II. Wedderburn-Artin Ring Theory, 76-122

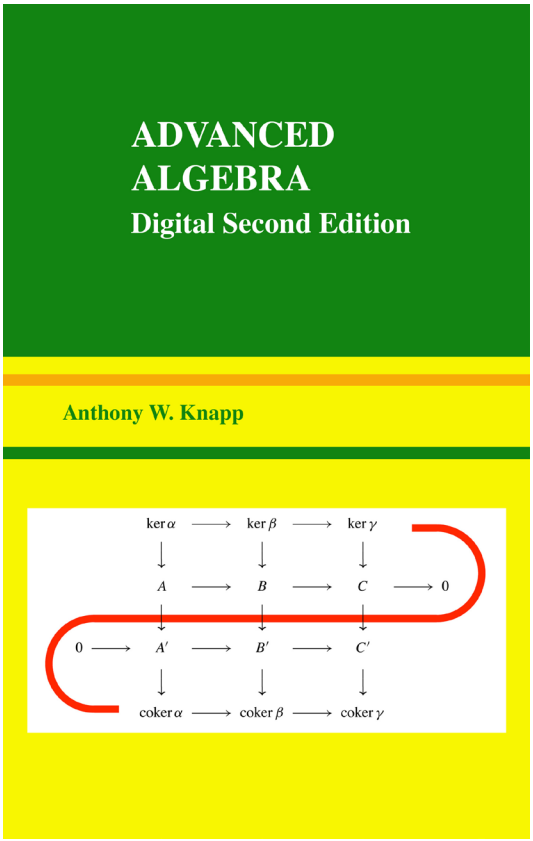
DOI: 10.3792/euclid/9781429799928-2

from

Advanced Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928
ISBN: 978-1-4297-9992-8



Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/~aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9

Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN

Published by the Author

CHAPTER II

Wedderburn–Artin Ring Theory

Abstract. This chapter studies finite-dimensional associative division algebras, as well as other finite-dimensional associative algebras and closely related rings. The chapter is in two parts that overlap slightly in Section 6. The first part gives the structure theory of the rings in question, and the second part aims at understanding limitations imposed by the structure of a division ring.

Section 1 briefly summarizes the structure theory for finite-dimensional (nonassociative) Lie algebras that was the primary historical motivation for structure theory in the associative case. All the algebras in this chapter except those explicitly called Lie algebras are understood to be associative.

Section 2 introduces left semisimple rings, defined as rings R with identity such that the left R module R is semisimple. Wedderburn's Theorem says that such a ring is the finite product of full matrix rings over division rings. The number of factors, the size of each matrix ring, and the isomorphism class of each division ring are uniquely determined. It follows that left semisimple and right semisimple are the same. If the ring is a finite-dimensional algebra over a field F, then the various division rings are finite-dimensional division algebras over F. The factors of semisimple rings are simple, i.e., are nonzero and have no nontrivial two-sided ideals, but an example is given to show that a simple ring need not be semisimple. Every finite-dimensional simple algebra is semisimple.

Section 3 introduces chain conditions into the discussion as a useful generalization of finite dimensionality. A ring R with identity is left Artinian if the left ideals of the ring satisfy the descending chain condition. Artin's Theorem for simple rings is that left Artinian is equivalent to semisimplicity, hence to the condition that the given ring be a full matrix ring over a division ring.

Sections 4–6 concern what happens when the assumption of semisimplicity is dropped but some finiteness condition is maintained. Section 4 introduces the Wedderburn–Artin radical $\operatorname{rad} R$ of a left Artinian ring R as the sum of all nilpotent left ideals. The radical is a two-sided nilpotent ideal. It is 0 if and only if the ring is semisimple. More generally $R/\operatorname{rad} R$ is always semisimple if R is left Artinian. Sections 5–6 state and prove Wedderburn's Main Theorem — that a finite-dimensional algebra R with identity over a field F of characteristic 0 has a semisimple subalgebra S such that R is isomorphic as a vector space to $S \oplus \operatorname{rad} R$. The semisimple algebra S is isomorphic to $R/\operatorname{rad} R$. Section 5 gives the hard part of the proof, which handles the special case that $R/\operatorname{rad} R$ is isomorphic to a product of full matrix algebras over F. The remainder of the proof, which appears in Section 6, follows relatively quickly from the special case in Section 5 and an investigation of circumstances under which the tensor product over F of two semisimple algebras is semisimple. Such a tensor product is not always semisimple, but it is semisimple in characteristic 0.

The results about tensor products in Section 6, but with other hypotheses in place of the condition of characteristic 0, play a role in the remainder of the chapter, which is aimed at identifying certain division rings. Sections 7–8 provide general tools. Section 7 begins with further results about tensor products. Then the Skolem–Noether Theorem gives a relationship between any two homomorphisms of a simple subalgebra into a simple algebra whose center coincides with the underlying field of

scalars. Section 8 proves the Double Centralizer Theorem, which says for this situation that the centralizer of the simple subalgebra in the whole algebra is simple and that the product of the dimensions of the subalgebra and the centralizer is the dimension of the whole algebra.

Sections 9–10 apply the results of Sections 6–8 to obtain two celebrated theorems — Wedderburn's Theorem about finite division rings and Frobenius's Theorem classifying the finite-dimensional associative division algebras over the reals.

1. Historical Motivation

Elementary ring theory came from several sources historically and was already in place by 1880. Some of the sources are field theory (studied by Galois and others), rings of algebraic integers (studied by Gauss, Dirichlet, Kummer, Kronecker, Dedekind, and others), and matrices (studied by Cayley, Hamilton, and others). More advanced general ring theory arose initially not on its own but as an effort to imitate the theory of "Lie algebras," which began about 1880.

A brief summary of some early theorems about Lie algebras will put matters in perspective. The term "algebra" in connection with a field F refers at least to an F vector space with a multiplication that is F bilinear. This chapter will deal only with two kinds of such algebras, the Lie algebras and those algebras whose multiplication is associative. If the modifier "Lie" is absent, the understanding is that the algebra is associative.

Lie algebras arose originally from "Lie groups" — which we can regard for current purposes as connected groups with finitely many smooth parameters — by a process of taking derivatives along curves at the identity element of the group. Precise knowledge of that process will be unnecessary in our treatment, but we describe one example: The vector space $M_n(\mathbb{R})$ of all n-by-n matrices over $\mathbb{R}$ becomes a Lie algebra with multiplication defined by the "bracket product" $[X, Y] = XY - YX$. If G is a closed subgroup of the matrix group $\mathrm{GL}(n, \mathbb{R})$ and $\mathfrak{g}$ is the set of all members of $M_n(\mathbb{R})$ of the form $X = c'(0)$, where c is a smooth curve in G with $c(0)$ equal to the identity, then it turns out that the vector space $\mathfrak{g}$ is closed under the bracket product and is a Lie algebra. Although one might expect the Lie algebra $\mathfrak{g}$ to give information about the Lie group G only infinitesimally at the identity, it turns out that $\mathfrak{g}$ determines the multiplication rule for G in a whole open neighborhood of the identity. Thus the Lie group and Lie algebra are much more closely related than one might at first expect.

We turn to the underlying definitions and early main theorems about Lie algebras. Let F be a field. A vector space A over F with an F bilinear multiplication $(X, Y) \mapsto [X, Y]$ is a **Lie algebra** if the multiplication has the two properties

(i) $[X, X] = 0$ for all $X \in A$,

(ii) **(Jacobi identity)** $[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$ for all $X, Y, Z \in A$.

Multiplication is often referred to as **bracket**. It is usually not associative. The vector space $M_n(F)$ with $[X, Y] = XY - YX$ is a Lie algebra, as one easily checks by expanding out the various brackets that are involved; it is denoted by $\mathfrak{gl}(n, F)$.

The elementary structural definitions with Lie algebras run parallel to those with rings. A **Lie subalgebra** S of A is a vector subspace closed under brackets, an **ideal** I of A is a vector subspace such that $[X, Y]$ is in I for $X \in I$ and $Y \in A$, a **homomorphism** $\varphi : A_1 \to A_2$ of Lie algebras is a linear mapping respecting brackets in the sense that $\varphi[X, Y] = [\varphi(X), \varphi(Y)]$ for all $X, Y \in A_1$, and an **isomorphism** is an invertible homomorphism. Every ideal is a Lie subalgebra. In contrast to the case of rings, there is no distinction between "left ideals" and "right ideals" because the bracket product is skew symmetric. Under the passage from Lie groups to Lie algebras, abelian Lie groups yield Lie algebras with all brackets 0, and thus one says that a Lie algebra is **abelian** if all its brackets are 0.

Examples of Lie subalgebras of $\mathfrak{gl}(n, F)$ are the subalgebra $\mathfrak{sl}(n, F)$ of all matrices of trace 0, the subalgebra $\mathfrak{so}(n, F)$ of all skew-symmetric matrices, and the subalgebra of all upper-triangular matrices.

The elementary properties of subalgebras, homomorphisms, and so on for Lie algebras mimic what is true for rings: The kernel of a homomorphism is an ideal. Any ideal is the kernel of a quotient homomorphism. If I is an ideal in A, then the ideals of A/I correspond to the ideals of A containing I, just as in the First Isomorphism Theorem for rings. If I and J are ideals in A, then $(I + J)/I \cong J/(I \cap J)$, just as in the Second Isomorphism Theorem for rings.

The connection of Lie algebras to Lie groups makes one want to introduce definitions that lead toward classifying all Lie algebras that are finite-dimensional. We therefore assume for the remainder of this section that all Lie algebras under discussion are finite-dimensional over F. Some of the steps require conditions on F, and we shall assume that F has characteristic 0.

Group theory already had a notion of "solvable group" from Galois, and this leads to the notion of solvable Lie algebra. In A, let $[A, A]$ denote the linear span of all $[X, Y]$ with $X, Y \in A$; $[A, A]$ is called the **commutator ideal** of A, and $A/[A, A]$ is abelian. In fact, $[A, A]$ is the smallest ideal I in A such that A/I is abelian. Starting from A, let us form successive commutator ideals. Thus put $A_0 = A$, $A_1 = [A_0, A_0], \dots, A_n = [A_{n-1}, A_{n-1}]$, so that

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n \supseteq \cdots .$$

The terms of this sequence are all the same from some point on, by finite dimensionality, and we say that A is **solvable** if the terms are ultimately 0. One easily checks that the sum $I + J$ of two solvable ideals in A, i.e., the set of sums, is a solvable ideal. By finite dimensionality, there exists a unique largest solvable ideal. This is called the **radical** of A and is denoted by rad A. The Lie algebra

A is said to be **semisimple** if $\operatorname{rad} A = 0$. It is easy to use the First Isomorphism Theorem to check that $A/\operatorname{rad} A$ is always semisimple.

In the direction of classifying Lie algebras, one might therefore want to see how all solvable Lie algebras can be constructed by successive extensions, identify all semisimple Lie algebras, and determine how a general Lie algebra can be constructed from a semisimple Lie algebra and a solvable Lie algebra by an extension.

The first step in this direction historically concerned identifying semisimple Lie algebras. We say that the Lie algebra A is **simple** if $\dim A > 1$ and if A contains no nonzero proper ideals.

Working with the field $\mathbb{C}$ but in a way that applies to other fields of characteristic 0, W. Killing proved in 1888 that A is semisimple if and only if A is the (internal) direct sum of simple ideals. In this case the direct summands are unique, and the only ideals in A are the partial direct sums.

This result is strikingly different from what happens for abelian Lie algebras, for which the theory reduces to the theory of vector spaces. A 2-dimensional vector space is the internal direct sum of two 1-dimensional subspaces in many ways. But Killing's theorem says that the decomposition of semisimple Lie algebras into simple ideals is unique, not just unique up to some isomorphism.

É. Cartan in his 1894 thesis classified the simple Lie algebras, up to isomorphism, for the case that the field is $\mathbb{C}$. The Lie algebras $\mathfrak{sl}(n, \mathbb{C})$ for $n \geq 2$ and $\mathfrak{so}(n, \mathbb{C})$ for $n = 3$ and $n \geq 5$ were in his list, and there were others. Killing had come close to this classification in his 1888 work, but he had made a number of errors in both his statements and his proofs.

E. E. Levi in 1905 addressed the extension problem for obtaining all finite-dimensional Lie algebras over $\mathbb{C}$ from semisimple ones and solvable ones. His theorem is that for any Lie algebra A, there exists a subalgebra S isomorphic to $A/\operatorname{rad} A$ such that $A = S \oplus \operatorname{rad} A$ as vector spaces. In essence, this result says that the extension defining A is given by a semidirect product.

The final theorem in this vein at this time in history was a 1914 result of Cartan classifying the simple Lie algebras when the field F is $\mathbb{R}$. This classification is a good bit more complicated than the classification when F is $\mathbb{C}$.

With this background in mind, we can put into context the corresponding developments for associative algebras. Although others had done some earlier work, J. H. M. Wedderburn made the first big advance for associative algebras in 1905. Wedderburn's theory in a certain sense is more complicated than the theory for Lie algebras because left ideals in the associative case are not necessarily two-sided ideals. Let us sketch this theory.

For the remainder of this section until the last paragraph, A will denote a finite-dimensional associative algebra over a field F of characteristic 0, possibly the 0

algebra. We shall always assume that A has an identity. Although we shall make some definitions here, we shall repeat them later in the chapter at the appropriate times. For many results later in the chapter, the field F will not be assumed to be of characteristic 0.

As in Chapter X of *Basic Algebra*, a unital left A module M is said to be simple if it is nonzero and it has no proper nonzero A submodules, semisimple if it is the sum (or equivalently the direct sum) of simple A submodules. The algebra A is **semisimple** if the left A module A is a semisimple module, i.e., if A is the direct sum of simple left ideals; A is **simple** if it is nonzero and has no nontrivial two-sided ideals. In contrast to the setting of Lie algebras, we make no exception for the 1-dimensional case; this distinction is necessary and is continually responsible for subtle differences between the two theories.

