1968

Ring and its complete matrix ring

Leonard Joseph McPeek

The University of Montana

A RING AND ITS COMPLETE MATRIX RING

By

Leonard Joseph McPeek

B.A., University of British Columbia, 1959

Presented in partial fulfillment of the requirements for the degree of

Master of Arts

UNIVERSITY OF MONTANA

1968

Approved by:

Gloria C. Hewitt

Chairman, Board of Examiners

John M. Stewart

Dean, Graduate School

August 6, 1968

Date

ACKNOWLEDGEMENTS

I am indebted to Professor Gloria Hewitt for suggesting the topic of this thesis and for the encouragement and guidance she provided during the preparation of this paper. I also want to thank Dr. Hewitt for her critical reading of the manuscript and for her many helpful suggestions during the writing of this thesis. In addition I want to thank Professor M. Manis for his critical reading of the manuscript, and my wife for her typing of the manuscript.

L. J. M.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION AND PRELIMINARIES

The theory of linear transformations from one vector space to another furnishes a convenient approach to the study of matrices over a field. Herstein [4] and Halmos [3] develop the theory of matrices over a field from this point of view.

This thesis will develop the more general notion of matrices over an arbitrary commutative ring with identity. The reader who is familiar with the theory of matrices over a field will recognize that many of the results we develop here are direct generalizations of results in the study of the theory of matrices over a field. In the development of the complete matrix ring, the basic concepts regarding modules come from notes taken during a seminar in Ring Theory that this author attended during the Summer of 1966. The basic concepts of modules may be found in Zariski and Samuel [10] and in Jans [5]. We will show that there is a one-to-one correspondence between the set of all n by m matrices over a commutative ring with identity and the set of homomorphisms from one unitary free module to another. Further, we show that the set of n by n matrices and the set of homomorphisms from one unitary free module into itself are isomorphic rings with identity.

In Chapter III we develop certain relationships between the ring itself and its complete matrix ring. The basic properties of rings and ideals, a development of which may be found in McCoy [8] , enable us to characterize the ideals in the complete matrix ring.

The concept of a ring being Noetherian may be found in Zariski and Samuel [11] . We are able to show under what circumstances the complete matrix ring becomes Noetherian. Chapter III concludes with a comparison of the radical properties of a ring and its complete matrix ring. Divinsky [2] provides us with a thorough development of radicals. We will show the equivalence of a commutative ring with identity and its complete matrix ring being both nil-semi-simple and prime-semi-simple. We also show when the complete matrix ring is Jacobson-semi-simple.

Chapter IV develops the theory of determinants over a commutative ring with identity along the lines that Artin [1] develops determinants over a field. We follow the development of McCoy [7] and characterize inverses and zero divisors in the complete matrix ring.

Before proceeding further, we list some of the notation that recurs throughout this paper.

Numbers in square brackets, such as [5] , indicate references.

We will use the symbol $\bigcup$ to represent set theoretic union, $\bigcap$ for intersection, $\subseteq$ for inclusion, etc. In addition to these symbols, we will use $\sum$ to represent a summation and $\cong$ to represent an isomorphism between two sets.

A map from one set to another will be indicated by f, g, h, ... If f maps M into N, this will be denoted by $f:M \to N$. For mappings $f:M \to N$ and $g:N \to V$, let $g \circ f$ denote the composite of the mappings. If T is a subset of M and S a subset of N, then $f[T] = \{f(t) \mid t \in T\}$ will represent the image of T in N under the map f.

$f^{-1}[S] = \{m \in M \mid f(m) \in S\}$ will represent the inverse image of S in M under the map f. For $a \in M$, f(a) denotes the image in N of the element a. We sometimes write im f for $f[M]$.

The set of natural numbers will be represented by $\mathbb{N}$ and the integers by $\mathbb{Z}$. Lower case Latin letters a, b, c, ..., will generally denote elements of sets with the exception that matrices will be denoted by capital Latin letters A, B, C, ... Subsets of matrices will be denoted by capital script letters $\mathcal{A}$, $\mathcal{B}$, ... When we wish to refer to the individual entries of a matrix A, the matrix will be denoted by $A = (a_{ij})$ or $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \vdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$

Throughout this thesis we will assume that the reader is familiar with the concepts and basic properties of rings, ideals, fields, matrices over a field, a vector space over a field, and determinants of matrices over a field.

If a ring has identity, 1 will stand for that identity. It is assumed that $1 \neq 0$. For non-empty subsets A and B of a ring R, A B is the set of all sums $\sum_{i=1}^{n} a_i b_i$ where $n \in \mathbb{N}$ and $a_i \in A$, $b_i \in B$.

If R is a ring and $S \subseteq R$, then $\langle S \rangle$ will denote the ideal in R generated by S. If $S = \{a_1, a_2, \ldots, a_n\}$, $\langle S \rangle$ will be written simply as $\langle a_1, \ldots, a_n \rangle$. In general, if $a \in R$, then $\langle a \rangle =$ $\{n a + r a + a s + \sum_{i=1}^{m} p_i a q_i \mid n, m \in \mathbb{N}; r, s, p_i, q_i \in R\}$. This may be indicated by $\langle a \rangle = \mathbb{N} a + R a + a R + R a R$. If R has 1, then $\langle a \rangle = \left\{ \sum_{i=1}^{m} p_i \, a \, q_i \;\middle|\; m \in \mathbb{N};\ p_i,\ q_i \in R \right\} =$ $R\,a\,R$. If R is commutative, then $\langle a \rangle = \left\{ n\,a + r\,a \;\middle|\; n \in \mathbb{N},\ r \in R \right\} = \mathbb{N}\,a + R\,a$. Finally if R is commutative with 1, then $\langle a \rangle = \left\{ r\,a \;\middle|\; r \in R \right\} = R\,a$.

We will have occasion to refer to Zorn's Lemma, which states that if each chain in a partially ordered set has an upper bound in the set, then there is a maximal element in the set.

A set, S, of elements in a partially ordered set P with ordering $\leqslant$ forms a chain if a, b $\in$ S implies $a \leqslant b$ or $b \leqslant a$.

CHAPTER II

THE DEVELOPMENT OF THE COMPLETE MATRIX RING

Definition 2.1 For a commutative ring R with 1, a non-empty set M is called a unitary module over R, or a unitary R-module, if:

1. (M, +) is an abelian group
2. there exists a map $f: R \times M \longrightarrow M$ such that for every $r, s \in R$ and for every $x, y \in M$,

   i) $f(r, x + y) = f(r, x) + f(r, y)$

   ii) $f(r + s, x) = f(r, x) + f(s, x)$

   iii) $f(rs, x) = f(r, f(s, x))$

   iv) $f(1, x) = x$.

We denote $f(r, x)$ by rx.

Examples:

1. Let $R = \mathbb{Z}$, M be any abelian group with respect to +. Then M is a unitary R-module.
2. Any vector space over a field F is a unitary F-module.
3. Let R be any ring with 1. Let M be any left ideal of R. Then M is a unitary R-module.
4. Let V be a finite dimensional vector space over a field F. Let A be a linear transformation of V. V can be considered as an $F[x]$ - module by defining:

   if $f = a_0 + a_1 x + \dots + a_n x$, then

   $fv = a_0 + a_1 (Av) + \dots + a_n (A^n v) = f[A]v$.

Definiton 2.2 For unitary R-modules M and N, let $h: M \longrightarrow N$. Then h is called a homomorphism if for every $r, s \in R$ and for every

$x, y \in M$, $h(rx + sy) = rh(x) + sh(y)$. h is called an epimorphism if h is onto, a monomorphism if h is 1-1, and an isomorphism if h is 1-1 and onto.

Definition 2.3 For a unitary R-module M and S a subgroup of M, S is called an R-submodule of M if $RS \subseteq S$.

We note that if R is a ring considered as an R-module, then the R-submodules are just the left ideals of R. If V is a vector space over a field F, the F-submodules of V are what we usually call the subspaces of V and the homomorphisms of V are just the linear mappings of V.

Definition 2.4 Let $L:M \longrightarrow N$ be a homomorphism, M and N unitary R-modules. $\{x \in M \mid h(x) = 0$, the identity in $N\}$ is called the kernel of h, denoted by ker h.

We now take a look at some of the properties of homomorphisms over unitary R-modules. The reader will recognize the corresponding properties as applied to linear transformations over a vector space.

Lemma 2.1 Let $h:M \longrightarrow N$ be a homomorphism. Let K be an R-submodule of M and H an R-submodule of N. Then:

i) $h[K]$ is an R-submodule of N.

ii) $h^{-1}[H]$ is an R-submodule of M.

iii) the mappings $f:K \longrightarrow h[K]$ and $g:H \longrightarrow h\,[H]$ are inverse one-to-one correspondences between the sets of R-submodules $\{K \subseteq M \mid K$ is a submodule of M, ker $h \subseteq K\}$ and $\{H \subseteq N \mid H$ is a submodule of N, $H \subseteq$ im $h\}$. Henceforth submodules will be abbreviated s.m.

Proof: i) Let $r \in R$ and $x, y \in h[K]$. Then there exist $a, b \in K$ such that $h(a) = x$ and $h(b) = y$. As K is a s.m. of M, $a - b \in K$. Thus $x - y = h(a) - h(b) = h(a - b) \in h[K]$. Also $rx = rh(a) = h(ra) \in h[K]$. Hence $h[K]$ is a s.m. of N.

ii) Let $r \in R$ and $x, y \in h^{-1}[H]$. Again there exist $a, b \in H$ such that $h(x) = a$ and $h(y) = b$. So $h(x - y) = h(x) - h(y) = a - b \in H$ and $h(rx) = rh(x) = ra \in H$. Hence $x - y$ and $rx \in h^{-1}[H]$. Thus $h^{-1}[H]$ is a s.m. of M.

iii) For any s.m. K of M, obviously $h[K] \subseteq$ im h and is a s.m. of N by i). Suppose ker h $\subseteq K$. Let $h[K] = H$. Let $h^{-1}[H] = J \subseteq M$. We must show that $J = K$. It is well known that $K \subseteq J$. Let $x \in J$. Then $h(x) \in H$. Thus there exists $y \in K$ such that $h(y) = h(x)$. Hence $h(x) - h(y) = h(x - y) = 0$; so $x - y \in$ ker h $\subseteq K$. As y and $x - y \in K$, $x \in K$. Thus $J \subseteq K$ and hence $J = K$.

Conversely, let H be a s.m. of N with $H \subseteq$ im h. It is well known that $h\left[h^{-1}[H]\right] \subseteq H$. As $0 \in H$, ker h $\subseteq h^{-1}[H]$. Let $x \in H$. As $H \subseteq$ im h, there exists $y \in M$ such that $h(y) = x$. Then $y \in h^{-1}[H]$ and $x = h(y) \in h\left[h^{-1}[H]\right]$. Thus $H \subseteq h\left[h^{-1}[H]\right]$. Thus we have $H = h\left[h^{-1}[H]\right]$ and $K = h^{-1}\left[h[K]\right]$ for all s.m.'s. H of N with $H \subseteq$ im h and s.m.'s K of M with ker h $\subseteq K$. Hence f and g are inverse 1 - 1 correspondences.

Observe that im h is a s.m. of N because im h $= h[M]$ and ker h is a s.m. of M because ker h $= h^{-1}\left[\{0\}\right]$.

<u>Lemma</u> 2.2 Any intersection of R-submodules of an R-module M is an R-module. Moreover if S and T are s.m.'s of M, then S + T is a s.m. of M.

Proof: Let $\{ S_j \mid j \in \Gamma \}$ be a family of s.m.'s of M. Clearly $\bigcap_{j \in \Gamma} S_j \subseteq M$. Let x, $y \in \bigcap_{j \in \Gamma} S_j$. Then x, $y \in S_j$ for all $j \in \Gamma$. As each S_j is a s.m. of M, $x - y \in S_j$ for all $j \in \Gamma$, which implies that $x - y \in \bigcap_{j \in \Gamma} S_j$. Next, let $r \in R$. Then $rx \in S_j$ for all $j \in \Gamma$. So $rx \in \bigcap_{j \in \Gamma} S_j$. Thus $\bigcap_{j \in \Gamma} S_j$ is a s.m. of M.

