

where each  $L_i$  is a simple module (i.e., a simple left ideal) with  $L_i = Re_i$ , for some  $e_i \in R$  with

$$(i) \quad e_i e_j = 0 \text{ if } i \neq j$$

$$(ii) \quad e_i^2 = e_i \text{ for all } i$$

$$(iii) \quad \sum_{i=1}^n e_i = 1$$

- (5) as rings,  $R$  is isomorphic to a direct product of matrix rings over division rings, i.e.,  $R = R_1 \times R_2 \times \cdots \times R_r$  where  $R_j$  is a two-sided ideal of  $R$  and  $R_j$  is isomorphic to the ring of all  $n_j \times n_j$  matrices with entries in a division ring  $\Delta_j$ ,  $j = 1, 2, \dots, r$ . The integer  $r$ , the integers  $n_j$ , and the division rings  $\Delta_j$  (up to isomorphism) are uniquely determined by  $R$ .

*Proof:* A proof of Wedderburn's Theorem is outlined in Exercises 1 to 10

**Definition.** A ring  $R$  satisfying any of the (equivalent) properties in Theorem 4 is called *semisimple with minimum condition*.

Rings  $R$  satisfying any of the equivalent conditions of Theorem 4 also satisfy the *minimum condition* or *descending chain condition (D.C.C)* on left ideals:

if  $I_1 \supseteq I_2 \supseteq \cdots$  is a descending chain of left ideals of  $R$

then there is an  $N \in \mathbb{Z}^+$  such that  $I_k = I_N$  for all  $k \geq N$

(which explains the use of this term in the definition above). The rings we deal with will all have this minimum condition. For example, group algebras always have this property since in any strictly descending chain of ideals the vector space dimensions of the ideals (which are  $F$ -subspaces of  $FG$ ) are strictly decreasing, hence the length of a strictly descending chain is at most the dimension of  $FG (= |G|)$ . We shall therefore use the term "semisimple" to mean "semisimple with minimum condition." The rings  $R_i$  in conclusion (5) of Wedderburn's Theorem are called the *Wedderburn components* of  $R$  and the direct product decomposition of  $R$  is called its *Wedderburn decomposition*. Note that Wedderburn's Theorem for commutative rings is a consequence of the classification of Artinian rings in Section 16.1. A commutative semisimple ring with minimum condition is an Artinian ring with Jacobson radical equal to zero and so is a direct product of fields (which are its Wedderburn components).

One should note that condition (5) is a two-sided condition which describes the overall structure of  $R$  completely (the ring operations in this direct product of rings are componentwise addition and multiplication). In particular it implies that a semisimple ring also has the minimum condition on right ideals. A useful way of thinking of the elements of the direct product  $R_1 \times \cdots \times R_r$  in conclusion (5) is as  $n \times n$  (block diagonal) matrices of the form

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}$$

where  $A_i$  is an arbitrary  $n_i \times n_i$  matrix with entries from  $\Delta_i$  (here  $n = \sum_{i=1}^r n_i$ ).

Recall from Section 10.5 that an  $R$ -module  $Q$  is *injective* if whenever  $Q$  is a submodule of any  $R$ -module  $M$ , then  $M$  has a submodule  $N$  such that  $M = Q \oplus N$ . Maschke's Theorem therefore implies:

**Corollary 5.** If  $G$  is a finite group and  $F$  is a field whose characteristic does not divide  $|G|$ , then the group algebra  $FG$  is a semisimple ring.

Before obtaining more precise information about how the invariants  $n, r, \Delta_j$ , etc., relate to invariants in group rings  $FG$  for certain fields  $F$ , we first study the structure of matrix rings (i.e., the rings described in conclusions (4) and (5) of Wedderburn's Theorem). We introduce some terminology which is used extensively in ring theory. Recall that the *center* of the ring  $R$  is the subring of elements commuting with all elements in  $R$ ; it will be denoted by  $Z(R)$  (the center will contain 1 if the ring has a 1).

**Definition.**

- (1) A nonzero element  $e$  in a ring  $R$  is called an *idempotent* if  $e^2 = e$ .
- (2) Idempotents  $e_1$  and  $e_2$  are said to be *orthogonal* if  $e_1e_2 = e_2e_1 = 0$ .
- (3) An idempotent  $e$  is said to be *primitive* if it cannot be written as a sum of two (commuting) orthogonal idempotents.
- (4) The idempotent  $e$  is called a *primitive central idempotent* if  $e \in Z(R)$  and  $e$  cannot be written as a sum of two orthogonal idempotents in the ring  $Z(R)$ .

Proposition 6 describes the ideal structure of a matrix ring and Proposition 8 extends these results to direct products of matrix rings.

**Proposition 6.** Let  $\Delta$  be a division ring, let  $n \in \mathbb{Z}^+$ , let  $R$  be the ring of all  $n \times n$  matrices with entries from  $\Delta$  and let  $I$  be the identity matrix (= the 1 of  $R$ ).