Wedderburn's first theorem has two parts to it, the first one modeled on Killing's theorem for Lie algebras and the second one modeled on Cartan's thesis:

(i) The algebra A is semisimple if and only if it is the (internal) direct sum of simple two-sided ideals. In this case the direct summands are unique, and the only two-sided ideals of A are the partial direct sums.

(ii) The algebra A is simple if and only if $A \cong M_n(D)$ for some integer $n \geq 1$ and some division algebra D over F. In particular, if F is algebraically closed, then $A \cong M_n(F)$ for some n.

E. Artin generalized the Wedderburn theory to a suitable kind of "semisimple ring." For part of the theory, he introduced a notion of "radical" for the associative case—the **radical** of a finite-dimensional associative algebra A being the sum of the "nilpotent" left ideals of A. Here a left ideal I is called **nilpotent** if $I^k = 0$ for some k. The radical $\operatorname{rad} A$ is a two-sided ideal, and $A/\operatorname{rad} A$ is a semisimple ring.

Wedderburn's Main Theorem, proved later in time and definitely assuming characteristic 0, is an analog for associative algebras of Levi's result about Lie algebras. The result for associative algebras is that A decomposes as a vector-space direct sum $A = S \oplus \operatorname{rad} A$, where S is a semisimple subalgebra isomorphic to $A/\operatorname{rad} A$.

The remaining structural question for finite-dimensional associative algebras is to say something about simple algebras when the field is not algebraically closed. Such a result may be regarded as an analog of the 1914 work by Cartan. In the associative case one then wants to know what the F isomorphism classes of finite-dimensional associative division algebras D are for a given field F. We now drop the assumption that the field F has characteristic 0. In asking this question, one does not want to repeat the theory of field extensions. Consequently one looks only for classes of division algebras whose center is F. If F is algebraically closed, the only such D is F itself, as we shall observe in more detail in Section 2.

If F is a finite field, one is led to another theorem of Wedderburn's, saying that D has to be commutative and hence that $D = F$; this theorem appears in Section 9. If F is $\mathbb{R}$, one is led to a theorem of Frobenius saying that there are just two such D's up to $\mathbb{R}$ isomorphism, namely $\mathbb{R}$ itself and the quaternions $\mathbb{H}$; this theorem appears in Section 10. For a general field F, it turns out that the set of classes of finite-dimensional division algebras with center F forms an abelian group. The group is called the "Brauer group" of F. Its multiplication is defined by the condition that the class of D_1 times D_2 is the class of a division algebra D_3 such that $D_1 \otimes_F D_2 \cong M_n(D_3)$ for some n; the inverse of the class of D is the class of the opposite algebra D^o, and the identity is the class of F. The study of the Brauer group is postponed to Chapter III. This group has an interpretation in terms of cohomology of groups, and it has applications to algebraic number theory.

2. Semisimple Rings and Wedderburn's Theorem

We now begin our detailed investigation of associative algebras over a field. In this section we shall address the first theorem of Wedderburn's that is mentioned in the previous section. It has two parts, one dealing with semisimple algebras and one dealing with finite-dimensional simple algebras. The first part does not need the finite dimensionality as a hypothesis, and we begin with that one.

Let R be a ring with identity. The ring R is **left semisimple** if the left R module R is a semisimple module, i.e., if R is the direct sum of minimal left ideals.[1] In this case $R = \bigoplus_{i \in S} I_i$ for some set S and suitable minimal left ideals I_i. Since R has an identity, we can decompose the identity according to the direct sum as $1 = 1_{i_1} + \cdots + 1_{i_n}$ for some finite subset $\{i_1, \ldots, i_n\}$ of S, where 1_{i_k} is the component of 1 in I_{i_k}. Multiplying by $r \in R$ on the left, we see that $R \subseteq \bigoplus_{k=1}^n I_{i_k}$. Consequently R has to be a *finite* sum of minimal left ideals. A ring R with identity is **right semisimple** if the right R module R is a semisimple module. We shall see later in this section that left semisimple and right semisimple are equivalent.

EXAMPLES OF SEMISIMPLE RINGS.

(1) If D is a division ring, then we saw in Example 4 in Section X.1 of *Basic Algebra* that the ring $R = M_n(D)$ is left semisimple in the sense of the above definition. Actually, that example showed more. It showed that R as a left R module is given by $M_n(D) \cong D^n \oplus \cdots \oplus D^n$, where each D^n is a simple left R module and the j^{th} summand D^n corresponds to the matrices whose only nonzero entries are in the j^{th} column. The left R module $M_n(D)$ has a composition series whose terms are the partial sums of the n summands D^n. If M is any simple left $M_n(D)$ module and if $x \neq 0$ is in M, then $M = M_n(D)x$. If we set $I = \{r \in M_n(D) \mid rx = 0\}$, then I is a left ideal in $M_n(D)$ and $M \cong M_n(D)/I$

[1] By convention, a "minimal left ideal" always means a "minimal nonzero left ideal."

as a left $M_n(D)$ module. In other words, M is an irreducible quotient module of the left $M_n(D)$ module $M_n(D)$. By the Jordan–Hölder Theorem (Corollary 10.7 of *Basic Algebra*), M occurs as a composition factor. Hence $M \cong D^n$ as a left $M_n(D)$ module. Hence every simple left $M_n(D)$ module is isomorphic to D^n. We shall use this style of argument repeatedly but will ordinarily include less detail.

(2) If $R_1, \dots, R_n$ are left semisimple rings, then the direct product $R = \prod_{i=1}^n R_i$ is left semisimple.[2] In fact, each minimal left ideal of R_i, when included into R, is a minimal left ideal of R. Hence R is the sum of minimal left ideals and is left semisimple. By the same kind of argument as for Example 1, every simple left R module is isomorphic to one of these minimal left ideals.

Lemma 2.1. Let D be a division ring, let $R = M_n(D)$, and let D^n be the simple left R module of column vectors. Each member of D acts on D^n by scalar multiplication on the *right* side, yielding a member of $\mathrm{End}_R(D^n)$. In turn, $\mathrm{End}_R(D^n)$ is a ring, and this identification therefore is an inclusion of the members of D into the right D module $\mathrm{End}_R(D^n)$. The inclusion is in fact an isomorphism of rings: $D^o \cong \mathrm{End}_R(D^n)$, where D^o is the opposite ring of D.

PROOF. Let $\varphi : D \to \mathrm{End}_R(D^n)$ be the function given by $\varphi(d)(v) = vd$. Then $\varphi(dd')(v) = v(dd') = (vd)d' = \varphi(d')(vd) = \varphi(d')(\varphi(d)(v))$. Since the order of multiplication in D is reversed by φ, φ is a ring homomorphism of D^o into $\mathrm{End}_R(D^n)$. It is one-one because D^o is a division ring and has no nontrivial two-sided ideals. To see that it is onto $\mathrm{End}_R(D^n)$, let f be in $\mathrm{End}_R(D^n)$. Put $f\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}d\\d_2\\\vdots\\d_n\end{pmatrix}$. Since f is an R module homomorphism,

$$f\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix} = f\left(\begin{pmatrix}a_1&0&\cdots&0\\a_2&0&\cdots&0\\&\vdots&&\\a_n&0&\cdots&0\end{pmatrix}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\right) = \begin{pmatrix}a_1&0&\cdots&0\\a_2&0&\cdots&0\\&\vdots&&\\a_n&0&\cdots&0\end{pmatrix} f\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$$

$$= \begin{pmatrix}a_1&0&\cdots&0\\a_2&0&\cdots&0\\&\vdots&&\\a_n&0&\cdots&0\end{pmatrix}\begin{pmatrix}d\\d_2\\\vdots\\d_n\end{pmatrix} = \begin{pmatrix}a_1d\\a_2d\\\vdots\\a_nd\end{pmatrix} = \varphi(d)\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}.$$

Therefore $\varphi(d) = f$, and φ is onto. □

[2]Some comment is appropriate about the notation $R = \prod_{i=1}^n R_i$ and the terminology "direct product." Indeed, $\prod_{i=1}^n R_i$ is a product in the sense of category theory within the category of rings or the category of rings with identity. Sometimes one views R alternatively as built from n two-sided ideals, each corresponding to one of the n coordinates; in this case, one may say that R is the "direct sum" of these ideals. This direct sum is to be regarded as a direct sum of abelian groups, or perhaps vector spaces or R modules, but it is not a coproduct within the category of rings with identity.

Theorem 2.2 (Wedderburn). If R is any left semisimple ring, then

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for suitable division rings $D_1, \ldots, D_n$ and positive integers $n_1, \ldots, n_r$. The number r is uniquely determined by R, and the ordered pairs $(n_1, D_1), \ldots, (n_r, D_r)$ are determined up to a permutation of $\{1, \ldots, r\}$ and an isomorphism of each D_j. There are exactly r mutually nonisomorphic simple left R modules, namely $(D_1)^{n_1}, \ldots, (D_r)^{n_r}$.

PROOF. Write R as the direct sum of minimal left ideals, and then regroup the summands according to their R isomorphism type as $R \cong \bigoplus_{j=1}^{r} n_j V_j$, where $n_j V_j$ is the direct sum of n_j submodules R isomorphic to V_j and where $V_i \ncong V_j$ for $i \neq j$. The isomorphism is one of unital left R modules. Put $D_i^o = \mathrm{End}_R(V_i)$. This is a division ring by Schur's Lemma (Proposition 10.4b of *Basic Algebra*). Using Proposition 10.14 of *Basic Algebra*, we obtain an isomorphism of rings

$$R^o \cong \mathrm{End}_R\, R \cong \mathrm{Hom}_R\Big(\bigoplus_{i=1}^{r} n_i V_i, \bigoplus_{j=1}^{r} n_j V_j\Big). \tag{$*$}$$

Define $p_i : \bigoplus_{j=1}^{r} n_j V_j \to n_i V_i$ to be the i^{th} projection and $q_i : n_i V_i \to \bigoplus_{j=1}^{r} n_j V_j$ to be the i^{th} inclusion. Let us see that the right side of $(*)$ is isomorphic as a ring to $\prod_i \mathrm{End}_R(n_i V_i)$ via the mapping $f \mapsto (p_1 f q_1, \ldots, p_r f q_r)$. What is to be shown is that $p_j f q_i = 0$ for $i \neq j$. Here $p_j f q_i$ is a member of $\mathrm{Hom}_R(n_i V_i, n_j V_j)$. The abelian group $\mathrm{Hom}_R(n_i V_i, n_j V_j)$ is the direct sum of abelian groups isomorphic to $\mathrm{Hom}_R(V_i, V_j)$ by Proposition 10.12, and each $\mathrm{Hom}_R(V_i, V_j)$ is 0 by Schur's Lemma (Proposition 10.4a).

Referring to $(*)$, we therefore obtain ring isomorphisms

$$\begin{aligned} R^o &\cong \prod_{i=1}^{r} \mathrm{Hom}_R(n_i V_i, n_i V_i) = \prod_{i=1}^{r} \mathrm{End}_R(n_i V_i) \\ &\cong \prod_{i=1}^{r} M_{n_i}(\mathrm{End}_R(V_i)) && \text{by Corollary 10.13} \\ &\cong \prod_{i=1}^{r} M_{n_i}(D_i^o) && \text{by definition of } D_i^o. \end{aligned}$$

Reversing the order of multiplication in R^o and using the transpose map to reverse the order of multiplication in each $M_{n_i}(D_i^o)$, we conclude that $R \cong \prod_{i=1}^{r} M_{n_i}(D_i)$. This proves existence of the decomposition in the theorem.

We still have to identify the simple left R modules and prove an appropriate uniqueness statement. As we recalled in Example 1, we have a decomposition

$M_{n_i}(D_i) \cong D_i^{n_i} \oplus \cdots \oplus D_i^{n_i}$ of left $M_{n_i}(D_i)$ modules, and each term $D_i^{n_i}$ is a simple left $M_{n_i}(D_i)$ module. The decomposition just proved allows us to regard each term $D_i^{n_i}$ as a simple left R module, $1 \le i \le r$. Each of these modules is acted upon by a different coordinate of R, and hence we have produced at least r nonisomorphic simple left R modules. Any simple left R module must be a quotient of R by a maximal left ideal, as we observed in Example 2, hence a composition factor as a consequence of the Jordan–Hölder Theorem. Thus it must be one of the V_j's in the previous part of the proof. There are only r nonisomorphic such V_j's, and we conclude that the number of simple left R modules, up to isomorphism, is exactly r.

For uniqueness suppose that $R \cong M_{n'_1}(D'_1) \times \cdots \times M_{n'_s}(D'_s)$ as rings. Let $V'_j = (D'_j)^{n'_j}$ be the unique simple left $M_{n'_j}(D'_j)$ module up to isomorphism, and regard V'_j as a simple left R module. Then we have $R \cong \bigoplus_{j=1}^{s} n'_j V'_j$ as left R modules. By the Jordan–Hölder Theorem we must have $r = s$ and, after a suitable renumbering, $n_i = n'_i$ and $V_i \cong V'_i$ for $1 \le i \le r$. Thus we have ring isomorphisms

$$\begin{aligned}
(D'_i)^o &\cong \mathrm{End}_{M_{n'_i}(D'_i)}(V'_i) && \text{by Lemma 2.1}\\
&\cong \mathrm{End}_R(V'_i)\\
&\cong \mathrm{End}_R(V_i) && \text{since } V_i \cong V'_i\\
&\cong D_i^o.
\end{aligned}$$

Reversing the order of multiplication gives $D'_i \cong D_i$, and the proof is complete. □

Corollary 2.3. For a ring R, left semisimple coincides with right semisimple.

REMARK. Therefore we can henceforth refer to left semisimple rings unambiguously as **semisimple**.