Let x, $y \in S + T$. Then $x = s + t$ and $y = \bar{s} + \bar{t}$ where s, $\bar{s} \in S$ and t, $\bar{t} \in T$. Since S and T are s.m.'s of M, $x - y = s + t - (\bar{s} + \bar{t}) = s - \bar{s} + t - \bar{t} \in S + T$. Finally, let $r \in R$. Then $r(s + t) = rs + rt \in S + T$. Hence S + T is a s.m. of M.

For S, a s.m. of M, let $M/_S$ denote the factor group of M. Then $^M/_S$ is a unitary R-module where the module operation is defined by $r(m + S) = rm + S$. The natural homomorphism $f:M \longrightarrow {}^M/_S$ given by $f(m) = m + S$ is a module epimorphism. For we know that f is a group epimorphism and if $r \in R$ and $m + S \in {}^M/_S$, then $f(rm) = rm + S = r(m + S) = rf(m)$. $^M/_S$ is called the <u>quotient</u> <u>unitary</u> <u>R-module</u> of M by S.

We now consider some fundamental properties of homomorphisms.

<u>Theorem</u> 2.1 Let $h:M \longrightarrow N$ be an epimorphism where M and N are unitary R-modules. Let ker h = K. Then K is a s.m. of M and $^M/K \cong N$.

Proof: Define $g:{}^M/_K \longrightarrow N$ by $g(m + K) = h(m)$. g is well defined, for if $x + K = y + K$ in $^M/_K$, then $x - y \in K$. So $h(x - y) = 0$ implies that $h(x) = h(y)$ which implies that $g(x + K) = g(y + K)$. g is onto because if $z \in N$, there exists $m \in M$ such that $h(m) = z$. Thus there exists $m + K$ in $^M/_K$ such that $g(m + K) = h(m) = z$ in N. Next, g is a homomorphism. For if x + K, y + K are in $^M/_K$ and r, $s \in R$, then $g(r(x + K) + s(y + K)) = g((rx + K) + (sy + K)) = g((rx + sy) + K) =$

$h(rx + sy) = rh(x) + sh(y) = rg(x + K) + sg(y + K)$. Finally, g is 1-1 because $g(x + K) = g(y + K)$ implies $h(x) = h(y)$ which implies $h(x) - h(y) = 0$. Thus $h(x - y) = 0$ and $x - y \in K$. That is, $x + K = y + K$. Thus g is an isomorphism and $M/_K \cong N$.

Theorem 2.2 For unitary R-modules M and N, let $h:M \longrightarrow N$ be an epimorphism. Let H be a s.m. of N. Then $h^{-1}[H] = K$ is a s.m. of M and $M/_K \cong N/H$.

Proof: By lemma 2.1, K is a s.m. of M. Let $f:N \longrightarrow N/_H$ be the natural homomorphism where $f(n) = n + H$. Define $g:M \longrightarrow N/_H$ by $g = f\circ h$. g is an epimorphism because f and h are epimorphisms. Now $\ker g = \{ x \in M \mid h(x) \in H\} = \{x \mid x \in h^{-1}[H]\} = \{x \mid x \in K\} = K$. Finally, by theorem 2.1 $M/K \cong N/H$.

Alternatively, this theorem may be restated:

Let $h:M \longrightarrow N$ be an epimorphism and K any s.m. of M such that $\ker h \subseteq K$. Then $h[K] = H$ is a s.m. of N and $M/_K \cong N/_H$.

Theorem 2.3 Let $U \subseteq S \subseteq T$ be submodules of the module M. Then S is a s.m. of T, $S/_U$ is a s.m. of $T/_U$, and $T/_U\Big/S/_U \cong T/_S$.

Proof: It is clear that S is a s.m. of T. Let $h:T \longrightarrow T/_U$ be the natural homomorphism. Then $\ker h = U \subseteq S$. Moreover $h[S] = S/_U$ is a s.m. of $T/_U$. So by theorem 2.2, $T/_S \cong T/_U\Big/S/_U$.

Theorem 2.4 If S and T are s.m.'s of a module M. Then

i) $S + T$ is a s.m. of M containing T as a s.m.

ii) $S \cap T$ is a s.m. of S.

iii) $(S + T)/_T \cong S/(S \cap T)$.

Proof: i) and ii) are clear by lemma 2.2.

iii) Clearly ${}^{(S + T)}/_{T}$ is a module. Define $h: S \longrightarrow {}^{(S + T)}/_{T}$ by $h(s) = s + T$. Let $(s + t) + T \in {}^{(S + T)}/_{T}$. Now $t \in T$ implies that $(s + t) + T = s + T$ and $h(s) = s + T$. Thus $h[S] \subseteq {}^{(S + T)}/_{T}$ and h is onto. Next, let $s, \bar{s} \in S$ and $r, \bar{r} \in R$. Then $h(rs + \bar{r}\bar{s}) = (rs + \bar{r}\bar{s}) + T = (rs + T) + (\bar{r}\bar{s} + T) = r(s + T) = \bar{r}(\bar{s} + T) = rh(s) + \bar{r}h(\bar{s})$. Thus h is an epimorphism. Now $\ker h = \{ x \in S \mid x + T = T \} = \{ x \in S \mid x \in T \} = S \cap T$. Thus by theorem 2.1 ${}^{S}/_{(S \cap T)} \cong {}^{(S + T)}/_{T}$.

Definition 2.5 Let M be a unitary R-module. Let $x_1, \ldots, x_n \in M$. Then M is generated by $x_1, \ldots, x_n$ if, for every $y \in M$ there exists $r_1, \ldots, r_n \in R$ such that $y = \sum_{i=1}^{n} r_i x_i$. $\{ x_1, \ldots, x_n \}$ is called a basis for M over R if $\{ x_1, \ldots, x_n \}$ generates M and whenever $0 = \sum_{i=1}^{n} r_i x_i$, then $r_i x_i = 0$ for $i = 1, \ldots, n$. If $\{ x_1, \ldots, x_n \}$ is a basis for M over R, we define the length of M, denoted $\ell(M)$, to be n. If $x_1, \ldots, x_n$ is a basis for M and if whenever $\sum_{i=1}^{n} r_i x_i = 0$, then $r_i = 0$ for $i = 1, \ldots, n$, then $\{ x_1, \ldots, x_n \}$ is called a free basis for M.

Examples:

1. In example No. 1 on page 5, if $M = \mathbb{Z}/(8)$, then $\mathbb{Z}/(8)$ is a unitary $\mathbb{Z}$-module and $\{ 1 \}$ is a basis for $\mathbb{Z}/(8)$ over $\mathbb{Z}$. Thus $\ell(\mathbb{Z}/(8)) = 1$.

2. Let M = E, the even integers, and $R = \mathbb{Z}$. Then E is a unitary $\mathbb{Z}$ - module with basis $\{ 2 \}$. So $\ell(E) = 1$.

3. Let V(F) be a finite dimensional vector space over a field F with dimension, n. Let $\{ x_1, \ldots, x_n \}$ be a basis for V over F.

Then $\{ x_1, \ldots, x_n \}$ is a basis for V considered as a unitary F-module and $\ell(V) = n$.

4. For indeterminants $x_1, \ldots x_n$, let $M = \{ \sum_{i=1}^{n} r_i x_i \mid r_i \in R,$ $i = 1, \ldots, n, n \in \mathbb{N} \}$. Define:

1. $\sum_{i=1}^{n} r_i x_i = \sum_{i=1}^{n} s_i x_i$ if $r_i = s_i$ for all i.
2. $\sum_{i=1}^{n} r_i x_i + \sum_{i=1}^{n} s_i x_i = \sum_{i=1}^{n} (r_i + s_i) x_i$
3. $1 \cdot x_i = x_i$ and $0 \cdot x_i = 0$ for all i.
4. $s(\sum_{i=1}^{n} r_i x_i) = \sum_{i=1}^{n} (sr_i) x_i$ for all $s \in R$.

Then M is a unitary R-module with basis $\{ x_1, \ldots, x_n \}$. This basis is a free basis for M over R. Moreover, every module with a free basis is isomorphic to a module of this form.

Theorem 2.5 For unitary R-modules M and N, let Hom(M,N) = $\{ h:M \longrightarrow N \mid h \text{ is a homomorphism} \}$. Define module operations in Hom(M,N) as follows: For f, g $\in$ Hom(M,N) and r $\in$ R, let (f + g) (x) = f(x) + g(x) and (rf) (x) = f(rx) for all x $\in$ M. Then Hom(M,N) is a unitary R-module.

Proof: Let f, g, h $\in$ Hom(M,N). Clearly f + g $\in$ Hom(M,N) and (f + g) + h = f + (g + h). Let $O:M \longrightarrow N$ by O(x) = 0 for all x $\in$ M. O is the zero in Hom(M,N). For f $\in$ Hom(M,N), let $j:M \longrightarrow N$ be given by $j(x) = {}^{-}1 \cdot f(x)$ for all x $\in$ M. Then j is the inverse of f with respect to + in Hom(M,N). Finally, rf $\in$ Hom(M,N) for all r $\in$ R. It is easy to check that properties 1 and 2 of definition 2.1 are satisfied. Hence Hom(M,N) is a unitary R-module.

Lemma 2.3 Let M be a module with a free basis, $x_1, \ldots, x_n$. If f, h $\in$ Hom(M,N) are such that $f(x_i) = h(x_i)$ for i = 1, ..., n, then f = h. Moreover, if $\{ a_1, \ldots, a_n \}$ is any subset of N and if

$h(x_i) = a_i$ is a mapping of $\{ x_1, \ldots, x_n \}$ into $\{ a_1, \ldots, a_n \}$, then h extends uniquely to an element in Hom(M,N).

Proof: Suppose $f(x_i) = h(x_i)$ for $i = 1, \ldots, n$. For any $x \in M$, $x = \sum_{i=1}^{n} r_i x_i$. As $f, h \in \text{Hom}(M,N)$, $f(x) = \sum_{i=1}^{n} r_i f(x_i) = \sum_{i=1}^{n} r_i h(x_i) = h(x)$. Hence $f = h$.

If $\{ a_1, \ldots, a_n \}$ is any subset of N and if $h(x_i) = a_i$ for $i = 1, \ldots, n$, extend h by letting $g(x) = \sum_{i=1}^{n} r_i\ h(x_i) = \sum_{i=1}^{h} r_i a_i$ where $x \in M$ is given by $x = \sum_{i=1}^{n} r_i x_i$. g is clearly in Hom(M,N) and this extension is unique by the above.

In referring to this lemma, we will say an element $h \in \text{Hom}(M,N)$ is completely determined by its values on a free basis.

Note that there is a difference between a basis and a free basis. Recall, from example 1 on page 10, that $\mathcal{l}(\mathbb{Z}/_{(8)}) = 1$ and $\{ 1 \}$ is a basis over $\mathbb{Z}$. However, $\{ 1 \}$ is not a free basis because $8 \cdot 1 = 0$ and $8 \neq 0$ in $\mathbb{Z}$. Let x be an indeterminant. Let M = $\{ nx \mid n \in \mathbb{Z} \}$. Then M is a unitary $\mathbb{Z}$-module with basis $\{ x \}$. So $\mathcal{l}(M) = 1$. Now as modules, $M \not\cong \mathbb{Z}/_{(8)}$ because M is infinite while $\mathbb{Z}/_{(8)}$ is finite. Thus for unitary R-modules M and N, $\mathcal{l}(M) = \mathcal{l}(N)$ does not imply that $M \cong N$. However, if M has a basis with n elements and $M \cong N$, then $\mathcal{l}(M) = \mathcal{l}(N)$. Also if M and N both have free bases $\{ x_1, \ldots, x_n \}$ and $\{ y_1, \ldots, y_n \}$ respectively, then $\mathcal{l}(M) = \mathcal{l}(N)$ and $M \cong N$. For let $f \in \text{Hom}(M,N)$ with $f(x_i) = y_i$ for $i = 1, \ldots, n$. Then if $x \in M$ with $f(x) = 0$, there exist $r_1, \ldots, r_n \in R$ such that $f(\sum_{i=1}^{n} r_i x_i) = \sum_{i=1}^{n} r_i f(x_i) = \sum_{i=1}^{n} r_i y_i = 0$. Hence $r_i = 0$ for $i = 1, \ldots, n$ which implies that $x = 0$. Thus $\ker f = \{ 0 \}$. That is, f is an isomorphism.

