil. Trans. Roy Soc. of London, 151(1861), 293-326.

9. Smith, H. J. S., On the arithmetical invariants of a rectangular matrix of which the constituents are integral numbers, Proc. London Math. Soc., IV(1873), 236-249.

10. Steinitz, E., Recteckige systeme und moduln in algebraischen zahlkorpern, Mathematishe Annalen, 71(1911), 328-354, and 72(1912), 297-345.

11. Stewart, B. M., A note on least common left-multiples, Bull. Amer, Math. Soc., 55(1949), 587-591.

12. Stewart, B. M., Left-associated matrices with elements in an algebraic domain, Amer. Jour. of Math., LXIX(1947), 562-574.

13. Sylvester, J., C. R. Acad. Sci., Paris, 99(1884), 117-118, 409-412, 432-436, 527-529.