PROOF. The theorem gives the form of any left semisimple ring, and each ring of this form is certainly right semisimple. □

Wedderburn's original formulation of Theorem 2.2 was for algebras over a field F, and he assumed finite dimensionality. The theorem in this case gives

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r),$$

and the proof shows that $D_i^o \cong \mathrm{End}_R(V_i)$, where V_i is a minimal left ideal of R of the i^{th} isomorphism type. The field F lies inside $\mathrm{End}_R(V_i)$, each member of F yielding a scalar mapping, and hence each D_i is a division algebra over F. Each D_i is necessarily finite-dimensional over F, since R was assumed to be finite-dimensional.

We shall make occasional use in this chapter of the fact that if D is a finite-dimensional division algebra over an algebraically closed field F, then $D = F$. To see this equality, suppose that x is a member of D but not of F, i.e., is not an F multiple of the identity. Then x and F together generate a subfield $F(x)$ of D that is a nontrivial algebraic extension of F, contradiction. Consequently every finite-dimensional semisimple algebra R over an algebraically closed field F is of the form

$$R \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F),$$

for suitable integers $n_1, \ldots, n_r$.

As we saw, the finite dimensionality plays no role in decomposing semisimple rings as the finite product of rings that we shall call "simple." The place where finite dimensionality enters the discussion is in identifying simple rings as semisimple, hence in establishing a converse theorem that every finite direct product of simple rings, each equal to an ideal of the given ring, is necessarily semisimple. We say that a nonzero ring R with identity is **simple** if its only two-sided ideals are 0 and R.

EXAMPLES OF SIMPLE RINGS.

(1) If D is a division ring, then $M_n(D)$ is a simple ring. In fact, let J be a two-sided ideal in $M_n(D)$, fix an ordered pair (i, j) of indices, and let

$$I = \{x \in D \mid \text{some member } X \text{ of } J \text{ has } X_{ij} = x\}.$$

Multiplying X in this definition on each side by scalar matrices with entries in D, we see that I is a two-sided ideal in D. If $I = 0$ for all (i, j), then $J = 0$. So assume for some (i, j) that $I \neq 0$. Then $I = D$ for that (i, j), and we may suppose that some X in J has $X_{ij} = 1$. If E_{kl} denotes the matrix that is 1 in the $(k, l)^{\text{th}}$ place and is 0 elsewhere, then $E_{ii}XE_{jj} = E_{ij}$ has to be in J. Hence $E_{kl} = E_{ki}E_{ij}E_{jl}$ has to be in J, and $J = M_n(D)$.

(2) Let R be the **Weyl algebra** over $\mathbb{C}$ in one variable, namely

$$R = \Big\{ \sum_{n \geq 0} P_n(x) \Big(\frac{d}{dx}\Big)^n \;\Big|\; \text{each } P_n \text{ is in } \mathbb{C}[x], \text{ and the sum is finite} \Big\}.$$

To give a more abstract construction of R, we can view R as $\mathbb{C}\big[x, \frac{d}{dx}\big]$ subject to the relation $\frac{d}{dx}\, x = x\, \frac{d}{dx} + 1$; this is not to be a quotient of a polynomial algebra in two variables but a quotient of a tensor algebra in two variables. We omit the details. We shall now prove that the ring R is simple but not semisimple.

To see that R is a simple ring, we easily check the two identities

(i) $\frac{d}{dx}\big(x^m\, \frac{d^n}{dx^n}\big) = mx^{m-1}\, \frac{d^n}{dx^n} + x^m\, \frac{d^{n+1}}{dx^{n+1}}$ by the product rule,

(ii) $\frac{d^n}{dx^n}\, x = n\, \frac{d^{n-1}}{dx^{n-1}} + x\, \frac{d^n}{dx^n}$ by induction when applied to a polynomial $f(x)$.

Let I be a nonzero two-sided ideal in R, and fix an element $X \neq 0$ in I. Let x^m be the highest power of x appearing in X, and let $\frac{d^n}{dx^n}$ be the highest power of $\frac{d}{dx}$ appearing in terms of X involving x^m. Let l and r denote "left multiplication by" and "right multiplication by," and apply $\left(l\left(\frac{d}{dx}\right) - r\left(\frac{d}{dx}\right)\right)^m$ to X. Since (i) shows that

$$\left(l\left(\tfrac{d}{dx}\right) - r\left(\tfrac{d}{dx}\right)\right)x^k\left(\tfrac{d}{dx}\right)^l = kx^{k-1}\left(\tfrac{d}{dx}\right)^l,$$

the result of computing $\left(l\left(\frac{d}{dx}\right) - r\left(\frac{d}{dx}\right)\right)^m X$ is a polynomial in $\frac{d}{dx}$ of degree exactly n with no x's. Application of $(r(x) - l(x))^n$ to the result, using (ii), yields a nonzero constant. We conclude that 1 is in I and therefore that $I = R$. Hence R is simple.

To show that R is not semisimple, first note that $\mathbb{C}[x]$ is a natural unital left R module. We shall show that R has infinite length as a left R module, in the sense of the length of finite filtrations. In fact,

$$R \supseteq R\left(\tfrac{d}{dx}\right) \supseteq R\left(\tfrac{d}{dx}\right)^2 \supseteq \cdots \supseteq R\left(\tfrac{d}{dx}\right)^n \qquad (*)$$

is a finite filtration of left R submodules of R. If $R\left(\frac{d}{dx}\right)^k = R\left(\frac{d}{dx}\right)^{k+1}$, then $\left(\frac{d}{dx}\right)^k = r\left(\frac{d}{dx}\right)^{k+1}$ for some $r \in R$. Applying these two equal expressions for a member of R to the member x^k of the left R module $\mathbb{C}[x]$, we arrive at a contradiction and conclude that every inclusion in $(*)$ is strict. Therefore R has infinite length and is not semisimple.

The extra hypothesis that Wedderburn imposed so that simple rings would turn out to be semisimple is finite dimensionality. Wedderburn's result in this direction is Theorem 2.4 below. This hypothesis is quite natural to the extent that the subject was originally motivated by the theory of Lie algebras. E. Artin found a substitute for the assumption of finite dimensionality that takes the result beyond the realm of algebras, and we take up Artin's idea in the next section.

Theorem 2.4 (Wedderburn). Let R be a finite-dimensional algebra with identity over a field F. If R is a simple ring, then R is semisimple and hence is isomorphic to $M_n(D)$ for some integer $n \geq 1$ and some finite-dimensional division algebra D over F. The integer n is uniquely determined by R, and D is unique up to isomorphism.

PROOF. By finite dimensionality, R has a minimal left ideal V. For r in R, form the set Vr. This is a left ideal, and we claim that it is minimal or is 0. In fact, the function $v \mapsto vr$ is R linear from V onto Vr. Since V is simple as a left R module, Vr is simple or 0. The sum $I = \sum_{r \text{ with } Vr \neq 0} Vr$ is a two-sided ideal in R, and it is not 0 because $V1 \neq 0$. Since R is simple, $I = R$. Then the left R module R is exhibited as the sum of simple left R modules and is therefore semisimple. The isomorphism with $M_n(D)$ and the uniqueness now follow from Theorem 2.2. □

3. Rings with Chain Condition and Artin's Theorem

Parts of Chapters VIII and IX of *Basic Algebra* made considerable use of a hypothesis that certain commutative rings are "Noetherian," and we now extend this notion to noncommutative rings. A ring R with identity is **left Noetherian** if the left R module R satisfies the ascending chain condition for its left ideals. It is **left Artinian** if the left R module R satisfies the descending chain condition for its left ideals. The notions of **right Noetherian** and **right Artinian** are defined similarly.

We saw many examples of Noetherian rings in the commutative case in *Basic Algebra*. The ring of integers $\mathbb{Z}$ is Noetherian, and so is the ring of polynomials $R[X]$ in an indeterminate over a nonzero Noetherian ring R. It follows from the latter example that the ring $F[X_1, \dots, X_n]$ in finitely many indeterminates over a field is a Noetherian ring. Other examples arose in connection with extensions of Dedekind domains.

Any finite direct product of fields is Noetherian and Artinian because it has a composition series and because its ideals therefore satisfy both chain conditions. If p is any prime, the ring $\mathbb{Z}/p^2\mathbb{Z}$ is Noetherian and Artinian for the same reason, and it is not a direct product of fields.

In the noncommutative setting, any semisimple ring is necessarily left Noetherian and left Artinian because it has a composition series for its left ideals and the left ideals therefore satisfy both chain conditions.

Proposition 2.5. Let R be a ring with identity, and let M be a finitely generated unital left R module. If R is left Noetherian, then M satisfies the ascending chain condition for its R submodules; if R is left Artinian, then M satisfies the descending chain condition for its R submodules.

PROOF. We prove the first conclusion by induction on the number of generators, and the proof of the second conclusion is completely similar. The result is trivial if M has 0 generators. If $M = Rx$, then M is a quotient of the left R module R and satisfies the ascending chain condition for its R submodules, according to Proposition 10.10 of *Basic Algebra*. For the inductive step with ≥ 2 generators, write $M = Rx_1 + \cdots + Rx_n$ and $N = Rx_1 + \cdots + Rx_{n-1}$. Then N satisfies the ascending chain condition for its R submodules by the inductive hypothesis, and M/N is isomorphic to $Rx_n/(N \cap Rx_n)$, which satisfies the ascending chain condition for its R submodules by the inductive hypothesis. Therefore M satisfies the ascending chain condition for its R submodules by application of the converse direction of Proposition 10.10. □

Artin's theorem (Theorem 2.6 below) will make use of the hypothesis "left Artinian" in identifying those simple rings that are semisimple. The hypothesis

left Artinian may therefore be regarded as a useful generalization of finite dimensionality. Before we come to that theorem, we give a construction that produces large numbers of nontrivial examples of such rings.

EXAMPLE (triangular rings). Let R and S be nonzero rings with identity, and let M be an (R, S) bimodule.[3] Define a set A and operations of addition and multiplication symbolically by

$$A = \begin{pmatrix} R & M \\ 0 & S \end{pmatrix} = \left\{ \begin{pmatrix} r & m \\ 0 & s \end{pmatrix} \,\middle|\, r \in R,\ m \in M,\ s \in S \right\}$$

with

$$\begin{pmatrix} r & m \\ 0 & s \end{pmatrix} \begin{pmatrix} r' & m' \\ 0 & s' \end{pmatrix} = \begin{pmatrix} rr' & rm' + ms' \\ 0 & ss' \end{pmatrix}.$$

Then A is a ring with identity, the bimodule property entering the proof of associativity of multiplication in A. We can identify R, M, and S with the additive subgroups of A given by $\left(\begin{smallmatrix} R & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & M \\ 0 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & S \end{smallmatrix}\right)$. Problems 8–11 at the end of the chapter ask one to check the following facts:

(i) The left ideals in A are of the form $I_1 \oplus I_2$, where I_2 is a left ideal in S and I_1 is a left R submodule of $R \oplus M$ containing MI_2.

(ii) The right ideals in A are of the form $J_1 \oplus J_2$, where J_1 is a right ideal in R and J_2 is a right S submodule of $M \oplus S$ containing $J_1 M$.

(iii) The ring A is left Noetherian if and only if R and S are left Noetherian and M satisfies the ascending chain condition for its left R submodules. The ring A is right Noetherian if and only if R and S are right Noetherian and M satisfies the ascending chain condition for its right S submodules.

(iv) The previous item remains valid if "Noetherian" is replaced by "Artinian" and "ascending" is replaced by "descending."

(v) If $A = \left(\begin{smallmatrix} R & R \\ 0 & S \end{smallmatrix}\right)$ is a ring such as $\left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$ in which S is a (commutative) Noetherian integral domain with field of fractions R and if $S \neq R$, then A is left Noetherian and not right Noetherian, and A is neither left nor right Artinian.

(vi) If $A = \left(\begin{smallmatrix} R & R \\ 0 & S \end{smallmatrix}\right)$ is a ring such as $\left(\begin{smallmatrix} \mathbb{Q}(x) & \mathbb{Q}(x) \\ 0 & \mathbb{Q} \end{smallmatrix}\right)$ in which R and S are fields with $S \subseteq R$ and $\dim_S R$ infinite, then A is left Noetherian and left Artinian, and A is neither right Noetherian nor right Artinian.

From these examples we see, among other things, that "left" and "right" are somewhat independent for both the Noetherian and the Artinian conditions. We

[3] This means that M is an abelian group with the structure of a unital left R module and the structure of a unital right S module in such a way that $(rm)s = r(ms)$ for all $r \in R$, $m \in M$, and $s \in S$.

already know from the commutative case that Noetherian does not imply Artinian, $\mathbb{Z}$ being a counterexample. We shall see in Theorem 2.15 later that left Artinian implies left Noetherian and that right Artinian implies right Noetherian.

Theorem 2.6 (E. Artin). If R is a simple ring, then the following conditions are equivalent:

(a) R is left Artinian,
(b) R is semisimple,
(c) R has a minimal left ideal,
(d) $R \cong M_n(D)$ for some integer $n \geq 1$ and some division ring D.

In particular, a left Artinian simple ring is right Artinian.

REMARK. Theorem 2.4 is a special case of the assertion that (a) implies (d). In fact, if R is a finite-dimensional algebra over a field F, then the finite dimensionality forces R to be left Artinian.

PROOF. It is evident from Wedderburn's Theorem (Theorem 2.2) that (b) and (d) are equivalent. For the rest we prove that (a) implies (c), that (c) implies (b), and that (b) implies (a).

Suppose that (a) holds. Applying the minimum condition for left ideals in R, we obtain a minimal left ideal. Thus (c) holds.

Suppose that (c) holds. Let V be a minimal left ideal. Then the sum $I = \sum_{r \in R} Vr$ is a two-sided ideal in R, and it is nonzero because the term for $r = 1$ is nonzero. Since R is simple, $I = R$. Then the left R module R is spanned by the simple left R modules Vr, and R is semisimple. Thus (b) holds.