Definition 2.6 Let M and N be unitary R-modules with free bases $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ respectively. Let $h \in \mathrm{Hom}(M,N)$. Then $h(x_j) = \sum_{i=1}^{n} a_{ij} y_i$ where $a_{ij} \in R$, $i = 1, \ldots, n$, and $j = 1, \ldots, m$. That is, h determines a rectangular array of nm elements $a_{ij} \in R$. This array $A_h = (a_{ij})$ is called the matrix of h with respect to the free bases $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$.

Note that $a_{1j}, \ldots, a_{nj}$ are uniquely determined by $h(x_j)$ for $j = 1, \ldots, m$. So each $h \in \mathrm{Hom}(M, N)$ determines an unique rectangular array, A_h, of elements of R. Conversely, let $A = (a_{ij})$ $i = 1, \ldots, n$, $j = 1, \ldots, m$ be any array of nm elements of R. Define $h_A : M \longrightarrow N$ by $h_A(x_j) = \sum_{i=1}^{n} a_{ij} y_i$. Then $h_A \in \mathrm{Hom}(M,N)$ and is uniquely determined by lemma 2.3, because $\{h(x_1), \ldots, h(x_m)\} \subseteq N$. So each array, A, of nm elements of R determines an unique element $h_A \in \mathrm{Hom}(M,N)$.

Let $M_{nm}(R) = \{ (a_{ij}) \mid a_{ij} \in R, i = 1, \ldots, n, j = 1, \ldots, m \}$ where R is commutative with identity 1.

Theorem 2.6 Using the notation above, $h \longrightarrow A_h$ and $A \longrightarrow h_A$ are inverse 1-1 correspondences between $M_{nm}(R)$ and $\mathrm{Hom}(M,N)$. That is, $h_{A_h} = h$ and $A_{h_A} = A$.

Proof: $h_A(x_j) = \sum_{i=1}^{n} a_{ij} y_i$, $j = 1, \ldots, m$, where $A = (a_{ij})$. Thus $A_{h_A} = (a_{ij}) = A$. Conversely, let $A_h = (a_{ij})$ where $h(x_j) = \sum_{i=1}^{n} a_{ij} y_i$. Then $h_{A_h}(x_j) = \sum_{i=1}^{n} a_{ij} y_i$. By lemma 2.3, $h = h_{A_h}$.

We now define operations on $M_{nm}(R)$ so that $M_{nm}(R)$ becomes an R-module and the correspondence above becomes a module isomorphism. Let $f \longrightarrow (a_{ij})$ and $g \longrightarrow (b_{ij})$. Then $f(x_j) = \sum_{i=1}^{n} a_{ij} y_i$ and

$g(x_j) = \sum_{i=1}^{n} b_{ij}y_i$. Now $(f + g)\ (x_j) = f(x_j) + g(x_j) = \sum_{i=1}^{n}(a_{ij} + b_{ij})y_i = \sum_{i=1}^{n} c_{ij}y_i$ where $c_{ij} = a_{ij} + b_{ij}$. Then $f + g \longrightarrow (c_{ij})$. (c_{ij}) will be called the sum of (a_{ij}) and (b_{ij}), denoted by $(a_{ij}) + (b_{ij})$. Now let $r \in R$. Define $r(a_{ij}) = (ra_{ij})$. It is clear that these module operations are preserved by the 1-1 correspondence $h \longrightarrow A_h$. Since Hom(M,N) is a unitary R-module, so is $M_{nm}(R)$ and Hom(M,N) $\cong M_{nm}(R)$ as R-modules.

Theorem 2.7 Let M and N be R-modules. Suppose M has a free basis $\{ x_1, \ldots, x_m \}$ and N has a basis $\{ y_1, \ldots, y_n \}$. For each $j = 1, \ldots, m$ and each $i = 1, \ldots, n$, define $h_{ij}: M \longrightarrow N$ by $h_{ij}(x_K) =$

$$\begin{cases} 0 \text{ if } K \neq j \ . \\ y_i \text{ if } K = j \end{cases}$$

Then $h_{ij} \in$ Hom(M,N) and $\{ h_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m \}$ is a basis for Hom(M,N). Thus ℓ(Hom(M,N)) = nm. If, in addition, $\{ y_1, \ldots, y_n \}$ is a free basis for N, then $\{ h_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m \}$ is a free basis for Hom(M,N).

Proof: First note that $h_{ij} \in$ Hom(M,N) by lemma 2.3. To show that $\{ h_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m \}$ generates Hom(M,N), let $g \in$ Hom(M,N). We know that $g(x_j) = \sum_{i=1}^{n} a_{ij}y_i$ where $a_{ij} \in R$. Thus $g = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}h_{ij})$, because $g(x_K) = \sum_{i=1}^{n} a_{iK}y_i = \sum_{i=1}^{n} a_{iK}h_{iK}(x_K) = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}h_{ij})\ (x_K) = (\sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}h_{ij}))\ (x_K)$. Therefore $\{ h_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m \}$ generates Hom(M,N). Let $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}h_{ij} = 0$. Then for $K = 1, \ldots, m$, $0 = (\sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}h_{ij}))\ (x_K) = \sum_{i=1}^{n} a_{iK}h_{iK}(x_K) = \sum_{i=1}^{n} a_{iK}y_i$, and $a_{iK}y_i = 0$ for $i = 1, \ldots, n$ because $\{ y_i \}$ is a basis for N. Thus $a_{iK}h_{iK}(x_K) = 0$ for $i = 1, \ldots, n$ and $k = 1, \ldots, m$. This implies that $a_{ij}h_{ij}(x_K) = 0$ for $i = 1, \ldots, n$ and $j, k = 1, \ldots, m$

and hence that $a_{ij} h_{ij} = 0$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$.

Therefore $\{ h_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, m \}$ is a basis for Hom(M,N). If $\{ y_i \}$ is a free basis for N, then $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} h_{ij} = 0$ implies that $a_{ik} = 0$ for $i = 1, \ldots, n$ and $k = 1, \ldots, m$. Thus $\{ h_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, m \}$ is a free basis for Hom(M,N). There are nm such h_{ij}. In either case $\ell(\mathrm{Hom}(M,N)) = nm$.

We remark that if $\ell(M) = m$, then $\ell(\mathrm{Hom}(M,M)) = m^2$ and $\ell(\mathrm{Hom}\ (M,R)) = m$. For, as an R-module, $\ell(R) = 1$. Note also that since $M_{nm}(R) \cong \mathrm{Hom}(M,N)$ as R-modules when both M and N have free bases, then $M_{nm}(R)$ has a free basis defined as follows: let $E_{ij} = (e_{rs})$ where $e_{rs} = 0$ if $r \neq i$ and $s \neq j$, and $e_{ij} = 1$ for $i = 1, \ldots, n$, $j = 1, \ldots, m$. To see that $\{ E_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, m \}$ is a free basis for $M_{nm}(R)$, observe that E_{ij} is the matrix of h_{ij} .

The basis elements $h_i \in \mathrm{Hom}(M,R)$ are given by $h_i(x_k) = 0$ if $k \neq i$ and $h_i(x_i) = 1$ for $i = 1, \ldots, m$. Using $\{ 1 \}$ as the free basis for R over R and $\{ x_1, \ldots, x_m \}$ as a free basis for M, $\{ h_i \mid i = 1, \ldots, m \}$ is a free basis for Hom(M,R) and $M \cong \mathrm{Hom}\ (M,R)$ by the mapping $f(x_i) = h_i$.

Extending one step further, if $x \in M$ is fixed, the mapping $f_x : \mathrm{Hom}(M,R) \longrightarrow R$ given by $f_x(h_i) = h_i(x)$ is in Hom(Hom(M,R),R),by lemma 2.3, with the free basis $\{ f_{x_i} \mid i = 1, \ldots, m \}$. Also $M \cong \mathrm{Hom}(\mathrm{Hom}(M,R), R)$ by the mapping $g(x_i) = f_{x_i}$.

<u>Theorem</u> 2.8 Let M,N, and T be R-modules with free bases $\{ x_1, \ldots, x_m \}$, $\{ y_1, \ldots, y_n \}$, and $\{ z_1, \ldots, z_p \}$ respectively. Let $f \in \mathrm{Hom}(M,N)$ and $g \in \mathrm{Hom}(N,T)$ have matrices $A = (a_{ij})$ and $B = (b_{ij})$ respectively. Then the composite mapping, g o f, is in

Hom(M,T) and has matrix C = (c_{ij}) where $c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$.

Proof: Let x, y ∈ M and r, s ∈ R. Then (g o f) (rx + sy) = g(f(rx + sy)) = g(rf(x) + sf(y)) = rg(f(x)) + sg(f(y)) implies that g o f ∈ Hom(M,T). Also (g o f) (x_j) = $g(f(x_j))$ = $g(\sum_{k=1}^{n} a_{kj}y_k)$ = $\sum_{k=1}^{n} a_{kj}g(y_k) = \sum_{k=1}^{n} a_{kj}(\sum_{i=1}^{p} b_{ik}z_i) = \sum_{i=1}^{p} (\sum_{k=1}^{n} b_{ik}a_{kj}) z_i = \sum_{i=1}^{p} c_{ij}z_i$ where $c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$. Thus g o f will have matrix C = (c_{ij}).

We call C the product of B and A and write C = BA. Note that if M = N = T, then products in $M_{mm}(R)$ are also preserved by the 1-1 correspondence between Hom(M,M) and $M_{mm}(R)$. That is, if f, g ∈ Hom(M,M) with matrices A and B respectively with respect to a free basis $\{ x_1, \ldots, x_m \}$, then g o f corresponds to the matrix BA by the above. Hence if Hom(M,M) is a ring with respect to this "multiplication", $M_{mm}(R)$ is also a ring and Hom(M,M) ≅ $M_{mm}(R)$ as rings.

Henceforth we will consider the case where N = M. We will write H(M) for Hom(M,M). Also for n = m we will write $M_n(R)$ for $M_{nn}(R)$ where R is an arbitrary commutative ring with identity. The word basis will be understood to mean a free basis. All modules will be understood as having a free basis.

Theorem 2.9 $M_n(R)$ and H(M) are rings with identity and $M_n(R)$ ≅ H(M) as rings.

Proof: The operations in H(M) are + and composition o. We know that H(M) is an R-module and thus (H(M) +) is an abelian group. Let f, g, h H(M). Let x ∈ M. Then o is associative, for (f o(g o h)) (x) = f((g o h) (x)) = f(g(h(x))) = (f o g) (h(x)) = ((f o g)o h) (x).

Similarly, $f \circ (g + h)\ (x) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = (f \circ g)\ (x) + (f \circ h)\ (x)$ implies that the left distributive law holds. In like manner the right distributive law holds. Thus H(M) is a ring. Let $i:M \longrightarrow M$ by $i(x) = x$ for all $x \in M$. Then i is the identity map in H(M). Thus H(M) is a ring with identity. Finally, by the preceeding remarks, $H(M) \cong M_n(R)$ as rings, so $M_n(R)$ is a ring with identity. i will correspond to $I = (\delta_{ij}) \in M_n(R)$ where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ii} = 1$.

Definition 2.7 $M_n(R)$ is called the complete matrix ring over R.

Thus far we can see similarities between H(M) and the set of linear transformations of a vector space V over a field F. For example, in M the free basis corresponds to the notion of a basis in the vector space, length to dimension, submodule to subspace, and quotient module to quotient space.

CHAPTER III

RELATIONSHIPS BETWEEN A RING AND ITS COMPLETE MATRIX RING

In this chapter we seek relationships between a commutative ring R with 1 and its complete matrix ring $M_n(R)$. In particular, we seek to find properties of R which are inherited by $M_n(R)$.

Definition 3.1 Let R be any ring. The center of R, $\mathcal{Z}(R)$, is the set, $\{ s \in R \mid sr = rs \text{ for all } r \in R \}$.

Lemma 3.1 $\mathcal{Z}(R)$ is a subring of R.