- (1) The only two-sided ideals of  $R$  are 0 and  $R$ .
- (2) The center of  $R$  consists of the scalar matrices  $\alpha I$ , where  $\alpha$  is in the center of  $\Delta$ :  $Z(R) = \{\alpha I \mid \alpha \in Z(\Delta)\}$ , and this is a field isomorphic to  $Z(\Delta)$ . In particular, if  $\Delta$  is a field, the center of  $R$  is the subring of all scalar matrices. The only central idempotent in  $R$  is  $I$  (in particular,  $I$  is primitive).
- (3) Let  $e_i$  be the matrix with a 1 in position  $i, i$  and zeros elsewhere. Then  $e_1, \dots, e_n$  are orthogonal primitive idempotents and  $\sum_{i=1}^n e_i = I$ .
- (4)  $L_i = Re_i$  is the left ideal consisting of arbitrary entries in column  $i$  and zeros in all other columns.  $L_i$  is a simple left  $R$ -module. Every simple left  $R$ -module is isomorphic to  $L_1$  (in particular, all  $L_i$  are isomorphic  $R$ -modules) and as a left  $R$ -module we have  $R = L_1 \oplus \dots \oplus L_n$ .

Before proving this proposition it will be useful to have the following result.

**Lemma 7.** Let  $R$  be an arbitrary nonzero ring.

- (1) If  $M$  and  $N$  are simple  $R$ -modules and  $\varphi : M \rightarrow N$  is a nonzero  $R$ -module homomorphism, then  $\varphi$  is an isomorphism.
- (2) (*Schur's Lemma*) If  $M$  is a simple  $R$ -module, then  $\text{Hom}_R(M, M)$  is a division ring.

*Proof of Lemma 7:* To prove (1) note that since  $\varphi$  is nonzero,  $\ker \varphi$  is a proper submodule of  $M$ . By simplicity of  $M$  we have  $\ker \varphi = 0$ . Similarly, the image of  $\varphi$  is a nonzero submodule of the simple module  $N$ , hence  $\varphi(M) = N$ . This proves  $\varphi$  is bijective, so (1) holds.

By part (1), every nonzero element of the ring  $\text{Hom}_R(M, M)$  is an isomorphism, hence has an inverse. This gives (2).

*Proof of Proposition 6* Let  $A$  be an arbitrary matrix in  $R$  whose  $i, j$  entry is  $a_{ij}$ . Let  $E_{ij}$  be the matrix with a 1 in position  $i, j$  and zeros elsewhere. The following straightforward computations are left as exercises:

- (i)  $E_{ij}A$  is the matrix whose  $i^{\text{th}}$  row equals the  $j^{\text{th}}$  row of  $A$  and all other rows are zero.
- (ii)  $AE_{ij}$  is the matrix whose  $j^{\text{th}}$  column equals the  $i^{\text{th}}$  column of  $A$  and all other columns are zero.
- (iii)  $E_{pq}AE_{rs}$  is the matrix whose  $p, s$  entry is  $a_{qr}$  and all other entries are zero.

To prove (1) suppose  $J$  is any nonzero 2-sided ideal of  $R$  and let  $A$  be an element of  $J$  with a nonzero entry in position  $q, r$ . Given any  $p, s \in \{1, \dots, n\}$  we obtain from (iii) that

$$E_{ps} = \frac{1}{a_{qr}} E_{pq} A E_{rs} \in J.$$

Since the  $\Delta$ -linear combinations of  $\{E_{ps} \mid 1 \leq p \leq n, 1 \leq s \leq n\}$  give all of  $R$ , it follows that  $J = R$ . This proves (1).

To prove (2) assume  $A \in Z(R)$ . Thus for all  $i, j$  we have  $E_{ij}A = AE_{ij}$ . From (i) and (ii) above it follows immediately that all off-diagonal entries of  $A$  are zero and all diagonal entries of  $A$  are equal. Thus  $A = \alpha I$  for some  $\alpha \in \Delta$ . Furthermore,  $A$  must also commute with the set of all scalar matrices  $\beta I, \beta \in \Delta$ , i.e.,  $\alpha$  must commute with all elements of  $\Delta$ . Finally, since  $Z(R)$  is a field, it is immediate that it contains a unique idempotent (namely  $I$ ). This establishes all parts of (2).

In part (3) it is clear that  $e_1, \dots, e_n$  are orthogonal idempotents whose sum is  $I$ . We defer proving that they are primitive until we have established (4).

Next we prove (4). From (ii) above it follows that  $Re_i = RE_{ii}$  is the set of matrices with arbitrary entries in the  $i^{\text{th}}$  column and zeros in all other columns. Furthermore, if  $A$  is any nonzero element of  $Re_i$ , then certainly  $RA \subseteq Re_i$ . The reverse inclusion holds because if  $a_{pi}$  is a nonzero entry of  $A$ , then by (i) above

$$e_i = E_{ii} = \frac{1}{a_{pi}} E_{ip} A \in RA.$$

This proves  $Re_i = RA$  for any nonzero element  $A \in Re_i$ , and so  $Re_i$  must be a simple  $R$ -module.

Let  $M$  be any simple  $R$ -module. Since  $Im = m$  for all  $m \in M$  and since  $I = \sum_{i=1}^n e_i$ , there exists some  $i$  and some  $m \in M$  such that  $e_i m \neq 0$ . For this  $i$  and  $m$  the map  $re_i \mapsto re_i m$  is a nonzero  $R$ -module homomorphism from the simple  $R$ -module  $Re_i$  to the simple module  $M$ . By Lemma 7(1) it is an isomorphism. By (ii), the map  $r \mapsto rE_{ii}$  gives  $Re_i \cong Re_1$ . Finally, every matrix is the direct sum of its columns so  $R = L_1 \oplus \dots \oplus L_n$ . This completes the proof of (4).