Suppose that (b) holds. Since R is semisimple, the left R module R has a composition series. Then the left ideals in R satisfy both chain conditions, and it follows that R is left Artinian. Thus (a) holds. □

4. Wedderburn–Artin Radical

In this section we introduce one notion of "radical" for certain rings with identity, and we show how it is related to semisimplicity. This notion, the "Wedderburn–Artin radical," is defined under the hypothesis that the ring is left Artinian. It is not the only notion of radical studied by ring theorists, however. There is a useful generalization, known as the "Jacobson radical," that is defined for arbitrary rings with identity. We shall not define and use the Jacobson radical in this text.

Fix a ring R with identity. A **nilpotent element** in R is an element a with $a^n = 0$ for some integer $n \geq 1$. A **nil left ideal** is a left ideal in which every element is nilpotent; nil right ideals and nil two-sided ideals are defined similarly.

A **nilpotent left ideal** is a left ideal I such that $I^n = 0$ for some integer $n \geq 1$, i.e., for which $a_1 \cdots a_n = 0$ for all n-fold products of elements from I; nilpotent right ideals and nilpotent two-sided ideals are defined similarly.

Lemma 2.7. If I_1 and I_2 are nilpotent left ideals in a ring R with identity, then $I_1 + I_2$ is nilpotent.

PROOF. Let $I_1^r = 0$ and $I_2^s = 0$. Expand $(I_1 + I_2)^k$ as $\sum I_{i_1} I_{i_2} \cdots I_{i_k}$ with each i_j equal to 1 or 2. Take $k = r + s$. In any term of the sum, there are $\geq r$ indices 1 or $\geq s$ indices 2. In the first case let there be t indices 2 at the right end. Since $I_2 I_1 \subseteq I_1$, we can absorb all other indices 2, and the term of the sum is contained in $I_1^r I_2^t = 0$. Similarly in the second case if there are t' indices 1 at the right end, then the term is contained in $I_2^s I_1^{t'} = 0$. □

Lemma 2.8. If I is a nilpotent left ideal in a ring R with identity, then I is contained in a nilpotent two-sided ideal J.

PROOF. Put $J = \sum_{r \in R} Ir$. This is a two-sided ideal. For any integer $k \geq 0$, $J^k = \left(\sum_{r \in R} Ir\right)^k \subseteq \sum_{r_1, \ldots, r_k} Ir_1 Ir_2 \cdots Ir_k \subseteq \sum_{r_k} I^k r_k$. If $I^k = 0$, then $J^k = 0$. □

Lemma 2.9. If R is a ring with identity, then the sum of all nilpotent left ideals in a nil two-sided ideal.

PROOF. Let K be the sum of all nilpotent left ideals in R, and let a be a member of K. Write $a = a_1 + \cdots + a_n$ with $a_i \in I_i$ for a nilpotent left ideal I_i. Lemma 2.7 shows that $I = \sum_{i=1}^n I_i$ is a nilpotent left ideal. Since a is in I, a is a nilpotent element.

The set K is certainly a left ideal, and we need to see that aR is in K in order to see that K is a two-sided ideal. Lemma 2.8 shows that $I \subseteq J$ for some nilpotent two-sided ideal J. Then $J \subseteq K$ because J is one of the nilpotent left ideals whose sum is K. Since a is in I and therefore in J and since J is a two-sided ideal, aR is contained in J. Therefore aR is contained in K, and K is a two-sided ideal. □

Theorem 2.10. If R is a left Artinian ring, then any nil left ideal in R is nilpotent.

REMARK. Readers familiar with a little structure theory for finite-dimensional Lie algebras will recognize this theorem as an analog for associative algebras of Engel's Theorem.

PROOF. Let I be a nil left ideal of R, and form the filtration

$$I \supseteq I^2 \supseteq I^3 \supseteq \cdots .$$

Since R is left Artinian, this filtration is constant from some point on, and we have $I^k = I^{k+1} = I^{k+2} = \cdots$ for some $k \geq 1$. Put $J = I^k$. We shall show that $J = 0$, and then we shall have proved that I is a nilpotent ideal.

Suppose that $J \neq 0$. Since $J^2 = I^{2k} = I^k = J$, we have $J^2 = J$. Thus the left ideal J has the property that $JJ \neq 0$. Since R is left Artinian, the set of left ideals $K \subseteq J$ with $JK \neq 0$ has a minimal element K_0. Choose $a \in K_0$ with $Ja \neq 0$. Since $Ja \subseteq JK_0 \subseteq K_0$ and $J(Ja) = J^2a = Ja \neq 0$, the minimality of K_0 implies that $Ja = K_0$. Thus there exists $x \in J$ with $xa = a$. Applying powers of x, we obtain $x^n a = a$ for every integer $n \geq 1$. But x is a nilpotent element, being in I, and thus we have a contradiction. □

Corollary 2.11. If R is a left Artinian ring, then there exists a unique largest nilpotent two-sided ideal I in R. This ideal is the sum of all nilpotent left ideals and also is the sum of all nilpotent right ideals.

REMARKS. The two-sided ideal I of the corollary is called the **Wedderburn–Artin radical** of R and will be denoted by rad R. This exists under the hypothesis that R is left Artinian.

PROOF. By Lemma 2.9 and Theorem 2.10 the sum of all nilpotent left ideals in R is a two-sided nilpotent ideal I. Lemma 2.8 shows that any nilpotent right ideal is contained in a nilpotent two-sided ideal J. Since J is in particular a nilpotent left ideal, the definition of I forces $J \subseteq I$. Hence the sum of all nilpotent right ideals is contained in I. But I itself is a nilpotent right ideal and hence equals the sum of all the nilpotent right ideals. □

Lemma 2.12 (Brauer's Lemma). If R is any ring with identity and if V is a minimal left ideal in R, then either $V^2 = 0$ or $V = Re$ for some element e of V with $e^2 = e$.

REMARK. An element e with the property that $e^2 = e$ is said to be **idempotent**.

PROOF. Being a minimal left ideal, V is a simple left R module. Schur's Lemma (Proposition 10.4b of *Basic Algebra*) shows that $\mathrm{End}_R V$ is a division ring. If a is in V, then the map $v \mapsto va$ of V into itself lies in $\mathrm{End}_R V$ and hence is the 0 map or is one-one onto. If it is the 0 map for all $a \in V$, then $V^2 = 0$. Otherwise suppose that a is an element for which $v \mapsto va$ is one-one onto. Then there exists $e \in V$ with $ea = a$. Multiplying on the left by e gives $e^2a = ea$ and therefore $(e^2 - e)a = 0$. Since the map $v \mapsto va$ is assumed to be one-one onto, we must have $e^2 - e = 0$ and $e^2 = e$. □

Theorem 2.13. If R is a left Artinian ring and if the Wedderburn–Artin radical of R is 0, then R is a semisimple ring.

REMARKS. Conversely semisimple rings are left Artinian and have radical 0. In fact, we already know that semisimple rings have a composition series for their left ideals and hence are left Artinian. To see that the radical is 0, apply Theorem 2.2 and write the ring as $R = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$. The two-sided ideals of R are the various subproducts, with 0 in the missing coordinates. Such a subproduct cannot be nilpotent as an ideal unless it is 0, since the identity element in any factor is not a nilpotent element in R.

PROOF. Let us see that any minimal left ideal I of R is a direct summand as a left R submodule. Since $\operatorname{rad} R = 0$, I is not nilpotent. Thus $I^2 \neq 0$, and Lemma 2.12 shows that I contains an idempotent e. This element satisfies $I = Re$. Put $I' = \{r \in R \mid re = 0\}$. Then I' is a left ideal in R. Since $I' \cap I \subseteq I$ and e is not in I', the minimality of I forces $I' \cap I = 0$. Writing $r = re + (r - re)$ with $re \in I$ and $r - re \in I'$, we see that $R = I + I'$. Therefore $R = I \oplus I'$.

Now put $I_1 = I$. If I' is not 0, choose a minimal left ideal $I_2 \subseteq I'$ by the minimum condition for left ideals in R. Arguing as in the previous paragraph, we have $I_2 = Re_2$ for some element e_2 with $e_2^2 = e_2$. The argument in the previous paragraph shows that $R = I_2 \oplus I_2'$, where $I_2' = \{r \in R \mid re_2 = 0\}$. Define $I'' = \{r \in R \mid re_1 = re_2 = 0\} = I' \cap I_2'$. Since I_2 is contained in I', we can intersect $R = I_2 \oplus I_2'$ with I' and obtain $I' = I_2 \oplus I''$. Then $R = I_1 \oplus I' = I_1 \oplus I_2 \oplus I''$. Continuing in this way, we obtain $R = I_1 \oplus I_2 \oplus I_3 \oplus I'''$, etc. As this construction continues, we have $I' \supseteq I'' \supseteq I''' \supseteq \cdots$. Since R is left Artinian, this sequence must terminate, evidently in 0. Then R is exhibited as the sum of simple left R modules and is semisimple. □

Corollary 2.14. If R is a left Artinian ring, then $R/\operatorname{rad} R$ is a semisimple ring.

PROOF. Let $I = \operatorname{rad} R$, and let $\varphi : R \to R/I$ be the quotient homomorphism. Arguing by contradiction, let $\overline{J}$ be a nonzero nilpotent left ideal in R/I, and let $J = \varphi^{-1}(\overline{J}) \subseteq R$. Since $\overline{J}$ is nilpotent, $J^k \subseteq I$ for some integer $k \geq 1$. But I, being the radical, is nilpotent, say with $I^l = 0$, and hence $J^{k+l} \subseteq I^l = 0$. Therefore J is a nilpotent left ideal in R strictly containing I, in contradiction to the maximality of I. We conclude that no such $\overline{J}$ exists. Then $\operatorname{rad}(R/\operatorname{rad} R) = 0$. Since $R/\operatorname{rad} R$ is left Artinian as a quotient of a left Artinian ring, Theorem 2.13 shows that $R/\operatorname{rad} R$ is a semisimple ring. □

We shall use this corollary to prove that left Artinian rings are left Noetherian. We state the theorem, state and prove a lemma, and then prove the theorem.

Theorem 2.15 (Hopkins). If R is a left Artinian ring, then R is left Noetherian.

Lemma 2.16. If R is a semisimple ring, then every unital left R module M is semisimple. Consequently any unital left R module satisfying the descending chain condition has a composition series and therefore satisfies the ascending chain condition.

PROOF. For each $m \in M$, let R_m be a copy of the left R module R, and define $\widetilde{M} = \bigoplus_{m \in M} R_m$ as a left R module. Since each R_m is semisimple, $\widetilde{M}$ is semisimple. Define a function $\varphi : \widetilde{M} \to M$ as follows: if $r_{m_1} + \cdots + r_{m_k}$ is given with r_{m_j} in R_{m_j} for each j, let $\varphi(r_{m_1} + \cdots + r_{m_k}) = \sum_{j=1}^{k} r_{m_j} m_j$. Then φ is an R module map with the property that $\varphi(1_m) = m$, and consequently φ carries $\widetilde{M}$ onto M. As the image of a semisimple R module under an R module map, M is semisimple.

Now suppose that M is a unital left R module satisfying the descending chain condition. We have just seen that M is semisimple, and thus we can write $M = \bigoplus_{i \in S} M_i$ as a direct sum over a set S of simple left R modules M_i. Let us see that S is a finite set. If S were not a finite set, then we could choose an infinite sequence $i_1, i_2, \ldots$ of distinct members of S, and we would obtain

$$M \supsetneqq \bigoplus_{i \neq i_1} M_i \supsetneqq \bigoplus_{i \neq i_1, i_2} M_i \supsetneqq \cdots,$$

in contradiction to the fact that the R submodules of M satisfy the descending chain condition. □

PROOF OF THEOREM 2.15. Let $I = \operatorname{rad} R$. Since I is nilpotent, $I^n = 0$ for some n. Each I^k for $k \geq 0$ is a left R submodule of R. Since R is left Artinian, its left R submodules satisfy the descending chain condition, and the same thing is true of the R submodules of each I^k. Consequently the R submodules of each I^k/I^{k+1} satisfy the descending chain condition.

In the action of R on I^k/I^{k+1} on the left, I acts as 0. Hence I^k/I^{k+1} becomes a left R/I module, and the R/I submodules of this left R/I module must satisfy the descending chain condition. Corollary 2.14 shows that $R/I = R/\operatorname{rad} R$ is a semisimple ring. Since the R/I submodules of I^k/I^{k+1} satisfy the descending chain condition, Lemma 2.16 shows that these R/I submodules satisfy the ascending chain condition. Therefore the R submodules of each left R module I^k/I^{k+1} satisfy the ascending chain condition.

We shall show inductively for $k \geq 0$ that the R submodules of R/I^{k+1} satisfy the ascending chain condition. Since $I^n = 0$, this conclusion will establish that R is left Noetherian, as required. The case $k = 0$ was shown in the previous paragraph. Assume inductively that the R submodules of R/I^k satisfy the ascending chain condition. Since $R/I^k \cong (R/I^{k+1})\big/(I^k/I^{k+1})$ and since the R submodules of R/I^k and of I^k/I^{k+1} satisfy the ascending chain condition, the same is true for R/I^{k+1}. This completes the proof. □

5. Wedderburn's Main Theorem

Wedderburn's Main Theorem is an analog for finite-dimensional associative algebras over a field of characteristic 0 of the Levi decomposition of a finite-dimensional Lie algebra over a field of characteristic 0. Each of these results says that the given algebra is a "semidirect product" of the radical and a semisimple subalgebra isomorphic to the quotient of the given algebra by the radical. In other words, the whole algebra, as a vector space, is the direct sum of the radical and a vector subspace that is closed under multiplication.

An example of this phenomenon occurs with a block upper-triangular subalgebra A of $M_n(D)$ whenever D is a finite-dimensional division algebra over the given field. Let the diagonal blocks be of sizes $n_1, \dots, n_r$ with $n_1 + \cdots + n_r = n$. The radical rad A is the nilpotent ideal of all matrices whose only nonzero entries are above and to the right of the diagonal blocks, and the semisimple subalgebra consists of all matrices whose only nonzero entries lie within the diagonal blocks.