Proof: As $0 \in \mathcal{Z}(R)$, $\mathcal{Z}(R) \neq \emptyset$. Let $x, y \in \mathcal{Z}(R)$. Then $xr = rx$ and $yr = ry$ for all $r \in R$. So $r(x - y) = rx - ry = xr - yr = (x - y)r$ implies that $x - y \in \mathcal{Z}(R)$. Also $(xy)r = x(yr) = x(ry) = (xr)y = (rx)y = r(xy)$ implies that $xy \in \mathcal{Z}(R)$. Thus $\mathcal{Z}(R)$ is a subring of R.

Definition 3.2 An ideal M of a ring R is a maximal ideal of R if $M \neq R$ and whenever there exists an ideal J of R such that $M \subseteq J \subseteq R$, then $J = M$ or $J = R$.

Definition 3.3 An ideal P of a ring R is a prime ideal of R if, whenever A and B are ideals of R, $AB \subsetneq P$ implies $A \subseteq P$ or $B \subseteq P$. A ring R is a prime ring if, whenever A and B are ideals of R with $AB = 0$, then $A = 0$ or $B = 0$.

It is easily seen that when R is a commutative ring, the usual definition for a prime ideal of R (J is a prime ideal of R if whenever $ab \in J$, then $a \in J$ or $b \in J$) is equivalent to the one above. For suppose that $ab \in J$ implies that $a \in J$ or $b \in J$. Let A, B be ideals of R with AB $\subseteq$ J. Then ab $\in$ J for all a $\in$ A and b $\in$ B. If A $\not\subseteq$ J, let a $\in$ A - J. Then as a $\notin$ J, ab $\in$ J for all b $\in$ B implies b $\in$ J for all b $\in$ B. Thus B $\subseteq$ J. Conversely, suppose that for all ideals A and B of R, AB $\subseteq$ J implies A $\subseteq$ J or B $\subseteq$ J. Let a, b $\in$ R with ab $\in$ J. Then if A = $\langle a \rangle$, and B = $\langle b \rangle$, AB = $\langle a \rangle \langle b \rangle$ = $\langle ab \rangle \subseteq$ J. If a $\notin$ J, then $\langle a \rangle \not\subseteq$ J. Thus $\langle b \rangle \subseteq$ J and hence b $\in$ J.

Definition 3.4 A ring R is simple if R has at least two elements and if the only ideals of R are R and $\langle 0 \rangle$.

Clearly any division ring is simple.

We now make a few easy observations about $M_n(R)$.

I If a commutative ring R does not have the zero multiplication, then $M_n(R)$ is non-commutative for n $\geqslant$ 2.

Proof: It is sufficient to give an example for the case n = 2. Let a, b $\in$ R with ba $\neq$ 0. Then $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, whereas

$$\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ba \\ 0 & 0 \end{pmatrix} .$$

Definition 3.5 An element 0 $\neq$ a of a ring R is a zero divisor if there exists 0 $\neq$ b $\in$ R such that ab = 0.

II If R is not the zero ring and R is commutative, then $M_n(R)$ has zero divisors for n $\geqslant$ 2.

Proof: Let a $\in$ R with a $\neq$ 0. Then $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

III A commutative ring R has 1 if and only if $M_n(R)$ has identity I and, in this case, I = (δ_{ij}).

Proof: Suppose R has 1. Then clearly I = (δ_{ij}) is the identity in $M_n(R)$

Conversely, let I = $\begin{pmatrix} a & \cdots & a \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a & \cdots & a \end{pmatrix} \in M_n(R)$ be the identity.

Let $(c_{ij}) \in M\ (R)$ such that $c_{ik} = 0$ for $k \neq i$ and $c_{ii} \neq 0$ for $i \leq n$.

Then

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} c_{11} & & 0 \\ & \ddots & \\ 0 & & c_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}c_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn}c_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & & 0 \\ & \ddots & \\ 0 & & c_{nn} \end{pmatrix}$$

Thus $a_{ii}\ c_{ii} = c_{ii}\ a_{ii} = c_{ii}$ for all $i \leq n$ which implies that a_{ii} is an identity in R. Hence R has 1. Finally, $a_{ik}c_{ii} = c_{ik} = 0$ for all $k \neq i$ implies $a_{ik} = 0$ for all $k \neq i$, taking $c_{ii} = 1 \in R$.

Thus I = $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M\ (R)$.

IV For a commutative ring R with 1, the center of $M_n(R)$, $\mathfrak{Z}\,(M_n(R)) = \{ a I \mid a \in R \}$ where I is the identity of $M_n(R)$.

Proof: Let $S = \{ a I \mid a \in R \}$. Let $a I \in S$ and $A \in M_n(R)$. Then $(aI)A = aA = aAI = A(aI)$. Thus $aI \in \mathfrak{Z}\,(M_n(R))$. So $S \subseteq \mathfrak{Z}\,(M_n(R))$,

Conversely, let $A = (a_{ij}) \in \mathfrak{Z}\,(M_n(R))$. Let E_{ij}, i, j, = 1, ..., n be defined by $E_{ij} = (e_{rs})$ where $e_{rs} = 0$ if $r \neq i$, $s \neq j$ and $e_{ij} = 1$. As was shown in Chapter II, $\{ E_{ij} \mid i, j = 1, \ldots, n \}$ is a basis for $M_n(R)$. Then $A\,E_{ij} = E_{ij}A$ for all i, j = 1, ..., n. Hence $a_{js} = 0 = a_{ri}$ for all $s \neq j$, $r \neq i$ and $a_{ii} = a_{jj}$. So $A = cI$ where $c = a_{ii}$ for any i. Thus $\mathfrak{Z}\,(M_n(R)) \subseteq S$.

We shall have occasion to use the following two lemmas.

<u>Lemma</u> 3.2 For a commutative ring R with 1, an ideal M of R is a

maximal ideal of R, if and only if $^R/_M$ is a field.

Proof: Suppose M is a maximal ideal of R. We know that $^R/_M$ is a comm. ring with 1. By definition of M, there exists $a \in R - M$. Consider $\langle a, M \rangle$, the ideal generated by a and M. $M \subsetneq \langle a, M \rangle \subseteq R$. Thus $\langle a, M \rangle = R$. Now $1 \in R$, so there exists $r \in R$ such that $1 = ar + m$ for some $m \in M$. So $1 + M = ar + M = (a + M)\ (r + M)$ which implies that $r + M$ is a multiplicative inverse of $a + M$. Thus the non-zero elements of $^R/_M$ have inverses. Hence $^R/_M$ is a field.

Conversely, let M be an ideal of R with $^R/_M$ a field. Let N be an ideal of R such that $M \subseteq N \subseteq R$. If $M \neq N$, choose $a \in N - M$. Then $a + M \neq M$. Let $b \in R$. As $^R/_M$ is a field, so $(a + M)\ (x + M) = b + M$ is solvable where $x \in R$. That is, $ax + M = b + M$. Thus $ax - b \in M \subset N$ and since $ax \in N$, $b \in N$. Therefore $R = N$. Thus M is a maximal ideal of R.

<u>Lemma</u> 3.3 Let R be any ring and let I be an ideal of R. Then $^R/_I$ is simple if and only if I is a maximal ideal of R.

Proof: Suppose I is a maximal ideal of R. Let $\mathcal{J}$ be an ideal of $^R/_I$. Then there exists an ideal A of R such that $I \subseteq A$ and $\mathcal{J} = {}^A/_I$. I is maximal implies that $A = I$ or $A = R$. But then $\mathcal{J} = (0)$ or $\mathcal{J} = {}^R/_I$. $^R/_I \neq \{ I \}$ since $I \neq R$. Hence $^R/_I$ is simple.

Conversely, let $I \subseteq A \subseteq R$ for some ideal A of R. Then $^A/_I$ is an ideal of $^R/_I$. Now since R/I is simple, $^A/_I = \langle 0 \rangle$ or $^A/_I = {}^R/_I$. If $^A/_I = \langle 0 \rangle$, $A = I$ since otherwise, there exists $a \in A$ with $a \notin I$. Then $a + I \in {}^A/_I$ and $a + I \neq I$. Thus $^A/_I \neq \langle 0 \rangle$. If $^A/_I = {}^R/_I$, then $A = R$ since otherwise, there exists $r \in R - A$. Then $r + I \in {}^A/_I$ implies there exists $a \in A$ such that $r + I = a + I$. But then

$r - a \in I \subseteq A$ and so $r \in A$. $I \neq R$ since $R/_I \neq \{I\}$. Hence I is a maximal ideal of R.

We now characterize simple commutative rings.

Theorem 3.1 A commutative ring R is simple if and only if R is a field or (R, +) is a cyclic group of prime order and R has the zero multiplication.

Proof: If R is a field, it is easily seen that R is a commutative simple ring. For if I is an ideal of R with $I \neq \langle 0 \rangle$, there exists $a \neq 0$ in I. As $a^{-1} \in R$, $1 = a\, a^{-1} \in I$. Hence I = R.

Alternatively, if (R, +) is a cyclic group of prime order and R has the zero multiplication, let (R, +) have order p. R is clearly commutative. Suppose I is an ideal of R. If $I \neq \langle 0 \rangle$, there is $0 \neq a \in I$. Since (R, +) has prime order p, a is a generator for (R, +) and so R = I. Thus R is a simple commutative ring.

Conversely, let $a \in R$. Let $Ra = \{ ra \mid r \in R \}$. Clearly $o \in Ra$. Let $xa, ya \in Ra$. Now $xa - ya = (x - y)a \in R$ since $x - y \in R$. If $b \in R$, $b(xa) = (bx)a \in Ra$ and $(xa)b = (xb)a \in Ra$. Thus Ra is an ideal of R. As R is simple, $Ra = \langle 0 \rangle$ or Ra = R. Let I = $\{ a \in R \mid Ra = 0 \}$. $I \neq \emptyset$ since $0 \in I$. Let $a, b \in I$. Then $r(a - b) = ra - rb = 0$ for all $r \in R$. Hence $a - b \in I$. Also $s(ra) = (sr)a = 0$ for all $s \in R$. So $ra \in I$. Hence I is an ideal of R. Again $I = \langle 0 \rangle$ or I = K.

Case 1. If $I = \langle 0 \rangle$, then for every $a \neq 0$ in R we have $Ra \neq 0$ implies Ra = R. Thus xa = b is solvable for all $a \neq 0$, and $b \in R$. So for every $a \neq 0$, there exists $x_a \in R$ such that $x_a a = a$. Let $a \neq 0$ and b be in R. Then there exists $y \in R$ with ya = b. Therefore

$x_a b = x_a ya = ya = b$. That is, $x_a b = b$ for any $b \in R$. Hence $x_a = 1$ is an identity for R. Now $xa = 1$ is solvable for all $a \neq 0$. So each $a \neq 0$ has an inverse in R. Thus R is a field.

Case 2. If I = R, then for every $a \in R$, $Ra = 0$ by definition of I. As R is simple, there is $0 \neq a \in R$. $\langle a \rangle = Ra + \mathbb{Z}a = \mathbb{Z}a$. Also $a \neq 0$ implies $\langle a \rangle \neq \langle 0 \rangle$. So $\langle a \rangle = R$. Now consider $\langle 2a \rangle$. If $2a = 0$, then the order of a is 2 and (R,+) is cyclic of order 2. If $2a \neq 0$, then $\langle 2a \rangle = \langle a \rangle$ implies $n2a = a$ for some $n \in \mathbb{Z}$. So $(2n - 1)a = 0$ implies a has a finite additive order. Thus (R, +) is cyclic of finite order. Let m be the order of a. If m is not prime, then $m = rp$ where p is prime and $r < m$. Then $ra \neq 0$ and $pra = ma = 0$. So ra has order p. Now $\langle ra \rangle \neq \langle 0 \rangle$ implies $\langle ra \rangle = R$. Hence (R, +) has p elements and is cyclic or prime order p.

Thus we see that the only simple commutative rings are fields and rings, $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ where p is a prime integer with the zero multiplication.

We now take a look at the ideal structure of $M_n(R)$ where R is a commutative ring with 1.

<u>Theorem</u> 3.2 If S is an ideal of R, then $M_n(S)$ is an ideal of $M_n(R)$. Conversely, if $\mathcal{L}$ is an ideal of $M_n(R)$, then there exists an ideal S of R such that $\mathcal{L} = M\ (S)$.