Theorem 2.17 (Wedderburn's Main Theorem). Let A be a finite-dimensional associative algebra with identity over a field F of characteristic 0, and let rad A be the Wedderburn–Artin radical. Then there exists a subalgebra S of A isomorphic as an F algebra to $A/\operatorname{rad} A$ such that $A = S \oplus \operatorname{rad} A$ as vector spaces.

REMARKS. The finite dimensionality implies that A is left Artinian, and Corollary 2.14 shows that $A/\operatorname{rad} A$ is a semisimple algebra. The decomposition $A = S \oplus \operatorname{rad} A$ is different in nature from the one in Theorem 2.2, which involves complementary ideals. When there are complementary ideals, the identity of A decomposes as the sum of the identities for each summand. Here the identity of A is the identity of S and has 0 component in rad A. To see this, write $1 = a + b$ with $a \in S$ and $b \in \operatorname{rad} A$. Multiplying $1 = a + b$ on the left and right by $s \in S$, we see that $as = s = sa$ and that $bs = sb = 0$. Hence $a = 1_S$ is the identity of S. Then $b^2 = (1 - 1_S)^2 = 1 - 2 \cdot 1_S + 1_S^2 = 1 - 2 \cdot 1_S + 1_S = 1 - 1_S = b$, and $b^n = b$ for all $n \geq 1$. Since rad A is nilpotent, $b^n = 0$ for some n. Thus $b = 0$, and $1 = 1_S$ as asserted.

Theorem 2.17 is a deep result, and the proof will occupy all of the present section and the next. The key special case to understand occurs when $A/\operatorname{rad} A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$. We shall handle this case by means of Theorem 2.18 below, whose proof will be the main goal of the present section. Corollary 2.27 (of Theorem 2.18) near the end of this section will show that Theorem 2.18 implies this special case of Theorem 2.17 for $r = 1$, and Corollary 2.28 will deduce this special case of Theorem 2.17 for general r from Corollary 2.27.

Theorem 2.18. Let A be a left Artinian ring with Wedderburn–Artin radical rad A, and suppose that $A/\operatorname{rad} A$ is simple, i.e., is of the form $A/\operatorname{rad} A \cong M_n(D)$ for some division ring D. Then A is isomorphic as a ring to $M_n(R)$ for some left Artinian ring R such that $R/\operatorname{rad} R \cong D$.

The idea behind the proof of Theorem 2.18 is to give an abstract characterization of a ring of matrices in terms of the elements E_{ij} that are 1 in the $(i, j)^{\text{th}}$ place and are 0 elsewhere. In turn, these elements arise from the diagonal such elements E_{ii}, which are idempotents, i.e., have $E_{ii}^2 = E_{ii}$. The critical issue in the proof of Theorem 2.18 is to show that each idempotent of $A/\operatorname{rad} A$, which is assumed to be a full matrix ring $M_n(D)$, has an idempotent in its preimage in A. The lifted idempotents then point to $M_n(R)$ for a certain R.

Thus we begin with some discussion of idempotents. We shall intersperse facts about general rings with facts about left Artinian rings as we go along. For the moment let R be any ring with identity, and let e be an idempotent. Then $1 - e$ is an idempotent, and we have the three **Peirce**[4] **decompositions**

$$\begin{aligned} R &= Re \oplus R(1-e), \\ R &= eR \oplus (1-e)R, \\ R &= eRe \oplus eR(1-e) \oplus (1-e)Re \oplus (1-e)R(1-e). \end{aligned}$$

All the direct sums may be regarded as direct sums of abelian groups. The two members of the right side in the first case are left ideals, and the two members of the right side in the second case are right ideals. If $r \in R$ is given, then the first decomposition is as $r = re + r(1 - e)$; the decomposition is direct because if $r_1 e = r_2(1 - e)$, then right multiplication by e gives $r_1 e = 0$ since $e^2 = e$. The second decomposition is proved similarly, and the third decomposition follows by combining the first two. In the third decomposition, eRe is a ring with e as identity, and $(1 - e)R(1 - e)$ is a ring with $1 - e$ as identity.

EXAMPLE. Let $R = M_n(F)$, and let

$$e = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}, \quad \text{so that} \quad 1 - e = \begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}.$$

[4]Pronounced "purse." Charles Sanders Peirce (1839–1914).

In block form we then have

$$eRe = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}, \qquad eR(1-e) = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix},$$

$$(1-e)Re = \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}, \qquad (1-e)R(1-e) = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}.$$

Proposition 2.19. In a ring R with identity, let e be an element of R with $e^2 = e$.

(a) If I is a left ideal in eRe, then $eRI = I$. Hence $I \mapsto RI$ is a one-one inclusion-preserving map of the left ideals of eRe to those of R.

(b) If J is a two-sided ideal of eRe, then $e(RJR)e = J$. Hence $J \mapsto RJR$ is a one-one inclusion-preserving map of the two-sided ideals of eRe to those of R. This map respects multiplication of ideals.

(c) If $\widetilde{J}$ is a two-sided ideal of R, then $e\widetilde{J}e$ is a two-sided ideal of eRe, and $eRe \cap \widetilde{J} = e\widetilde{J}e$.

PROOF. For (a), we have $eRI = eR(eI) = (eRe)I = I$, the first equality holding because e is the identity in eRe and the third equality holding because eRe contains its identity e. The rest of (a) then follows.

For (b), J satisfies $J = eJe$, since $ej = je = j$ for every $j \in eRe$, and therefore $eRJRe = eReJeRe = (eRe)J(eRe) = J$, the last equality holding because eRe contains its identity e. To see that $J \mapsto RJR$ respects multiplication, we compute that $(RJR)(RJ'R) = RJRJ'R = R(Je)R(eJ')R = RJ(eRe)J'R = RJJ'R$.

For (c), $eRe \cap \widetilde{J} \supseteq e\widetilde{J}e$ certainly. In the reverse direction, let j be in $eRe \cap \widetilde{J}$. Then $j = ere$ for some $r \in R$, and hence $eje = e^2re^2 = ere = j$ shows that j is in $e\widetilde{J}e$. □

Corollary 2.20. In a left Artinian ring R, let e be an element with $e^2 = e$. Then the ring eRe is left Artinian, and

$$\operatorname{rad}(eRe) = eRe \cap \operatorname{rad} R = e(\operatorname{rad} R)e.$$

If $\overline{R}$ denotes the quotient ring $R/\operatorname{rad} R$ and $\bar{e}$ denotes the element $e + \operatorname{rad} R$ of the quotient, then the quotient map carries eRe onto $\bar{e}\overline{R}\bar{e}$ and has kernel $\operatorname{rad}(eRe)$. Consequently

$$eRe/\operatorname{rad}(eRe) \cong \bar{e}\overline{R}\bar{e}.$$

PROOF. The ring eRe is left Artinian as an immediate consequence of Proposition 2.19a. For the first display we may assume that R and eRe are both left Artinian. Then $eRe \cap \operatorname{rad} R$ is a two-sided ideal of eRe, and $(eRe \cap \operatorname{rad} R)^n \subseteq$

$(\operatorname{rad} R)^n$ for every n. Since $(\operatorname{rad} R)^N = 0$ for some N, $eRe \cap \operatorname{rad} R$ is nilpotent, and $eRe \cap \operatorname{rad} R \subseteq \operatorname{rad}(eRe)$. Since the reverse inclusion is evident, we obtain $\operatorname{rad}(eRe) = eRe \cap \operatorname{rad} R$. The equality $eRe \cap \operatorname{rad} R = e(\operatorname{rad} R)e$ is the special case of Proposition 2.19c in which $\widetilde{J} = \operatorname{rad} R$. This proves the equalities in the first display.

For the isomorphism in the second display, the quotient mapping carries ere to $ere + \operatorname{rad} R = (e + \operatorname{rad} R)(r + \operatorname{rad} R)(e + \operatorname{rad} R) = \bar{e}(r + \operatorname{rad} R)\bar{e}$. Thus the quotient map $R \to \overline{R}$ carries eRe onto $\bar{e}\overline{R}\bar{e}$. The kernel is $eRe \cap \operatorname{rad} R$, which we have just proved is $\operatorname{rad}(eRe)$. Therefore the quotient map exhibits an isomorphism of rings $eRe/\operatorname{rad}(eRe) \cong \bar{e}\overline{R}\bar{e}$. □

Proposition 2.21. In a ring R with identity, let e_1 and e_2 be idempotents. Then the unital left R modules Re_1 and Re_2 are isomorphic as left R modules if and only if there exist elements e_{12} and e_{21} in R such that

$$e_1e_{12}e_2 = e_{12}, \qquad e_2e_{21}e_1 = e_{21},$$
$$e_{12}e_{21} = e_1, \qquad e_{21}e_{12} = e_2.$$

REMARK. In this case we shall say that e_1 and e_2 are **isomorphic idempotents**, and we shall write $e_1 \cong e_2$.

PROOF. Let $\varphi : Re_1 \to Re_2$ be an R isomorphism. Define $e_{12} = \varphi(e_1)$ and $e_{21} = \varphi^{-1}(e_2)$. Every element s of Re_2 has the property that $se_2 = s$ because $e_2^2 = e_2$; since e_{12} lies in Re_2, $e_{12}e_2 = e_{12}$. Meanwhile, $e_{12} = \varphi(e_1) = \varphi(e_1^2) = e_1\varphi(e_1) = e_1e_{12}$. Putting these two facts together gives $e_{12} = e_{12}e_2 = e_1e_{12}e_2$. This proves the first equality in the display, and the equality $e_{21} = e_2e_{21}e_1$ is proved similarly. Also, $e_1 = \varphi^{-1}(\varphi(e_1)) = \varphi^{-1}(e_{12}) = \varphi^{-1}(e_{12}e_2) = e_{12}\varphi^{-1}(e_2) = e_{12}e_{21}$, and similarly $e_{21}e_{12} = e_2$. This completes the proof that an R isomorphism $Re_1 \cong Re_2$ leads to elements e_{12} and e_{21} such that the four displayed identities hold.

For the converse, suppose that e_{12} and e_{21} exist and satisfy the four displayed identities. Define $\varphi : Re_1 \to R$ by $\varphi(re_1) = re_{12}$. To see that this map is well defined, suppose that $re_1 = 0$; then $re_{12} = r(e_1e_{12}e_2) = (re_1)e_{12}e_2 = 0$, as required. Similarly we can define $\psi : Re_2 \to R$ by $\psi(re_2) = re_{21}$. Then

$$\psi\varphi(e_1) = \psi(e_{12}) = \psi(e_{12}e_2) = e_{12}\psi(e_2) = e_{12}e_{21} = e_1,$$

and similarly $\varphi\psi(e_2) = e_2$. Since $\psi\varphi$ and $\varphi\psi$ are R module homomorphisms, each is the identity on its domain. □

Corollary 2.22. Let R be a left Artinian ring. For each r in R, let $\bar{r}$ be the coset $r + \operatorname{rad} R$ in $R/\operatorname{rad} R$. If e_1 and e_2 are idempotents in R, then e_1 and e_2 are isomorphic if and only if $\bar{e}_1$ and $\bar{e}_2$ are isomorphic.

PROOF. If e_1 and e_2 are given as isomorphic in R, let e_{12} and e_{21} be as in Proposition 2.21, and pass to $R/\operatorname{rad} R$ by the quotient homomorphism to obtain elements $\bar{e}_{12}$ and $\bar{e}_{21}$ that exhibit $\bar{e}_1$ and $\bar{e}_2$ as isomorphic idempotents.

Conversely let $\bar{e}_1$ and $\bar{e}_2$ be isomorphic idempotents in $R/\operatorname{rad} R$, and use Proposition 2.21 to produce elements $\bar{u}_{12}$ and $\bar{u}_{21}$ in $R/\operatorname{rad} R$ such that

$$\bar{e}_1\bar{u}_{12}\bar{e}_2 = \bar{u}_{12}, \quad \bar{e}_2\bar{u}_{21}\bar{e}_1 = \bar{u}_{21}, \quad \bar{u}_{12}\bar{u}_{21} = \bar{e}_1, \quad \bar{u}_{21}\bar{u}_{12} = \bar{e}_2.$$

Let u_{12} and u_{21} be preimages of $\bar{u}_{12}$ and $\bar{u}_{21}$ in R. Possibly replacing u_{12} by $e_1u_{12}e_2$ and u_{21} by $e_2u_{21}e_1$, we may assume that $e_1u_{12}e_2 = u_{12}$ and $e_2u_{21}e_1 = u_{21}$. Our construction is such that $u_{12}u_{21} = e_1 - z_1$ with z_1 in rad R and $e_1z_1 = z_1 = z_1e_1$. Since z_1 is a nilpotent element,

$$(e_1 - z_1)(e_1 + z_1 + z_1^2 + \cdots + z_1^n) = e_1$$

as soon as $z_1^{n+1} = 0$. Thus we have $u_{12}u_{21}(e_1 + z_1 + z_1^2 + \cdots + z_1^n) = e_1$. Define $e_{12} = u_{12}$ and $e_{21} = u_{21}(e_1 + z_1 + z_1^2 + \cdots + z_1^n)$. Then it is immediate that $\bar{e}_{12} = \bar{u}_{12}$, $\bar{e}_{21} = \bar{u}_{21}$, and $e_{12}e_{21} = e_1$. Also, the equality $e_1u_{12}e_2 = u_{12}$ implies that $e_1e_{12}e_2 = e_{12}$, and the equality $e_2u_{21}e_1(e_1 + z_1 + z_1^2 + \cdots + z_1^n) = u_{21}(e_1 + z_1 + z_1^2 + \cdots + z_1^n)$ implies that $e_2e_{21}e_1 = e_{21}$ since $e_1z_1 = z_1 = z_1e_1$.

In view of Proposition 2.21, we are left with checking the value of $e_{21}e_{12}$. We know that $\bar{e}_{21}\bar{e}_{12} = \bar{u}_{21}\bar{u}_{12} = \bar{e}_2$, and hence $e_{21}e_{12} = e_2 - z_2$ for some z_2 in rad R. Multiplying by e_2 on both sides, we see that

$$e_2z_2 = z_2 = z_2e_2. \tag{$*$}$$

Now $(e_{21}e_{12})(e_{21}e_{12}) = e_{21}e_1e_{12} = e_{21}e_{12}$, and thus $(e_2 - z_2)^2 = e_2 - z_2$. Expanding out this equality and using $(*)$ gives $e_2 - 2z_2 + z_2^2 = e_2 - z_2$ and therefore gives $z_2^2 = z_2$. Hence $z_2^n = z_2$ for every $n \geq 1$. But z_2 is in rad R, and every element of rad R is nilpotent. Thus $z_2 = 0$, and $e_{12}e_{21} = e_1$ as required. □

The proof of Corollary 2.22 shows a little more than the statement asserts, and we shall use this little extra conclusion when we finally get to the proof of Theorem 2.18. The extra fact is that any elements $\bar{u}_{12}$ and $\bar{u}_{21}$ exhibiting $\bar{e}_1$ and $\bar{e}_2$ have lifts to elements e_{12} and e_{21} exhibiting e_1 and e_2 as isomorphic.

The critical step of lifting a single idempotent from $A/\operatorname{rad} A$ to A is accomplished by the following proposition.

Proposition 2.23. Let R be a left Artinian ring. For each r in R, let $\bar{r}$ be the element $r + \operatorname{rad} R$ of $R/\operatorname{rad} R$. If a is an element of R such that $\bar{a}$ is idempotent in $R/\operatorname{rad} R$, then there exists an idempotent e in R such that $\bar{e} = \bar{a}$.

PROOF. Set $b = 1 - a$. The elements a and b commute, and $ab = a(1-a)$ maps to $\bar{a} - \bar{a}^2 = 0$ in $R/\operatorname{rad} R$, since $\bar{a}$ is idempotent. Therefore ab lies in $\operatorname{rad} R$ and must satisfy $(ab)^n = 0$ for some n. Since a and b commute, we can apply the Binomial Theorem to obtain

$$1 = (a+b)^{2n} = \sum_{k=0}^{2n} \tbinom{2n}{k} a^{2n-k} b^k.$$

Define $$e = \sum_{k=0}^{n} \tbinom{2n}{k} a^{2n-k} b^k \quad \text{and} \quad f = \sum_{k=n+1}^{2n} \tbinom{2n}{k} a^{2n-k} b^k.$$

Each term of e contains at least the n^{th} power of a, and each term of b contains at least the n^{th} power of b. Thus each term of ef contains at least a factor $a^n b^n = (ab)^n = 0$, and we see that $ef = 0$. Therefore $e = e1 = e(e+f) = e^2 + 0 = e^2$, and e is an idempotent. Each term of e except the one for $k = 0$ contains a factor ab, and thus $e \equiv a^{2n} \bmod \operatorname{rad} R$. Since $\bar{a}$ is idempotent, $a^{2n} \equiv a \bmod \operatorname{rad} R$, and therefore $\bar{e} = \bar{a}$. □

For the proof of Theorem 2.18, we need to lift an entire matrix ring to obtain a matrix ring, and this involves lifting more than a single idempotent. In effect, we have to lift compatibly an entire system $\bar{e}_{ij}$ that behaves like the usual system of E_{ij} for matrices. The idea is that if $R/\operatorname{rad} R$ is a matrix ring $M_n(K)$ with some ring of coefficients K, then the i^{th} and j^{th} columns of $M_n(K)$ may be described compatibly as $M_n(K)\bar{e}_{ii}$ and $M_n(K)\bar{e}_{jj}$. Proposition 2.23 allows us to lift $\bar{e}_{ii}$ and $\bar{e}_{jj}$ to idempotents e_{ii} and e_{jj}, and Corollary 2.22 shows that an isomorphism $\bar{e}_{ii} \cong \bar{e}_{jj}$ implies an isomorphism $e_{ii} \cong e_{jj}$. The isomorphism gives us elements e_{ij} and e_{ji}, and then we can piece these together to form matrices.

Two idempotents e and f in a ring R with identity are said to be **orthogonal** if $ef = 0 = fe$. Suppose that $e_1, \ldots, e_n$ are mutually orthogonal idempotents such that $\sum_{i=1}^n e_i = 1$. Let us see in this case that

$$R = Re_1 \oplus \cdots \oplus Re_n$$

as left R modules. In fact, the condition $\sum_{i=1}^n e_i = 1$ shows that $r = \sum_{i=1}^n re_i$ for each $r \in R$, and thus $R = Re_1 + \cdots + Re_n$. If r lies in $Re_j \cap \sum_{i \neq j} Re_i$, then $r = se_j$ and $r = \sum_{i \neq j} r_i e_i$. Multiplying the first of these equalities on the right by e_j gives $re_j = se_j^2 = se_j = r$. Hence the second of these equalities, upon multiplication by e_j, yields $r = re_j = \sum_{i \neq j} r_i e_i e_j = 0$. In other words, the sum is direct, as asserted.

Corollary 2.24. Let R be a left Artinian ring. For each r in R, let $\bar{r}$ be the coset $r + \operatorname{rad} R$ in $R/\operatorname{rad} R$. If x and y are orthogonal idempotents in $\overline{R} = R/\operatorname{rad} R$ and if e is an idempotent in R with $\bar{e} = x$, then there exists an idempotent f in R with $\bar{f} = y$ and $ef = fe = 0$.

PROOF. By Proposition 2.23 choose an idempotent f_0 in R with $\bar{f_0} = y$. Then f_0e has $\overline{f_0e} = yx = 0$. Hence f_0e is in rad R, and $(f_0e)^{n+1} = 0$ for some n. Consequently $1 + f_0e + (f_0e)^2 + \cdots + (f_0e)^n$ is a two-sided inverse to $1 - f_0e$. Define

$$f = (1-e)\big(1 + f_0e + (f_0e)^2 + \cdots + (f_0e)^n\big) f_0(1 - f_0e).$$

Then $\bar{f} = (1-x)(y+0+\cdots+0)y(1-0) = (1-x)y = y-xy = y$. Moreover,

$$fe = (1-e)\big(1 + f_0e + (f_0e)^2 + \cdots + (f_0e)^n\big)(f_0e - f_0^2e^2) = 0$$

since $f_0e - f_0^2e^2 = f_0e - f_0e = 0$, and

$$ef = e(1-e)\big(1 + f_0e + (f_0e)^2 + \cdots + (f_0e)^n\big) f_0(1 - f_0e) = 0$$

since $e(1-e) = 0$.

We still need to see that $f^2 = 0$. Since $f_0(1 - f_0e) = f_0(1-e)$, we can write $f = (1-e)(1 + f_0e + \cdots) f_0(1-e)$ and

$$\begin{aligned} f^2 &= (1-e)(1 + f_0e + \cdots) f_0(1-e)(1 + f_0e + \cdots) f_0(1-e) \\ &= (1-e)(1 + f_0e + \cdots) f_0(1 - f_0e)(1 + f_0e + \cdots) f_0(1-e) \\ &= (1-e)(1 + f_0e + \cdots) f_0 \cdot 1 \cdot f_0(1-e) \\ &= (1-e)(1 + f_0e + \cdots) f_0(1 - f_0e) \\ &= f, \end{aligned}$$

as required. □

Corollary 2.25. Let R be a left Artinian ring. For each r in R, let $\bar{r}$ be the coset $r +$ rad R in $R/\text{rad}\, R$. If $\{x_1, \ldots, x_N\}$ is a finite set of mutually orthogonal idempotents in $\overline{R} = R/\text{rad}\, R$, then there exists a set of mutually orthogonal idempotents $\{e_1, \ldots, e_N\}$ in R such that $\bar{e}_i = x_i$ for all i. If $\sum_{i=1}^N x_i = 1$, then $\sum_{i=1}^N e_i = 1$.

PROOF. For the existence of $\{x_1, \ldots, x_N\}$, we proceed by induction on N, the case $N = 1$ being Proposition 2.23. Suppose we have found $e_1, \ldots, e_n$ and we want to find e_{n+1}. Let e be the idempotent $e_1 + \cdots + e_n$, and apply Corollary 2.24 to the idempotent e in R and the idempotent x_{n+1} in $R/\text{rad}\, R$. The corollary gives us e_{n+1} orthogonal to e with $\bar{e}_{n+1} = x_{n+1}$. Since $e_i = e_ie = ee_i$ for $i \le n$, we obtain $e_{n+1}e_i = e_{n+1}(ee_i) = (e_{n+1}e)e_i = 0$ and similarly $e_ie_{n+1} = 0$ for those i's, and the induction is complete.

Finally $\sum_i x_i = 1$ implies that $\sum_i e_i = 1 + r$ for some r in rad R. Then the idempotent $1 - \sum_i e_i$ is exhibited as in rad R and must be 0 because every element of rad R is nilpotent. □

In a nonzero ring R with identity, a finite subset $\{e_{ij} \mid i, j \in \{1, \dots, n\}\}$ is called a set of **matrix units** in R if $\sum_{i=1}^{n} e_{ii} = 1$ and $e_{ij}e_{kl} = \delta_{jk}e_{il}$ for all i, j, k, l. It follows from these conditions that the e_{ii} are mutually orthogonal idempotents with sum 1, since $e_{ii}e_{jj} = \delta_{ij}e_{ij} = \delta_{ij}e_{ii}$. In view of the remarks before Corollary 2.24, we automatically have $R = \bigoplus_{i=1}^{n} Re_{ii}$. In addition, the product rule gives $e_{ii}e_{ij}e_{jj} = e_{ij}$, $e_{jj}e_{ji}e_{ii} = e_{ji}$, $e_{ij}e_{ji} = e_{ii}$, and $e_{ji}e_{ij} = e_{jj}$; by Proposition 2.21 the idempotents e_{ii} and e_{jj} are isomorphic in the sense that there is a left R module isomorphism $Re_{ii} \cong Re_{jj}$.

If $A = M_n(R)$, define E_{ij} to be the matrix that is 1 in the $(i, j)^{\text{th}}$ place and is 0 elsewhere. Then it is immediate that $\{E_{ij}\}$ is a set of matrix units in A. To recognize matrix rings, we prove the following converse.

Proposition 2.26. For a nonzero ring A with identity, suppose that

$$\{e_{ij} \mid i, j \in \{1, \dots, n\}\}$$

is a set of matrix units in A. Let R be the subring of A of all elements of A commuting with all e_{ij}. Then every element of A can be written in one and only one way as $\sum_{i,j} r_{ij}e_{ij}$ with $r_{ij} \in R$ for all i and j, and the map $A \to M_n(R)$ given by $a \mapsto [r_{ij}]$ is a ring isomorphism. The ring R can be recovered from A by means of the isomorphism $R \cong e_{11}Ae_{11}$.

PROOF. To each $a \in A$, associate the matrix $[r_{ij}]$ in $M_n(A)$ whose entries are given by $r_{ij} = \sum_k e_{ki}ae_{jk}$. Then

$$r_{ij}e_{lm} = \sum_k e_{ki}ae_{jk}e_{lm} = \sum_k e_{ki}a\delta_{kl}e_{jm} = e_{li}ae_{jm}, \tag{$*$}$$

and

$$e_{lm}r_{ij} = \sum_k e_{lm}e_{ki}ae_{jk} = \sum_k \delta_{mk}e_{li}ae_{jk} = e_{li}ae_{jm}.$$

Thus $r_{ij}e_{lm} = e_{li}ae_{jm} = e_{lm}r_{ij}$. Because of the definition of R, this equality shows that r_{ij} is in R. In particular, $[r_{ij}]$ is in $M_n(R)$. A special case of $(*)$ is that $r_{ij}e_{ij} = e_{ii}ae_{jj}$. Hence

$$\sum_{i,j} r_{ij}e_{ij} = \sum_{i,j} e_{ii}ae_{jj} = 1a1 = a.$$

This proves that a can be expanded as $a = \sum_{i,j} r_{ij}e_{ij}$.

For uniqueness, suppose that $a = \sum_{i,j} s_{ij}e_{ij}$ is given with each s_{ij} in R. Multiplication on the left by e_{kp} and right by e_{qk}, followed by addition, gives

$$r_{pq} = \sum_k e_{kp}ae_{qk} = \sum_k e_{kp}\Big(\sum_{i,j} s_{ij}e_{ij}\Big)e_{qk} = \sum_{i,j,k} s_{ij}e_{kp}e_{ij}e_{qk} = \sum_k s_{pq}e_{kk} = s_{pq}.$$

This proves that the map $A \to M_n(R)$ is one-one onto.

To see that the map $A \to M_n(R)$ respects multiplication, let a and a' be in A, and let the effect of the map on a, a', and aa' be $a \mapsto [r_{ij}]$, $a' \mapsto [r'_{ij}]$, and $aa' \mapsto [s_{ij}]$. Then we have

$$\sum_l r_{il} r'_{lj} = \sum_{l,k,k'} e_{ki} a e_{lk} e_{k'l} a' e_{jk'} = \sum_{l,k} e_{ki} a e_{ll} a' e_{jk} = \sum_k e_{ki} a a' e_{jk} = s_{ij},$$

and the matrix product of the images of a and a' coincides with the image of aa'.