Proof: Let S be an ideal of R. Then S is a ring and so $M_n(S)$ is a ring. Let $(r_{ij}) \in M_n(R)$ and $(a_{ij}) \in M_n(S)$. Then $(r_{ij})\ (a_{ij}) = (c_{ij})$ where $c_{ij} = \sum_{k=1}^{n} r_{ik} a_{kj} \in S$ since $r_{ik} a_{kj} \in S$. Thus $(c_{ij}) \in M_n(S)$. Similarly $(a_{ij})\ (r_{ij}) \in M_n(S)$. Hence M (S) is an ideal of M (R).

Conversely, let $S = \{ a \in R \mid$ there exists $(a_{ij}) \in \mathcal{L}$ with $a_{11} = a \}$. $S \neq \phi$ as $0 \in S$. Let $a, b \in S$. Then there are (a_{ij}) and $(b_{ij}) \in \mathcal{L}$ with $a_{11} = a$, $b_{11} = b$. Now $(a_{ij}) - (b_{ij}) \in \mathcal{L}$ and $c_{11} = a_{11} - b_{11} = a - b$ implies $a - b \in S$. Let $r \in R$. Choose $A = (a_{ij}) \in \mathcal{L}$ with $a_{11} = a$. Let $E_{ij} = (e_{rs})$ where $e_{rs} = 0$ if $i \neq r$, $j \neq s$ and $e_{ij} = 1$. Clearly $E_{ij} \in M_n(R)$. Since $\mathcal{L}$ is an ideal, $(rE_{11})A \in \mathcal{L}$. Also $rE_{11}\,A = (c_{ij})$ where $c_{ij} = \sum_{K=1}^{n} re_{iK}\,a_{Kj} = ra_{1j}$ if $i = 1$ and 0 otherwise. Hence $ra = ra_{11} = c_{11} \in S$. Similarly $ar \in S$. Thus S is an ideal of R. To show $M_n(S) = \mathcal{L}$, let $(a_{ij}) \in \mathcal{L}$.

Now for $1 \leqslant r, s \leqslant n$, $E_{1r}(a_{ij})\,E_{s1} = E_{1r}(\sum_{i,j=1}^{n} a_{ij}\,E_{ij})E_{s1} = \sum_{i,j=1}^{n} a_{ij}\,(E_{1r}\,E_{ij}\,E_{s1}) = a_{rs}\,E_{1r}\,E_{rs}\,E_{s1} = a_{rs}\,E_{11} \in \mathcal{L}$. Hence we have $a_{rs} \in S$ for all $r, s \leqslant n$. Since r, s are arbitrary, $(a_{ij}) \in M_n(S)$. Hence $\mathcal{L} \subseteq M_n(S)$.

Now let $(a_{ij}) \in M_r(S)$. By the definition of S, for every $p, q \leqslant n$, there is $(b_{ij}) \in \mathcal{L}$ with $a_{pq} = b_{11}$. So $E_{p1}\,(b_{ij})\,E_{1q} = b_{11}\,E_{pq} \in \mathcal{L}$. Then $a_{pq}\,E_{pq} \in \mathcal{L}$ for all p.q. But then $(a_{ij}) = \sum_{p,q=1}^{n} a_{pq}\,E_{pq} \in \mathcal{L}$ since $\mathcal{L}$ is an ideal. Thus $M_n(S) \subseteq \mathcal{L}$. Hence $\mathcal{L} = M\ (S)$.

<u>Corollary</u> 3.2.1 There exists a one-to-one correspondence between the ideals of R and the ideals of $M_n(R)$. This correspondence preserves inclusion; that is, $S \subset P \subset R$ if and only if $M_n(S) \subset M_n(P) \subset M_n(R)$. Moreover, maximal and prime ideals correspond to maximal and prime ideals respectively.

Proof: Let $\mathcal{L}$ be the set of ideals of R and $\mathcal{M}$ be the set of ideals of $M_n(R)$. Define $f: \mathcal{I} \longrightarrow \mathcal{M}$ by $f(S) = M_n(S)$. Define $g: \mathcal{M} \longrightarrow \mathcal{I}$ by $g(\mathcal{J}) = S$ where S is an ideal of R and $M_n(S) = \mathcal{J}$. Clearly f and g are well defined. Now $(g \circ f): \mathcal{I} \longrightarrow \mathcal{I}$ and $(g \circ f)\ (S) = g\left[M_n(S)\right] = S$. So $g \circ f$ is the identity mapping on $\mathcal{I}$. Similarly, $(f \circ g): \mathcal{M} \longrightarrow \mathcal{M}$ and $(f \circ g)\ (\mathcal{J}) = f[S] = M_n(S) = \mathcal{J}$. Thus $f \circ g$ is the identity mapping on $\mathcal{M}$. Hence f and g are inverse correspondences.

Clearly if $S \subset P$ are ideals of R, $M_n(S) \subset M_n(P)$. Conversely let $M_n(S) \subset M_n(P)$ be ideals of $M_n(R)$. Let $a \in S$. Take $(a_{ij}) \in M_n(S)$ such that $a_{ij} = a$ if $i = 1 = j$ and 0 otherwise. Then $(a_{ij}) \in M_n(P)$ implies $a_{ij} \in P$ for all i, j implies $a \in P$. Hence $S \subset P$ and f and g preserve inclusion.

From this we can see that maximal ideals correspond to maximal ideals. For if P is maximal in R and $\mathcal{J}$ is any ideal of $M_n(R)$ with $M_n(P) \subset \mathcal{I} \subset M_n(R)$, then by theorem 3.2, there exists an ideal J of R such that $\mathcal{J} = M_n(J)$. P maximal implies $J = P$ or $J = R$. Hence $M_n(J) = M_n(P)$ or $M_n(J) = M_n(R)$ implies $M_n(P)$ is maximal.

Conversely, let $M_n(P)$ be a maximal ideal of $M_n(R)$. Let J be an ideal of R with $P \subseteq J \subseteq R$. By corollary 3.2.1, we have $M_n(P) \subseteq M_n(J) \subseteq M_n(R)$. $M_n(P)$ maximal implies $M_n(J) = M_n(P)$ or $M_n(J) = M_n(R)$. Thus $J = P$ or $J = R$ implies that P is maximal.

Also, prime ideals correspond to prime ideals. For let P be a prime ideal of R and suppose $M_n(T)\ M_n(S) \subseteq M_n(P)$ where T and S are ideals of R. Suppose $M_n(S) \nsubseteq M_n(P)$. Choose $A \in M_n(S) - M_n(P)$. Let a_{rs} be an entry of A with $a_{rs} \notin P$. Let $b \in T$ be arbitrary. Then $bE_{11} \in M_n(T)$ and $a_{rs}E_{11} = E_{1r}AE_{s1} \in M_n(S)$. Hence $a_{rs}bE_{11} \in M_n(P)$.

Thus $a_{rs} b \in P$ and $b \in P$. This says that $T \subseteq P$ and hence that $M_n(T) \subseteq M_n(P)$. That is, $M_n(P)$ is a prime ideal of $M_n(R)$.

Conversely, let $M_n(P)$ be a prime ideal of $M_n(R)$. Let $a, b \in R$ with $ab \in P$. Choose $A = aI$ and $B = bI$ in $M_n(R)$. Elements in $\langle A \rangle$ and $\langle B \rangle$ have the form $\sum_{i=1}^{r} A_i aIC_i$ and $\sum_{j=1}^{s} B_j bID_j$ where A_i, C_i, B_j, D_j $\in M_n(R)$. Then $(\sum_{i=1}^{r} A_i aIC_i)(\sum_{j=1}^{s} B_j bID_j) = ab(\sum_{i=1}^{r} A_i C_i)(\sum_{j=1}^{s} B_j D_j)$ $\in M_n(P)$ because $ab \in P$. As $M_n(P)$ is a prime ideal $\langle A \rangle \langle B \rangle \subseteq M_n(P)$ and thus $\langle A \rangle \subseteq M_n(P)$ or $\langle B \rangle \subseteq M_n(P)$. Hence $a \in P$ or $b \in P$ and P is a prime ideal of R.

Corollary 3.2.2 Let R be a commutative ring with 1. Then R is simple if and only if $M_n(R)$ is simple. Hence $M_n(R)$ is simple if and only if R is a field.

Proof: Suppose R is simple. Let $\mathcal{J}$ be an ideal of $M_n(R)$. By theorem 3.2 there exists an ideal S of R with $\mathcal{J} = M\ (S)$. If $S = \{0\}$, then $\mathcal{J} = \{0\}$, and if $S = R$, then $\mathcal{J} = M\ (R)$. Hence $M_n(R)$ is simple.

Conversely, suppose $M_n(R)$ is simple and let S be an ideal of R. Again by theorem 3.2, $M_n(S)$ is an ideal of $M_n(R)$. If $M_n(S) = \{0\}$, then $S = \{0\}$, and if $M_n(S) = M_n(R)$, then $S = R$. Hence R is simple.

Definition 3.6 Let R be a ring with 1. An R-module A is called Noetherian if every submodule is finitely generated over R. That is, for every s.m. S of A, there are elements $x_1, x_2, \ldots, x_m$ of S such that for every $x \in S$, $x = \sum_{i=1}^{m} r_i x_i$ where $r_i \in R$. A ring R is (left) Noetherian provided it is Noetherian considered as a module over itself. That is, every left ideal is finitely generated.

For a commutative ring R with 1, if $M_n(R)$ is Noetherian as an

R-module, then $M_n(R)$ is Noetherian considered as a ring. For if $\mathcal{L}$ is any left ideal of $M_n(R)$ then $\mathcal{L}$ is a s.m. of $M_n(R)$ because, for any $r \in R$ and any $B \in \mathcal{L}$, $rB = (rI)B \in \mathcal{L}$ considered as a left ideal. Hence $R\mathcal{L} \subseteq \mathcal{L}$. Then as an R-s.m., there are elements $A_1, \ldots, A_t$ of $\mathcal{L}$ such that for any $A \in \mathcal{L}$, $A = \sum_{i=1}^{t} a_i A_i$ where $a_i \in R$. Pick $B_i \in M_n(R)$ so that $B_i = a_i I$ for $i = 1, \ldots, t$. Then $A = \sum_{i=1}^{t} B_i A_i$; that is, $\mathcal{L}$ is finitely generated over $M_n(R)$.

<u>Theorem</u> 3.3 Let R be a commutative ring with 1. Suppose that $M_n(R)$ is left Noetherian considered as a ring. Then R is Noetherian.

Proof: Let S be a left ideal of R. Then $M_n(S)$ is a left ideal of $M_n(R)$. $M_n(R)$ is left Noetherian implies $M_n(S)$ is finitely generated over $M_n(R)$. That is, there are elements $A_1, \ldots, A_m$ of $M_n(S)$ such that for any $A \in M_n(S)$, $A = \sum_{i=1}^{m} B_i A_i$ where $B_i \in M_n(R)$. Now $A = \sum_{p,q=1}^{n} a_{pq} E_{pq} = \sum_{i=1}^{m} \left[\left(\sum_{p,q=1}^{n} b^i_{pq} E_{pq} \right) \left(\sum_{p,q=1}^{n} c^i_{pq} E_{pq} \right) \right] = \sum_{i=1}^{m} \left[\sum_{p,q=1}^{n} \left(\sum_{K=1}^{n} b^i_{pK} c^i_{Kq} \right) E_{pq} \right] = \sum_{p,q=1}^{n} \left[\sum_{i=1}^{m} \left(\sum_{K=1}^{n} b^i_{pK} c^i_{Kq} \right) \right] E_{pq}$ since $E_{pq} E_{rs} = 0$ if $q \neq r$ and $E_{pq} E_{rs} = E_{ps}$ if $q = r$. Thus $a_{pq} = \sum_{i=1}^{m} \sum_{K=1}^{n} b^i_{pK} c^i_{Kq}$. Let $a \in S$. Then $A = aE_{11} \in M_n(S)$ and $a = \sum_{i=1}^{m} \sum_{K=1}^{n} b^i_{1K} c^i_{K1}$. Thus $\{ c^i_{p1} \mid p = 1, \ldots, n;\ i = 1, \ldots, m \}$ generates S over R. Hence R is Noetherian.

<u>Theorem</u> 3.4 Let R be any ring with 1. Let M be a finitely generated R-module. Then if R is Noetherian, M is Noetherian.