Finally consider the image $E_{11} = [r_{ij}]$ of the element $a = e_{11}$ of A. It has $r_{ij} = \sum_k e_{ki} e_{11} e_{jk} = \delta_{i1}\delta_{1j} \sum_k e_{kk} = \delta_{i1}\delta_{1j}$. If a is a general element of A and its image is $[r_{ij}]$, then the result of the previous paragraph shows that $e_{11} a e_{11}$ maps to $E_{11}[r_{ij}]E_{11} = r_{11}E_{11}$. Hence the map $e_{11} a e_{11} \mapsto r_{11}$ is an isomorphism of $e_{11} A e_{11}$ with R. □

PROOF OF THEOREM 2.18. Let $\{x_{ij} \mid i, j \in \{1, \dots, n\}\}$ be a set of matrix units for the matrix ring $A/\operatorname{rad} A \cong M_n(D)$. Then $x_{11}, \dots, x_{nn}$ are mutually orthogonal idempotents in $A/\operatorname{rad} A$ with sum 1. By Corollary 2.25 we can choose mutually orthogonal idempotents $e_{11}, \dots, e_{nn}$ in A with $\sum_{i=1}^n e_{ii} = 1$ and with $\bar{e}_{ii} = x_{ii}$.

We observed at the time of defining matrix units that $x_{11}, \dots, x_{nn}$ are isomorphic as idempotents. Corollary 2.22 shows as a consequence that $e_{11}, \dots, e_{nn}$ are isomorphic as idempotents. The remarks following Corollary 2.22 show that the isomorphism of Re_{11} with Re_{ii} can be exhibited by elements e_{1i} and e_{i1} in A satisfying the usual properties

$$e_{11} e_{1i} e_{ii} = e_{1i}, \quad e_{ii} e_{i1} e_{11} = e_{i1}, \quad e_{1i} e_{i1} = e_{11}, \qquad e_{i1} e_{1i} = e_{ii}$$

and also the properties $\bar{e}_{1i} = x_{1i}$ and $\bar{e}_{i1} = x_{i1}$. Here $\bar{a}$ is shorthand for $a + \operatorname{rad} A$. Define $e_{ij} = e_{i1} e_{1j}$. Then $\bar{e}_{ij} = \bar{e}_{i1}\bar{e}_{1j} = x_{i1}x_{1j} = x_{ij}$, and we readily check that $\{e_{ij}\}$ is a set of matrix units for A.

By Proposition 2.26, $A \cong M_n(R)$ with $R \cong e_{11} A e_{11}$. From Corollary 2.20 we know that $e_{11} A e_{11}/\operatorname{rad}(e_{11} A e_{11}) \cong \bar{e}_{11}(A/\operatorname{rad} A)\bar{e}_{11}$, where $\bar{e}_{11}$ denotes the element $e_{11} + \operatorname{rad} A$ of $A/\operatorname{rad} A$. Hence

$$R/\operatorname{rad} R \cong \bar{e}_{11}(A/\operatorname{rad} A)\bar{e}_{11} \cong \bar{e}_{11} M_n(D) \bar{e}_{11} \cong D,$$

and the proof is complete. □

Corollary 2.27. If A is a finite-dimensional algebra with identity over a field F and if $A/\operatorname{rad} A \cong M_n(F)$ as algebras, then there is a subalgebra S isomorphic to $M_n(F)$ such that $A \cong S \oplus \operatorname{rad} A$ as vector spaces.

REMARKS. This corollary shows that Theorem 2.18 implies Theorem 2.17 under the additional assumption that the algebra A of Theorem 2.17 satisfies $A/\operatorname{rad} A \cong M_n(F)$. It is not necessary to assume characteristic 0.

PROOF. Suppose that A is a finite-dimensional algebra with identity over F such that $A/\operatorname{rad} A \cong M_n(F)$. Then A is left Artinian, and Theorem 2.18 produces a certain ring R with $A \cong M_n(R)$. Here Proposition 2.26 shows that R is isomorphic as a ring to $e_{11}Ae_{11}$ for a certain idempotent e_{11} in A. It follows that R is an algebra with identity over F, necessarily finite-dimensional because A is finite-dimensional. The algebra R, according to Theorem 2.18, has $R/\operatorname{rad} R \cong F$. Therefore $R \cong F \oplus \operatorname{rad} R$ as F vector spaces. If we allow $M_n(\cdot)$ to be defined even for rings without identity, then we have F algebra isomorphisms

$$A \cong M_n(R) \cong M_n(F \oplus \operatorname{rad} R) \cong M_n(F) \oplus M_n(\operatorname{rad} R)$$

in which the direct sums are understood to be direct sums of vector spaces. We shall show that

$$\operatorname{rad}(M_n(R)) = M_n(\operatorname{rad} R), \tag{$*$}$$

and then the decomposition $A = S \oplus \operatorname{rad} A$ will have been proved with $S \cong M_n(F)$.

To prove $(*)$, let E_{ij} be the member of $M_n(R)$ that is 1 in the $(i, j)^{\text{th}}$ place and is 0 elsewhere. Suppose that J is a two-sided ideal in $M_n(R)$. Let $I \subseteq R$ be the set of all elements x_{11} for $x \in J$. If r is in R, then rE_{11} is a member of $M_n(R)$, and the $(1, 1)^{\text{th}}$ entry of the element $(rE_{11})x$ of J is rx_{11}. Thus rx_{11} is in I. Similarly $x_{11}r$ is in I, and I is a two-sided ideal in R. Let us see that

$$J = M_n(I). \tag{$**$}$$

If x is in J, then so is $E_{i1}xE_{1j} = x_{11}E_{ij}$, and hence IE_{ij} is in J; taking sums over i and j shows that $M_n(I) \subseteq J$. In the reverse direction if x is in J, then so is $E_{1i}xE_{j1} = x_{ij}E_{11}$, and hence x_{ij} is in I; therefore $J \subseteq M_n(I)$. This proves $(**)$. Let us apply $(**)$ with $J = \operatorname{rad}(M_n(R))$. The corresponding ideal I of R consists of all entries x_{11} of members x of J. Using Corollary 2.20, we obtain

$$IE_{11} = E_{11}JE_{11} = E_{11}\operatorname{rad}(M_n(R))E_{11} = \operatorname{rad}(E_{11}M_n(R)E_{11}) = \operatorname{rad}(RE_{11}).$$

Thus $I = \operatorname{rad} R$. Taking $M_n(\cdot)$ of both sides and applying $(**)$, we arrive at $(*)$. This completes the proof. □

Corollary 2.28. If A is a finite-dimensional associative algebra with identity over a field F and if $A/\operatorname{rad} A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$, then there is a subalgebra S of A isomorphic as an algebra to $A/\operatorname{rad} A$ such that $A \cong S \oplus \operatorname{rad} A$ as vector spaces.

REMARKS. This corollary gives the conclusion of Theorem 2.17 under the additional assumption that the semisimple algebra $A/\operatorname{rad} A$ over F is of the form $A/\operatorname{rad} A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$. If F is algebraically closed, then the division rings D_k in Theorem 2.2 are finite-dimensional division algebras over F and necessarily equal F, as was observed in the discussion after Corollary 2.3. Thus Theorem 2.2 shows that the additional assumption about the form of $A/\operatorname{rad} A$ is automatically satisfied if F is algebraically closed. In other words, Corollary 2.28 completes the proof of Theorem 2.17 if F is algebraically closed.

PROOF. For $1 \le j \le r$, let x_j be the identity matrix of $M_{n_j}(F)$ when $M_{n_j}(F)$ is regarded as a subalgebra of $A/\operatorname{rad} A$. The elements x_j are orthogonal idempotents in $A/\operatorname{rad} A$ with sum 1, and Corollary 2.25 shows that they lift to orthogonal idempotents e_j of A with sum 1. For each j, Corollary 2.20 shows that $e_jAe_j/\operatorname{rad}(e_jAe_j) = x_j(A/\operatorname{rad} A)x_j \cong M_{n_j}(F)$. By Corollary 2.27, e_jAe_j has a subalgebra $S_j \cong M_{n_j}(F)$ with $e_jAe_j = S_j \oplus \operatorname{rad}(e_jAe_j)$ as vector spaces. Put $S = \bigoplus_{j=1}^r S_j$, the direct sum being understood in the sense of vector spaces. The subalgebra S_j has identity e_j, and the product of e_j with any other S_i is 0 because $e_ie_j = e_je_i = 0$ when $i \ne j$. If $s = \sum_j s_j$ and $s' = \sum_j s'_j$ are two elements of S, then $ss' = \big(\sum_i s_ie_i\big)\big(\sum_j e_js'_j\big) = \sum_{i,j} s_ie_ie_js'_j = \sum_j s_je_js'_j = \sum_j s_js'_j$. Hence S is a subalgebra. The element $\sum_{j=1}^r e_j$ is a two-sided identity in S.

Let us prove that $S \cap \operatorname{rad} A = 0$. If $s = \sum_j s_j$ is in $S \cap \operatorname{rad} A$, then $s_j = e_jse_j$ is in $S_j = e_jSe_j$ and is in $e_j(\operatorname{rad} A)e_j$, which equals $\operatorname{rad}(e_jAe_j)$ by Corollary 2.20. Since $S_j \cap \operatorname{rad}(e_jAe_j) = 0$ by construction, $s_j = 0$. Thus $s = \sum_j s_j = 0$.

Consequently $S \cap \operatorname{rad} A = 0$. A count of dimensions gives $\dim S = \sum_j \dim S_j = \sum_j n_j^2 = \dim(A/\operatorname{rad} A)$. Thus $\dim A = \dim S + \dim(\operatorname{rad} A)$, and we conclude that $A = S \oplus \operatorname{rad} A$ as vector spaces. □

6. Semisimplicity and Tensor Products

In this section we shall complete the proof of Wedderburn's Main Theorem (Theorem 2.17). In the previous section we proved in Corollary 2.28 the special case in which $A/\operatorname{rad} A$ is isomorphic to a product of full matrix rings over the base field F. This special case includes all cases of Theorem 2.17 in which F is algebraically closed.

The idea for the general case is to make a change of rings by tensoring A with the algebraic closure of the underlying field F, or at least with a large enough finite extension K of F for Corollary 2.28 to be applicable. That is, we first consider $A_K = A \otimes_F K$ and $(A/\operatorname{rad} A) \otimes_F K$ in place of A and $A/\operatorname{rad} A$. Inside A_K we can recognize $(\operatorname{rad} A) \otimes_F K$ as a subalgebra defined over K, and we expect that it is $\operatorname{rad} A_K$ and that we can find a complementary subalgebra S over

K; then the question is one of showing that S is of the form $S_0 \otimes_F K$ for some semisimple subalgebra S_0 of A defined over F. The trouble with this style of argument is that the tensor product $(A/\operatorname{rad} A) \otimes_F K$ need not be semisimple and there need not be a candidate for S. Some question about separability of field extensions plays a role, as the following example shows, and the assumption of characteristic 0 will ensure this separability.

EXAMPLE. We exhibit two extension fields K and L of a base field F such that $K \otimes_F L$ is not a semisimple algebra over F. The field extensions are each 1-by-1 matrix algebras over an extension field of F and hence are simple algebras, yet the tensor product is not semisimple. Fix a prime field $\mathbb{F}_p$, and let $F = \mathbb{F}_p(x^p)$ be a simple transcendental extension of $\mathbb{F}_p$. Define $K = L = \mathbb{F}_p(x) = F(\sqrt[p]{x^p})$. Both K and L are field extensions of F of degree p. Thus $K \otimes_F L$ is a finite-dimensional commutative algebra with identity over F, by the construction in Proposition 10.24 of *Basic Algebra*. The element $z = x \otimes 1 - 1 \otimes x$ in $K \otimes_F L$ is nonzero but has $z^p = x^p \otimes 1 - 1 \otimes x^p = x^p \otimes 1 - x^p \otimes 1 = 0$, the next-to-last equality following because x^p lies in the base field F. Consequently $K \otimes_F L$ has a nonzero nilpotent element. If $K \otimes_F L$ were semisimple, Theorem 2.2 would show that it was the direct product of fields, and it could not have any nonzero nilpotent elements. We conclude that $K \otimes_F L$ is not a semisimple algebra.

Proposition 2.29. Let F be a field, let $K = F(\alpha)$ be a simple algebraic extension, let $g(X)$ be the minimal polynomial of α over F, and let L be another field extension of F. Then

(a) $K \otimes_F L \cong L[X]/(g(X))$ as associative algebras over L,
(b) $K \otimes_F L$ is a semisimple algebra if the polynomial $g(X)$ is separable.

REMARKS. Proposition 10.24 of *Basic Algebra* shows that the tensor product $A \otimes_F B$ of two associative algebras with identity over F has a unique associative algebra structure such that $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$. Problem 8 at the end of Chapter X shows that if B is an extension field of F, then $A \otimes_F B$ is in fact an associative algebra with identity over B, the multiplication by $b \in B$ being given by the mapping $1 \otimes$ (left by b).

PROOF. For (a), let $n = [K : F]$. Form the F bilinear mapping of $F[X] \times L$ into $L[X]$ given by $(P(X), \ell) \mapsto \ell P(X)$. Corresponding to this F bilinear mapping is a unique F linear map $\varphi : F[X] \otimes_F L \to L[X]$ carrying $P(X) \otimes \ell$ to $\ell P(X)$ for $P(X) \in F[X]$ and $\ell \in L$. The F vector space $F[X] \otimes_F L$ is an L vector space with multiplication by $\ell_0 \in L$ given by the linear mapping $1 \otimes$ (left by ℓ_0). Since $\varphi\big((1 \otimes (\text{left by } \ell_0))(P(X) \otimes \ell)\big) = \ell_0 \ell P(X) = \ell_0 \varphi(P(X) \otimes \ell))$, φ is L linear. In addition, $\varphi((P(X) \otimes \ell)(Q(X) \otimes \ell')) = \varphi(P(X)Q(X) \otimes \ell\ell') = \ell\ell' P(X)Q(X) = \varphi(P(X) \otimes \ell)\varphi(Q(X) \otimes \ell')$, and therefore φ is an algebra homomorphism.