Proof: We induct on the number, n, of generators. For $n = 1$, $M \cong R$ by the map $r \longrightarrow ra$ where a is the generator of M. Hence M is Noetherian. Assume the theorem holds for all finitely generated R-modules with less than n generators. Let M be generated by $x_1, \ldots, x_n$. Let M_1 be the s.m. of M generated by $x_1, \ldots, x_{n-1}$. By the induction hypothesis, M_1 and M/M_1 are Noetherian since they have n-1 and 1 generator respectively. Let f be the natural homomorphism mapping M onto $^{M}/_{M_1}$. Let S be any s.m. of M. Then f $[S]$ is a s.m. of $^{M}/_{M_1}$ and so has generators $\bar{y}_1, \ldots, \bar{y}_m$. Choose $y_1, \ldots, y_m$ in S such that $f(y_i) = \bar{y}_i$. Now $S \cap M_1$ is a s.m. of M_1. Since M_1 is Noetherian, $S \cap M_1$ is finitely generated by, say, $z_1, \ldots, z_p$. Let $a \in S$. Then $f(a) = a + M_1 = \sum_{i=1}^{m} a_i \bar{y}_i = \sum_{i=1}^{m} a_i f(y_i) = \sum_{i=1}^{m} a_i (y_i + M_1) = \sum_{i=1}^{m} a_i y_i + M_1$, where $a_i \in R$. Then $a - \sum_{i=1}^{m} a_i y_i \in M_1$. Thus $a - \sum_{i=1}^{m} a_i y_i = \sum_{i=1}^{p} b_i z_i$ where $b_i \in R$. Hence $a = \sum_{i=1}^{m} a_i y_i + \sum_{i=1}^{p} b_i z_i$ and S is finitely generated over R. That is, M is Noetherian.

$M_n(R)$ is an R-module and is finitely generated by $\{ E_{ij} \mid i, j = 1, \ldots, n \}$. So we have that if R is Noetherian, then $M_n(R)$ is Noetherian considered as an R-module and hence as a ring. Also, since $M_n(R)$ is Noetherian as a module implies that $M_n(R)$ is Noetherian as a ring, we have that if $M_n(R)$ is Noetherian as a module, then R is Noetherian. In summary, we state the following theorem, considering $M_n(R)$ as a ring.

Theorem 3.5 R is Noetherian if and only if $M_n(R)$ is Noetherian.

Definition 3.7 A ring R is called a regular ring if for every $a \in R$, there is an $x \in R$ such that $a\,x\,a = a$.

Examples:

1. Any division ring, and hence any field, is regular.

2. Let p be a fixed prime. Let R be any ring with at least two elements such that for every $a \in R$, $a^p = a$ and $pa = 0$. We call such a ring a p-ring. Then any p-ring R is regular. That is, for any $a \in R$, pick $x = a^{p-2}$ if $p > 2$ and $x = a$ if $p = 2$.

Von Neumann stated, in [9], that if a ring R with 1 is regular, then $M_n(R)$ is a regular ring with identity. We do not prove this statement here, but we prove a weaker theorem.

<u>Theorem</u> 3.6 If R is a field, then $M_n(R)$ is a regular ring.

Proof: We will regard $M_n(R)$ as the set of all linear transformations on an n-dimensional vector space V over R. Let $A \neq 0$ be an element of $M_n(R)$. Let $N_A = \{ v \in V \mid A v = 0 \}$ be the null space of A. We know from the theory developed in Chapter II that N_A is a subspace of V. $A \neq 0$ implies that $N_A \neq V$. Let $\mathcal{A} = \{ v_1 , \dots , v_t \}$ be a basis for N_A. We can extend $\mathcal{A}$ to $\mathcal{A} \cup \mathcal{B}$ a basis for V. Let $A[\mathcal{B}] = \{ Av \mid v \in \mathcal{B} \}$. The map $v \longrightarrow Av$ is 1-1, for if $u_1, u_2 \in \mathcal{B}$ are such that $Au_1 = Au_2$, then $Au_1 - Au_2 = A(u_1 - u_2) = 0$ which implies that $u_1 - u_2 \in N_A$. Therefore $u_1 - u_2 = \sum_{i=1}^{t} a_i v_i$ where $a_i \in R$. Now $\sum_{i=1}^{t} a_i v_i - u_1 + u_2 = 0$ implies that $a_i = 0$ for $i = 1, \dots , t$ since $\mathcal{A} \cup \mathcal{B}$ is an independent set. Thus $u_1 = u_2$ and the mapping is 1-1. Further $A[\mathcal{B}]$ has n-t distinct elements. Let $\mathcal{B} = \{ v_{t+1}, \dots , v_n \}$. Then $\sum_{i=t+1}^{n} a_i Av_i = 0$ implies that $\sum_{i=t+1}^{n} Aa_i v_i = A(\sum_{i=t+1}^{n} a_i v_i) = 0$ implies $\sum_{i=t+1}^{n} a_i v_i \in N_A$. Thus $\sum_{i=t+1}^{n} a_i v_i = \sum_{j=1}^{t} b_j v_j$ where $b_j \in R$. So $\sum_{j=1}^{t} b_j v_j - \sum_{i=t+1}^{n} a_i v_i = 0$ implies $b_j = 0 = a_i$ for $j = 1, \dots , t$, $i = t + 1, \dots , n$, because $\mathcal{A} \cup \mathcal{B}$ is an independent set. Hence $A[\mathcal{B}]$ is an independent set. We can extend $A[\mathcal{B}]$ to $A[\mathcal{B}] \cup \mathcal{D}$ a basis for V. Choose the mapping $\bar{A} \in M_n(R)$ given by $\bar{A}(Av_i) = v_i$ for $i = t + 1, \dots , n$ and $\bar{A}(v) = v$ for $v \in \mathcal{D}$. Then $(A\bar{A}A)v_i = A(\bar{A}Av_i) = Av_i$ for every $v_i \in \mathcal{B}$ and $(A\bar{A}A)v_j = A\bar{A}(0) = 0 = Av_j$ for every $v_j \in \mathcal{A}$. Since $A\bar{A}A$ and A have the same effect on all basis elements v_i of $\mathcal{A} \cup \mathcal{B}$ for V, we have that $A\bar{A}A = A$. Hence $M_n(R)$ is a regular ring.

We conclude this chapter with an examination of radical properties of a ring and its complete matrix ring. Throughout our discussion of radicals, all rings have 1.

<u>Definition</u> 3.8 Let $\mathcal{C}$ be a class of rings that is closed under isomorphism. For any ring R, let $N_{\mathcal{C}}(R) = \{ J \mid J$ is an ideal of R and $R/J \in \mathcal{C} \}$. $N_{\mathcal{C}}(R)$ is called the <u>$\mathcal{C}$-radical</u> of R. R is called $\mathcal{C}$-semi-simple if $N_{\mathcal{C}}(R) = 0$. If R has an ideal J such that $R/J \in \mathcal{C}$, then $N_{\mathcal{C}}(R)$ is an ideal of R. Moreover, $R/N_{\mathcal{C}}(R)$ is $\mathcal{C}$-semi-simple since $N_{\mathcal{C}}(R/N_{\mathcal{C}}(R)) = 0$. To see this, recall that if $\mathcal{J}$ is an ideal of $R/N_{\mathcal{C}}(R)$, then $\mathcal{J} = J/N_{\mathcal{C}}(R)$ for some ideal J of R such that $N_{\mathcal{C}}(R) \subseteq J$. $\dfrac{R/N_{\mathcal{C}}(R)}{J/N_{\mathcal{C}}(R)} \cong R/J \in \mathcal{C}$ implies $N_{\mathcal{C}}(R/N_{\mathcal{C}}(R)) = \bigcap \{ J/N_{\mathcal{C}}(R) \mid N_{\mathcal{C}}(R) \subseteq J$ and $R/J \in \mathcal{C} \} =$ $\bigcap \{ J \mid R/J \in \mathcal{C} \} \big/ N_{\mathcal{C}}(R) = N_{\mathcal{C}}(R)/N_{\mathcal{C}}(R) = 0$.

<u>Definition</u> 3.9 For any ring R, if $\mathcal{C}$ is the class of prime rings, $N_{\mathcal{C}}(R)$ is called the <u>prime radical</u> of R. For any ring R, if $\mathcal{C}$ is the class of simple rings, then $N_{\mathcal{C}}(R)$ is called the <u>Jacobson radical</u> of R. As above, we will refer to R as being <u>prime-semi-simple</u> or <u>Jacobson-semi-simple</u> accordingl

<u>Lemma</u> 3.4 For any ring R (not necessarily commutative), and ideal J of R is prime if and only if R/J is a prime ring.

Proof: Let J be a prime ideal of R. Let $\mathcal{A}$ and $\mathcal{B}$ be ideals of R/J with $\mathcal{A}\mathcal{B} = 0$. Then there are ideals A and B of R such that $J \subseteq A$, $J \subseteq B$ and $\mathcal{A} = A/J$, $\mathcal{B} = B/J$. Now $A/J \cdot B/J = 0$ in R/J implies $AB \subseteq J$, so that $A \subseteq J$ or $B \subseteq J$. That is $\mathcal{A} = 0$ or $\mathcal{B} = 0$. Hence R/J is a prime ring.

Conversely, let J be an ideal of R such that $^R/_J$ is a prime ring. Let A, B be ideals of R such that $AB \subseteq J$. Let $\bar{A} = A + J$ and $\bar{B} = B + J$. Clearly $\bar{A}$, $\bar{B}$ are ideals of R and $J \subseteq \bar{A}$, $J \subseteq \bar{B}$. Thus $^{\bar{A}}/_J$ and $^{\bar{B}}/_J$ are ideals in $^R/_J$. If $\bar{x} \in {}^{\bar{A}}/_J \cdot {}^{\bar{B}}/_J$, then $\bar{x} = \sum_{i=1}^{n} (a_i + J)(b_i + J) = \sum_{i=1}^{n} a_i b_i + J = J$ since $a_i \in A$, $b_i \in B$. That is, $^{\bar{A}}/_J \cdot {}^{\bar{B}}/_J = 0$ in $^R/_J$. As $^R/_J$ is prime, $^{\bar{A}}/_J = 0$ or $^{\bar{B}}/_J = 0$. Thus $\bar{A} \subseteq J$ or $\bar{B} \subseteq J$ implies $A \subseteq J$ or $B \subseteq J$. Hence J is a prime ideal of R.

In the following, let $\mathcal{C}$ be the class of simple rings; $\mathcal{L}$, the class of prime rings; $\mathfrak{A}$, the class of fields; and $\mathfrak{N}$, the class of integral domains.

Lemma 3.5 For any ring R,

1. $N_{\mathcal{C}}(R) = \bigcap \{ J \mid J \text{ is a maximal ideal of } R \}$;
2. $N_{\mathcal{L}}(R) = \bigcap \{ J \mid J \text{ is a prime ideal of } R \}$.

For a commutative ring R with 1,

3. $N_{\mathfrak{A}}(R) = N_{\mathcal{C}}(R)$;
4. $N_{\mathcal{L}}(R) = N_{\mathfrak{N}}(R)$.

Proof: 1. By lemma 3.3, $^R/_J$ is simple if and only if J is a maximal ideal of R. Thus $\{ J \mid J \text{ is an ideal of } R \text{ and } {}^R/_J \text{ is simple} \} = \{ J \mid J \text{ is a maximal ideal of } R \}$.

2. By lemma 3.4, $^R/_J$ is prime if and only if J is prime.

For a commutative ring R with 1, we know that an ideal I of R is prime if and only if $^R/_I$ is an integral domain and that an ideal I is maximal if and only if $^R/_I$ is a field. Hence 3. and 4. follow from 1., 2., and lemma 3.2 and 3.4.

Definiton 3.10 Let R be a ring. An ideal J of R is called a nil ideal if for every $x \in J$, there is an $n \in \mathbb{N}$ such that $x^n = 0$.

R is called nil-semi-simple if R has no non-zero nil ideals.

Lemma 3.6 Let R be any ring with 1. Let S be a multiplicatively closed subset of R which does not contain zero. Then there exists a prime ideal, P, of R such that $P \cap S = \emptyset$.

Proof: Let $\mathcal{A} = \{ U \mid U \text{ is an ideal of } R,\ U \cap S = \emptyset \}$. As $\langle 0 \rangle \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$. Also $\mathcal{A}$ is partially ordered by inclusion. Let $\mathcal{A}_0$ be a chain in $\mathcal{A}$. Let $D = \bigcup \{ U \mid U \in \mathcal{A}_0 \}$. Then D is an ideal of R. For let x, y $\in$ D and r $\in$ R. Then there are U_1 and U_2 in $\mathcal{A}_0$ with $x \in U_1$ and $y \in U_2$. We know that $U_1 \subseteq U_2$ or $U_2 \subseteq U_1$, Let $U_1 \subseteq U_2$. Then $x,y \in U_2$. Hence $x - y \in U_2$ and $xr, rx \in U_2$. Thus $x - y \in D$ and rx, ry $\in$ D. Further, $D \cap S = \emptyset$. For if $x \in D \cap S$, then there exists $U \in \mathcal{A}_0$ with $x \in U$ and $x \in S$. Thus $S \cap U \neq \emptyset$, a contradiction. Hence $D \in \mathcal{A}$ and D is an upper bound for $\mathcal{A}_0$. By Zorn's Lemma, $\mathcal{A}$ has a maximal element, say P. To show that P is a prime ideal of R, let A, B be ideals of R such that $AB \subseteq P$. Suppose P is not prime. That is, let $x \in A$, $y \in B$ and $x, y \notin P$. Then $P \subsetneq P + \langle x \rangle$ and $P \subsetneq P + \langle y \rangle$. As P is maximal in $\mathcal{A}$, $P + \langle x \rangle$ and $P + \langle y \rangle$ have a point in S. Let $p + \sum_{i=1}^{m} r_i x s_i$ and $g + \sum_{i=1}^{n} t_i y u_i$ be points of $P + \langle x \rangle$ and $P + \langle y \rangle$ respectively in S. Then $(p + \sum_{i=1}^{m} r_i x s_i)(q + \sum_{i=1}^{n} t_i y u_i) = pq + p \sum_{i=1}^{n} t_i y u_i + (\sum_{i=1}^{m} r_i x s_i)q + (\sum_{i=1}^{m} r_i x s_i)(\sum_{i=1}^{n} t_i y u_i) \in S \cap P$. Hence $(p + \sum_{i=1}^{m} r_i x s_i)(q + \sum_{i=1}^{n} t_i y u_i) \in P \cap S$, a contradiction. Thus we have that $A \subseteq P$ or $B \subseteq P$, and hence that P is a prime ideal.

Corollary 3.6.1 If R is any ring, the prime radical of R, $N_{\mathcal{P}}(R) \subseteq \{ x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N} \}$.

Proof: Let $T = \{ x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N} \}$. Suppose $u \notin T$. Let $S = \{ u^n \mid n \in \mathbb{N} \}$. By lemma 3.6 there is a prime ideal P of R such that $P \cap S = \emptyset$. Therefore $u \notin N_{\mathcal{L}}(R)$ and hence $N_{\mathcal{L}}(R) \subseteq T$.

Corollary 3.6.2 For a commutative ring R, $N_{\mathcal{L}}(R) = \{ x \in R \mid x^n = 0$ for some $n \in \mathbb{N} \}$.

Proof: Let $T = \{ x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N} \}$. Let $x \in T$. Then $x^n = 0$ for some $n \in \mathbb{N}$. Hence $x^n \in P$ for every prime ideal P of R. Thus $x \in P$ for every prime ideal P of R. That is, $x \in N_{\mathcal{L}}(R)$. Hence $T \subseteq N_{\mathcal{L}}(R)$. By corollary 3.6.1, $N_{\mathcal{L}}(R) \subseteq T$. Thus $T = N_{\mathcal{L}}(R)$.

By corollary 3.6.2, we see that for a commutative ring, the notions of being prime-semi-simple and nil-semi-simple coincide. We further observe that for any ring R, if R id nil-semi-simple, then R is prime-semi-simple. This follows from corollary 3.6.1 by noting that $N_{\mathcal{L}}(R)$ is a nil ideal of R. It follows from lemma 3.5 and corollary 3.6.2 that, for a commutative ring, the radical $N_{\mathcal{N}}(R) = 0$ if and only if R is nil-semi-simple.

Theorem 3.7 For a commutative ring R, the following are equivalent:

1. R is nil-semi-simple.
2. $M_n(R)$ is nil-semi-simple.
3. $M_n(R)$ is prime-semi-simple.
4. R is prime-semi-simple.

Proof: By the remarks above, 2. implies 3. and 4. implies 1. To show 1. implies 2., let $\mathcal{I}$ be a nil ideal of $M_n(R)$. Then there is an ideal S of R such that $\mathcal{I} = M_n(S)$. Let $x \in S$. Then $A = xE_{11} \in M_n(S)$. Hence there exists an $m \in \mathbb{N}$ such that $A^m = x^m E_{11} = 0$ which implies $x^m = 0$ and thus S is a nil ideal of R. As R is nil-s-s. (semi-simple), $S = 0$. Hence $M_n(S) = 0$. Therefore $M_n(R)$ is nil-s-s. To show 3. implies 4., let $M_n(R)$ be prime-s-s. Then the prime radical of $M_n(R)$, $N_{\mathcal{L}}(M_n(R)) = 0$. Now $N_{\mathcal{L}}(M_n(R)) = \bigcap \{ M_n(P) \mid P$ is a prime ideal of $R \}$ by lemma 3.5 and corollary 3.2.1. If $x \in N_{\mathcal{L}}(R)$, then $x \in \bigcap \{ P \mid P$ is prime ideal of $R \}$ and hence $xE_{11} \in \bigcap \{ M_n(P) \mid P$ is a prime ideal of $R \} = N_{\mathcal{L}}(M_n(R))$. Thus $xE_{11} = 0$ and $x = 0$. That is $N_{\mathcal{L}}(R) = 0$ and so R is prime-s-s.

Theorem 3.8 For any commutative ring R, R is Jacobson-s-s. if and only if $M_n(R)$ is Jacobson-s-s.

Proof: By corollary 3.2.1 the maximal ideals of $M_n(R)$ are precisely the ideals $M_n(I)$ where I is a maximal ideal of R. Thus with lemma 3.5, $N_{\mathcal{G}}(M_n(R)) = \bigcap \{ M_n(I) \mid I$ is a maximal ideal of $R \}$ and $N_{\mathcal{G}}(R) = \bigcap \{ I \mid I$ is a maximal ideal of $R \}$. Now $A = (a_{ij}) \in N_{\mathcal{G}}(M_n(R))$ if and only if $A \in M_n(I)$ for every maximal ideal I of R, if and only if $a_{ij} \in I$ for every maximal ideal I of R, if and only if $a_{ij} \in N_{\mathcal{G}}(R)$. Thus $A \in M_n(N_{\mathcal{G}}(R))$ if and only if $a_{ij} \in N_{\mathcal{G}}(R)$.

Hence $N_{\mathcal{G}}(R) = 0$ implies $a_{ij} = 0$ for all i, j and thus $A = 0$. That is, $N_{\mathcal{G}}(M_n(R)) = 0$. Conversely, if $N_{\mathcal{G}}(M_n(R)) = 0$, then $x \in N_{\mathcal{G}}(R)$ implies $xE_{11} \in N_{\mathcal{G}}(M_n(R)) = 0$. Hence $x = 0$ and $N_{\mathcal{G}}(R) = 0$.

CHAPTER IV

DETERMINANTS AND SYSTEMS OF LINEAR HOMOGENEOUS EQUATIONS

In this chapter we present the notions of determinants and linear equations over a commutative ring with identity. The development here parallels the usual development of these notions over the field of real or complex numbers. It is easy to see that most of the theory developed for determinants over the real or complex numbers, see [1] , carry over to our more general situation. We list, without proof, some of the familiar results. The definition of a determinant that we take here is the usual one.

<u>Definition</u> 4.1 Let R be a commutative ring with 1. A <u>determinant</u> is a function $\text{Det}:M\ (R) \longrightarrow R$ such that, if $A \in M_n(R)$ and if $A_1, \ldots, A_n$ represent its columns, the following properties are satisfied:

1. $\text{Det}(A_1, \ldots, A_K, \ldots, A_n) + \text{Det}(A_1, \ldots, A_{K-1}, B_K, A_{K+1}, \ldots, A_n) = \text{Det}(A_1, \ldots, A_{K-1}, A_K + B_K, A_{K+1}, \ldots, A_n)$
2. $\text{Det}(A_1, \ldots, A_{K-1}, aA_K, A_{K+1}, \ldots, A_n) = a\,\text{Det}(A_1, \ldots, A_n)$
3. $\text{Det}(A) = 0$ if any two columns are equal.
4. $\text{Det}(I) = 1$ where $I = (\delta_{ij})$ in the identity matrix.

Observe that, if such a function exists, the following properties will be satisfied:

1. $\text{Det}(A) = 0$ if any column A_K of A is zero.
2. $\text{Det}(A)$ is unchanged if a multiple of one column is added to another column.
3. $\text{Det}(A)$ changes sign if we interchange any two columns.

4. Det(AB) = Det(A) Det(B).

We proceed now to define such a function. Let $D:M_n(R) \longrightarrow R$ be defined inductively as follows: For n = 1, $A \in M_n(R)$ implies $A = (a_{11})$; let $D(A) = a_{11}$. Clearly D works. Assume we have a function $\bar{D}:M_{n-1}(R) \longrightarrow R$ which is a determinant. Let $D:M_n(R) \longrightarrow R$ be defined as follows: for $A \in M_n(R)$ and for each i, j, $1 \leqslant i, j \leqslant n$, let $M_{ij} \in M_{n-1}(R)$ be formed from A by deleting the ith row and the jth column of A. Let $A_{ij} = (-1)^{i+j} \bar{D}(M_{ij})$. A_{ij} is called the <u>cofactor</u> of a_{ij}. For a fixed i, $1 \leq i \leqslant n$, let $D(A) = a_{i1} A_{i1} + a_{i2} A_{i2} + \ldots + a_{in} A_{in}$. This is the usual definition in case R is the field of real or complex numbers. The proof that this definition gives a determinant in our more general situation is analogous to the proof that such a definition, in the case of a field, gives a determinant.

Note that if, in the above discussion, the word "column" is replaced by the word "row" throughout, we get analogous results in terms of rows.

Observe that, for $A = (a_{ij}) \in M_n(R)$, $\sum_{j=1}^{n} a_{ij} A_{kj} = \delta_{ik} D(A) = 0$ if $k \neq i$ and D(A) if k = i; $\sum_{i=1}^{n} a_{ij} A_{ik} = \delta_{jk} D(A) = 0$ if $k \neq j$ and D(A) if k = j. To see this, notice that if $k \neq i$ and if we replace row k of A by row i we get a new matrix B with two rows equal. If B_{kj} is the cofactor of b_{kj} in $B = (b_{ij})$, then for each j, $1 \leq j \leq n$, $b_{kj} = a_{ij}$ and $A_{kj} = B_{kj}$. Hence $\sum_{j=1}^{n} a_{ij} A_{kj} = \sum_{j=1}^{n} b_{kj} B_{kj} = D(B) = 0$.

If k = i then clearly $\sum_{j=1}^{n} a_{ij} A_{ij} = D(A)$. Hence $\sum_{j=1}^{n} a_{ij} A_{kj} = \delta_{ik} D(A)$. The second expression above follows by a similar argument after we replace column k by column j in A.

The determinant of $A \in M_n(R)$ will hereafter be denoted by $|A|$.

Definition 4.2 Let $A \in M_n(R)$. Let A_{ij} be the cofactor of a_{ij}. The adjoint of A, denoted adj A, is adj A = $\begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ & \vdots & & \\ A_{1n} & A_{2n} & & A_{nn} \end{pmatrix} \in M_n(R)$.

Lemma 4.1 For $A \in M_n(R)$, $A(\text{adj } A) = (\text{adj } A)\, A = |A|\, I$.

Proof: Let $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ and adj $A = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \vdots & & \vdots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}$

where A_{ij} is the cofactor of a_{ij} in A. Then $A(\text{adj } A) = (b_{ij}) \in M_n(R)$ where $b_{ij} = \sum_{k=1}^{n} a_{ik} A_{jk}$ and $(\text{adj } A)A = (c_{ij}) \in M_n(R)$ where $c_{ij} = \sum_{k=1}^{n} a_{kj} A_{ki}$. By the remarks above, $b_{ij} = \delta_{ij} |A|$ and $c_{ij} = \delta_{ij} |A|$. Thus $A(\text{adj } A) = |A|\, I = (\text{adj } A)A$.

For any ring R with 1, if $a \in R$ and $a \neq 0$, an element $b \in R$ is called an inverse of a if $ab = ba = 1$. It is easy to check that if a has an inverse, then it is unique. Note also that for a commutative ring R with 1, we take $aA = Aa$ for any $a \in R$ and $A \in M_n(R)$.

Theorem 4.1 Let $A \in M_n(R)$. Then A has an inverse in $M_n(R)$ if and only if $|A|$ has an inverse in R.

Proof: Let $B \in M_n(R)$ with $AB = BA = I$. Then $|A| \cdot |B| = |AB| = |I| = 1$. Hence $|B|$ is an inverse for $|A|$ in R.

Conversely, let $d \in R$ be such that $|A|\, d = d|A| = 1$. By lemma 4.1, $A(\text{adj } A)d = I$ and $d(\text{adj } A)A = I$. Hence $d(\text{adj } A)$ is an inverse for A in $M_n(R)$.

Definition 4.3 Let $Q \subseteq R$. An element $a \in R$ is called an annihilator of the set Q if $aQ = \{ ax \mid x \in Q \} = \{ 0 \}$.

Note that if R is an integral domain, that is, if R is a commutative ring with 1 which has no zero divisors, then $Q \subseteq R$ has a non-zero annihilator if and only if $Q = \{ 0 \}$.

For a commutative ring R with 1, let $A \in M_{nm}(R)$ and let $1 \leqslant r \leqslant k$ where $k = \min \{ n, m \}$. Let M be any square submatrix of A which contains r rows and r columns. Then $|M|$ is called a minor of A of order r.

Let $A \in M_{nm}(R)$. If $\{ a_{ij} \mid a_{ij}$ is an entry of $A \}$ has a non-zero annihilator, we say that A has rank zero. If A does not have rank zero, then the set of all minors of A of order 1 has no non-zero annihilators. That is, $aA \neq 0$ for all $a \neq 0$ in R. In this case we define the rank of A to be the largest integer, r, $1 \leqslant r \leqslant k$ where $k = \min \{m, n\}$, such that the set of all minors of A of order r has no non-zero annihilator. Note that if $r < s < k$, then the set of all minors of A of order s has a non-zero annihilator. We will denote the rank of A by r(A).

Let R be an integral domain and $A \in M_n(R)$. If $r(A) = 0$, then there exists an $a \in R$, $a \neq 0$, such that $aA = 0$. That is, $A = 0$ which implies that all minors of A are zero. If A has rank $r \neq 0$, then the set of all minors of A of order r has no non-zero annihilator. Hence, there is a minor $|M|$ of A of order r such that $|M| \neq 0$. Moreover, by definition of rank, the set of all minors of A of order s, $r < s < k$, has a non-zero annihilator. That is, there is an $a \in R$, $a \neq 0$ such that, if $|L|$ is a minor of A of order s, then $a|L| = 0$. Since R is an integral domain, $L = 0$. Hence r is the largest order of the non-vanishing minors of A. Thus we see that r(A) satisfies the usual definition of rank in case R is the set of real or complex numbers (see [6]). In fact, it follows that the two definitions are equivalent in this case.

Definition 4.5 Let $x_1, \ldots, x_n$ be indeterminants. Let c_{ij}, $b_i \in R$ for $i = 1, \ldots, m$, $j = 1, \ldots, n$. Then $\sum_{j=1}^{n} c_{ij} x_j = b_i$ for $i = 1, \ldots, m$, is called a system of m linear equations in n unknowns. The system above is called homogeneous if $b_i = 0$ for all i. The set $\{a_1, \ldots, a_m\} \subseteq R$ is called a solution to the system $\sum_{j=1}^{n} c_{ij} x_j = 0$, $i = 1, \ldots, m$ if $\sum_{j=1}^{n} c_{ij} a_j = 0$, $i = 1, \ldots, m$. The matrix $A = (c_{ij}) \in M_{nm}(R)$ will be called the matrix of coefficients of the system.

Theorem 4.2 The system $\sum_{j=1}^{n} c_{ij} x_j = 0$, $i = 1, \ldots, m$, where $c_{ij} \in R$, a commutative ring with 1, has a non-trivial solution if and only if the rank of the matrix of coefficients is less than the numbers of unknowns.

Proof: Suppose $a_1, \ldots, a_n$ is a solution to the system with $a_k \neq 0$. Then $\sum_{j=1}^{n} c_{ij} a_j = 0$ for $i = 1, \ldots, m$. Let $A = (c_{ij})$. We must show $r(A) < n$.

Case 1. If $m < n$, then the largest minors of A have order m. Hence $r(A) \leqslant m < n$ and we are done.

Case 2. If $m \geqslant n$, the largest minors of A have order n. Let $|M|$ be any minor of A of order n. For each i_t, $1 \leqslant i_t \leqslant m$, for which the i_tth row of A is a row of M, multiply the i_tth equation by the cofactor, $M_{i_t k}$, of $c_{i_t k}$ in M. We have n equations of the form:

$$M_{i_t k} c_{i_t 1} a_1 + M_{i_t k} c_{i_t 2} a_2 + \ldots + M_{i_t k} c_{i_t k} a_k + \ldots + M_{i_t k} c_{i_t n} a_n = 0.$$

Adding these equations, we get:

$$0 = a_1 \sum_{t=1}^{n} c_{i_t 1} M_{i_t k} + \ldots + a_k \sum_{t=1}^{n} c_{i_t k} M_{i_t k} + \ldots + a_n \sum_{t=1}^{n} c_{i_t n} M_{i_t k} =$$

$$a_1 \delta_{1k} |M| + \ldots + a_k \delta_{kk} |M| + \ldots + a_n \delta_{nk} |M| = a_k |M|.$$

Since $|M|$ was an arbitrary minor of A of order n, and since $a_k \neq 0$, the set of minors of A of order n has a non-zero annihilator. That is, $r(A) < n$.

Conversely, let $r(A) = r < n$. If $r = m$, $\sum_{i=1}^{m} c_{ij} x_j = 0$ has a non-trivial solution if and only if $\sum_{k=1}^{m+1} b_{kj} x_j = 0$ has a non-trivial solution, where $b_{kj} = c_{kj}$ if $1 \leq k \leq m$ and $b_{m+1\, j} = 0$. Let $B = (b_{ij})$. Clearly $r(B) = r(A) = m < m + 1$. Hence we may assume $r < m$. Let $a \in R$ with $a \neq 0$ such that $a|M| = 0$ for all minors M of A of order $r + 1$.

Case 1. If $r = 0$, then $aA = 0$ and $\sum_{j=1}^{n} ac_{ij} = 0$ for $i = 1, \ldots, m$. Hence $x_j = a$, for all j, is a non-trivial solution to the system $\sum_{j=1}^{n} c_{ij} x_j = 0$, $i = 1, \ldots, m$.

Case 2. If $r > 0$, then there is a minor $|M|$ of A of order r such that $a|M| \neq 0$. Since interchanging any two rows or columns in M changes the sign in $|M|$ only, we can rearrange the rows and columns of A so that M appears in the upper left corner of A. Let $|\bar{M}|$ be the minor of order $r + 1$ in the upper left corner of A. Let $d_1, \ldots, d_{r+1}$ be the cofactors in $\bar{M}$ of the elements in the $r + 1^{st}$ row of $\bar{M}$. Notice that $a|M| = ad_{r+1} \neq 0$. Let $x_j = ad_j$ for $j = 1, \ldots, r + 1$ and $x_j = 0$ for $j = r + 2, \ldots, n$. For any i, $1 \leq i \leq m$, let $B = (b_{kj}) \in M_{r+1}(R)$ where $b_{kj} = c_{kj}$ if $1 \leq k \leq r$ and $b_{r+1,\, j} = c_{ij}$. Then $|B|$ is a minor of A of order $r + 1$; so $a|B| = 0$. Moreover, if $B_{r+1,\, j}$ is the cofactor of $b_{r+1,\, j}$ in B, $B_{r+1,\, j} = d_j$. Hence for any i, $1 \leq i \leq m$, $\sum_{j=1}^{r+1} c_{ij} (ad_j) = a \sum_{j=1}^{r+1} b_{r+1,\, j} B_{r+1,\, j} = a|B| = 0$.

Thus $\sum_{j=1}^{n} c_{ij} x_j = \sum_{j=1}^{r+1} c_{ij} (ad_j) + \sum_{j=r+2}^{n} c_{ij} \cdot 0 = 0$, $i = 1, \ldots, m$ where $ad_{r+1} \neq 0$. Hence we have a non-trivial solution to the system.

<u>Corollary</u> 4.2.1 $A \in M_n(R)$ is a zero-divisor in $M_n(R)$ if and only if

$|A|$ is a zero-divisor in R.

Proof: Suppose $A \in M_n(R)$ is a zero-divisor. Then there exists $B \in M_n(R)$, $B \neq 0$ with $AB = 0$ or $BA = 0$. Suppose $AB = 0$. Let $A = (a_{ij})$ and $B = (b_{ij})$ with $b_{kt} \neq 0$. In the t^{th} column of AB, we have $\sum_{j=1}^{n} a_{ij} b_{jt} = 0$, $i = 1, \ldots, n$. Thus we have a non-trivial solution to the system $\sum_{j=1}^{n} a_{ij} x_j = 0$, $i = 1, \ldots, n$, of n equations in n unknowns. By theorem 4.2, $r(A) = r < n$. Thus every minor of A of order $s > r$ has a non-zero annihilator. In particular, $|A|$ has a non-zero annihilator. That is, $|A|$ is a zero-divisor in R.

Conversely, let $|A|$ be a zero-divisor in R. Then as a minor of A, $|A|$ has a non-zero annihilator. Thus for any set of minors of A of order r, $1 \leqslant r \leqslant n$, that has no non-zero annihilator, r must be less than n. That is $r(A) < n$. By theorem 4.2, there exist $y_k \in R$, for $k = 1, \ldots, n$, not all zero, such that $\sum_{k=1}^{n} a_{ik} y_k = 0$ for $i = 1, \ldots, n$. Let $Y \in M_n(R)$ be defined by: $Y = (c_{kj})$ where $c_{k1} = y_k$ and $c_{kj} = 0$ for $j = 2, \ldots, n$. Then $AY = (a_{ij})(c_{ij}) = (d_{ij})$ where $d_{ij} = \sum_{k=1}^{n} a_{ik} c_{kj}$. Now $d_{i1} = \sum_{k=1}^{n} a_{ik} y_k = 0$ and $d_{ij} = 0$ for $2 \leqslant j \leqslant n$. Hence $AY = 0$ and A is a zero-divisor in $M_n(R)$.

REFERENCES

1. Artin, E., Galois Theory, Notre Dame Mathematical Lectures, no. 2 (Second Edition), 1942, pp. 11 - 20.

2. Divinsky, N., Rings and Radicals, Mathematical Expositions, no. 14, University of Toronto Press, 1965.

3. Halmos, P., Finite Dimensional Vector Spaces, D. Van Nostrand Co., New York, 1958.

4. Herstein, I., Topics in Algebra, Blaisdell Co., New York, 1964, Chapters 4 and 6.

5. Jans, J., Rings and Homology, Holt, Rinehart and Winston, New York, 1964, pp. 1 - 3.

6. MacDuffee, C., The Theory of Matrices, Chelsea, New York, 1946, pp. 10.

7. McCoy, N., Rings and Ideals, Carus Mathematical Monographs, no. 8, 1948, pp. 155 - 162.

8. ————, Theory of Rings, MacMillan Co., New York, 1964, Chapter 4.

9. Von Neumann, J., On Regular Rings, Nat. Acad. Sci., Vol. 22, 1936, pp. 713.

10. Zariski, O. and Samuel, P., Commutative Algebra, vol. 1, D. Van Nostrand Co., New York, 1951, Chapter 3.

11. ————————————————, chapter 4.