We follow φ with the quotient homomorphism $\psi : L[X] \to L[X]/(g(X))$, and the composition $\psi\varphi$ is 0 on the ideal $(g(x)) \otimes_F L$ of $F[X] \otimes_F L$. Therefore $\psi\varphi$ descends to a homomorphism $(F[X]/(g(X))) \otimes_F L \to L[X]/(g(X))$, hence to a homomorphism $\eta : K \otimes_F L \to L[X]/(g(X))$. Since φ and ψ are onto, so is η.

It is enough to prove that η is one-one. Thus suppose that $\eta\big(\sum_i k_i \otimes \ell_i\big) = 0$ with all k_i in K, all ℓ_i in L, and the ℓ_i linearly independent over F. Write $k_i = P_i(X) + (g(X))$ with $\deg P_i(X) < n$ whenever $P_i \neq 0$. Then $\sum_i \ell_i P_i(X) \equiv 0 \bmod g(X)$. Since $g(X)$ has degree n and each nonzero $P_i(X)$ has degree at most n, $\sum_i \ell_i P_i(X) = 0$. Write $P_i(X) = \sum_j c_{ij} X^j$ with each c_{ij} in F. Then $\sum_j \big(\sum_i \ell_i c_{ij}\big) X^j = 0$, and $\sum_i \ell_i c_{ij} = 0$ for all j. Since the ℓ_i are linearly independent over F, $c_{ij} = 0$ for all i and j. Thus $k_i = 0$ for all i, $\sum_i k_i \otimes \ell_i = 0$, and η is one-one. This proves (a).

For (b), factor $g(X)$ over L as $g_1(X) \cdots g_m(X)$ for polynomials $g_j(X)$ irreducible over L. Since the separability of g forces $g_1, \ldots, g_m$ to be relatively prime in pairs, the Chinese Remainder Theorem implies that

$$L[X]/(g_1(X) \cdots g_m(X)) \cong L[X]/(g_1(X)) \times \cdots \times L[X]/(g_m(X)).$$

Each $L[X]/(g_j(X))$ is a field, and thus $L[X]/(g(X))$ is exhibited as a product of fields and is semisimple. □

Corollary 2.30. Let F be a field, let K be a finite separable algebraic extension of F, and let L be another field extension of F. Then the algebra $K \otimes_F L$ is semisimple.

REMARKS. The condition of separability of the extension K/F is automatic in characteristic 0. The two field extensions K and L in the example before Proposition 2.29 both failed to be separable extensions of the base field F.

PROOF. The Theorem of the Primitive Element (Theorem 9.34 of *Basic Algebra*) shows that K/F is a simple extension, say with $K = F(\alpha)$. Since this extension is assumed separable, the minimal polynomial over F of any element of K is a separable polynomial. The hypotheses of Proposition 2.29b are therefore satisfied, and $K \otimes_F L$ is semisimple. □

Proposition 2.31. Suppose that A and B are algebras with identity over a field F, that B is simple, and that B has center F. Then the two-sided ideals of the tensor-product algebra $A \otimes_F B$ are all subsets $I \otimes_F B$ such that I is a two-sided ideal of A.

PROOF. The set $I \otimes_F B$ is a two-sided ideal of $A \otimes_F B$, since $(a \otimes b)(i \otimes b') = ai \otimes bb'$ and since a similar identity applies to multiplication in the other order.

Conversely suppose that J is an ideal in $A \otimes_F B$. Let 1_B be the identity of B, and define $I = \{a \in A \mid a \otimes 1_B \in J\}$. Then I is a two-sided ideal of A, and we shall prove that $J = I \otimes_F B$. The easy inclusion is $I \otimes_F B \subseteq J$. For this, let i be in I and b be in B. Then $i \otimes 1_B$ is in J and $1_A \otimes b$ is in $A \otimes_F B$. Their product $i \otimes b$ has to be in J, and thus $I \otimes_F B \subseteq J$.

For the reverse inclusion, take a basis $\{x_i\}$ of I over F and extend it to a basis of A by adjoining some vectors $\{y_j\}$. It is enough to show that any finite sum $\sum_j y_j \otimes b_j$ in J necessarily has all b_j equal to 0. Arguing by contradiction, suppose that $\sum_{k=1}^m y_{j_k} \otimes b_{j_k}$ is a nonzero sum in J with m as small as possible and in particular with all b_{j_k} nonzero. Let H be the subset of B defined by

$$H = \left\{ c_{j_1} \;\middle|\; \sum_{k=1}^m y_{j_k} \otimes c_{j_k} \in J \text{ for some } m\text{-tuple } \{c_{j_k}\} \subseteq B \right\}.$$

The set H is a two-sided ideal of B containing the nonzero element b_{j_1} of B. Since B is simple by assumption, $H = B$. Thus 1_B is in H. Therefore some element

$$y_{j_1} \otimes 1_B + \sum_{k=2}^m y_{j_k} \otimes c_{j_k}$$

is in J. Let $b \in B$ be arbitrary. Multiplying the displayed element on the left and right by $1_A \otimes b$ and subtracting the results shows that

$$y_{j_2} \otimes (bc_{j_2} - c_{j_2} b) + \cdots + y_{j_m} \otimes (bc_{j_m} - c_{j_m} b)$$

is in J. Since m was chosen to be minimal, this element must be 0 for all choices of b. Then all coefficients are 0, and the conclusion is that all coefficients c_{j_k} are in the center of B, which is F by assumption. Consequently we can rewrite our element of J as

$$y_{j_1} \otimes 1_B + \sum_{k=2}^m y_{j_k} \otimes c_{j_k} = y_{j_1} \otimes 1_B + \sum_{k=2}^m c_{j_k} y_{j_k} \otimes 1_B = \left(y_{j_1} + c_{j_2} y_{j_2} + \cdots + c_{j_m} y_{j_m}\right) \otimes 1_B.$$

The definition of I shows that the factor $y_{j_1} + c_{j_2} y_{j_2} + \cdots + c_{j_m} y_{j_m}$ in the pure tensor on the right is in I. Since the y_j's form a basis of a vector-space complement to I, this vector must be 0. The linear independence of the y_j's over F forces each coefficient to be 0, and we have arrived at a contradiction because the coefficient of y_{j_1} is 1, not 0. □

Lemma 2.32. The center of a finite-dimensional simple algebra A over a field F is a field that is a finite extension of F.

PROOF. By Theorem 2.4, $A \cong M_n(D)$ for some finite-dimensional division algebra D over F. Let Z be the center of A. By inspection this consists of the scalar matrices whose entries lie in the center of D. The center of D is a field. Hence Z is a field, necessarily a finite extension of F. □

Proposition 2.33. Let A be a finite-dimensional semisimple algebra over a field F of characteristic 0, and suppose that K is a field containing F. Then the algebra $A \otimes_F K$ over K is semisimple.

PROOF. Since the tensor product of a finite direct sum is the direct sum of tensor products, we may assume without loss of generality that A is simple. Lemma 2.32 shows that the center Z of A is a finite extension field of F. By Corollary 2.30 and the assumption that F has characteristic 0, the algebra $Z \otimes_F K$ is semisimple. Being commutative, it must be of the form $K_1 \oplus \cdots \oplus K_s$ with each ideal K_i equal to a field, by Theorem 2.2.

Each ideal K_i is a unital $Z \otimes_F K$ module, hence is both a unital Z module and a unital K module. Thus we can regard each K_i as an extension field of Z or of K, whichever we choose. First let us regard K_i as an extension field of Z. Since K_i has no nontrivial ideals and A has center Z, Proposition 2.31 shows that the Z algebra $A \otimes_Z K_i$ is simple as a ring.

Next let us regard K_i as an extension field of K; since A is finite-dimensional over F, so is Z. Therefore $Z \otimes_F K$ is finite-dimensional over K, and K_i is a finite extension of K. Hence $A \otimes_Z K_i$ is a finite-dimensional algebra over K, and it is left Artinian as a ring.

By Theorem 2.6, any left Artinian simple ring such as $A \otimes_Z K_i$ is necessarily semisimple. Using the associativity formula for tensor products given in Proposition 10.22 of *Basic Algebra*, we obtain an isomorphism of rings

$$\begin{aligned} A \otimes_F K &\cong (A \otimes_Z Z) \otimes_F K \cong A \otimes_Z (Z \otimes_F K) \\ &\cong A \otimes_Z (K_1 \oplus \cdots \oplus K_s) \cong \bigoplus_{j=1}^{s} (A \otimes_Z K_j), \end{aligned}$$

the summands being two-sided ideals in each case. Since each $A \otimes_Z K_j$ is a finite-dimensional simple algebra over K, $A \otimes_F K$ is a semisimple algebra over K by Theorem 2.4. □

Let us digress for a moment, returning in Lemma 2.34 to the argument that leads to the proof of Theorem 2.17. In the next section we shall want to know circumstances under which we can draw the same conclusion as in Proposition 2.33 without assuming that the characteristic is 0. Write the finite-dimensional semisimple algebra A as $A = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where each D_r is a division algebra over F. Let $Z_1, \ldots, Z_r$ be the respective centers of the simple factors of A. Lemma 2.32 observes that each Z_j is a finite extension field of F. The proof of Proposition 2.33 appealed to Corollary 2.30 to conclude from the condition characteristic 0 that $Z_j \otimes_F K$ is semisimple. Instead, by rereading the statement of Corollary 2.30, we see that it would have been enough for each Z_j to be a finite *separable* field extension of F, even if F did not have characteristic 0.

Then the rest of the above proof goes through without change. Accordingly we define a finite-dimensional semisimple algebra A over a field F to be a **separable** semisimple algebra if the center of each simple component of A is a separable extension field of F. In terms of this definition, we obtain the following improved version of Proposition 2.33.

Proposition 2.33′. Let A be a finite-dimensional separable semisimple algebra over a field F, and suppose that K is a field containing F. Then the algebra $A \otimes_F K$ over K is semisimple.

Lemma 2.34. Suppose that A is a finite-dimensional algebra with identity over a field F, and suppose that N is a nilpotent two-sided ideal of A such that the algebra A/N is semisimple. Then $N = \operatorname{rad} A$.

PROOF. The algebra A is left Artinian, being finite-dimensional. Since N is nilpotent, we must have $N \subseteq \operatorname{rad} A$. The two-sided ideal $(\operatorname{rad} A)/N$ of the semisimple algebra A/N is nilpotent and hence must be 0. Therefore $N = \operatorname{rad} A$. □

PROOF OF THEOREM 2.17. Let A be the given finite-dimensional algebra of the field F of characteristic 0, and write N for $\operatorname{rad} A$ and $\overline{A}$ for A/N. For any extension field K of F, we write $A_K = A \otimes_F K$, $N_K = N \otimes_F K$, and $\overline{A}_K = \overline{A} \otimes_F K$.

For most of the proof, we shall treat the special case that $N^2 = 0$. Let $\overline{F}$ be an algebraic closure of F. Then $\overline{A}_{\overline{F}} = \overline{A} \otimes_F \overline{F} = (A/N) \otimes_F \overline{F} \cong (A \otimes_F \overline{F})/(N \otimes_F \overline{F}) = A_{\overline{F}}/N_{\overline{F}}$. Proposition 2.33 shows that $\overline{A}_{\overline{F}} = \overline{A} \otimes_F \overline{F}$ is a semisimple algebra over $\overline{F}$, and the claim is that the two-sided ideal $N_{\overline{F}}$ of $A_{\overline{F}}$ is nilpotent. In fact, any element of $N_{\overline{F}}$ is a finite sum of the form $\sum_i (a_i \otimes c_i)$ with each a_i in N and each c_i in $\overline{F}$. The product of this element with $\sum_j (a'_j \otimes c'_j)$ is $\sum_{i,j} (a_i a'_j \otimes c_i c'_j)$, and this is 0 because the assumption $N^2 = 0$ implies that $a_i a'_j = 0$ for all i and j. Thus $N_{\overline{F}}^2 = 0$, and $N_{\overline{F}}$ is nilpotent.

Since $A_{\overline{F}}/N_{\overline{F}}$ is semisimple and $N_{\overline{F}}$ is nilpotent, Lemma 2.34 shows that $N_{\overline{F}} = \operatorname{rad}(A_{\overline{F}})$. Corollary 2.28 (a special case of Theorem 2.17) is applicable to $A_{\overline{F}}$ because $\overline{F}$ is algebraically closed, and it follows that there exists a subalgebra $\widetilde{S}$ of $A_{\overline{F}}$ such that $A_{\overline{F}} = \widetilde{S} \oplus N_{\overline{F}}$ as vector spaces. Here $\widetilde{S}$ is a product of finitely many algebras $M_{n_j}(\overline{F})$. The embedded matrix units e_{ij} of $\widetilde{S}$ obtained from each $M_{n_j}(\overline{F})$ are members of $A_{\overline{F}} = A \otimes_F \overline{F}$ and hence are of the form $\sum_l x_l \otimes c_l$, where $\{x_l\}_{l=1}^n$ is a vector-space basis of A over F and each c_l is in $\overline{F}$. Only finitely many such c_l's are needed to handle all e_{ij}'s, and we let K be a finite extension of F within $\overline{F}$ containing all of them. Let $\rho_0 = 1, \rho_1, \dots, \rho_s$ be a vector-space basis of K over F.

Relative to this K, we form A_K, N_K, and $\overline{A}_K$ as in the first paragraph of the proof. The same argument as with $\overline{F}$ shows that $\overline{A}_K \cong A_K/N_K$ is semisimple and that N_K is nilpotent. By Lemma 2.34, $N_K = \operatorname{rad} A_K$. The formulas for the e_{ij}'s in the previous paragraph are valid in A_K and give us a system of matrix units. As in the previous paragraph, Corollary 2.28 produces a subalgebra S of A_K isomorphic to some $M_{n_1}(K) \times \cdots \times M_{n_r}(K)$ such that $A_K = S \oplus N_K$ as vector spaces.

In the basis $\{x_i\}_{i=1}^n$ of A over F, we may assume that the first t vectors form a basis of $N = \operatorname{rad} A$ and the remaining vectors form a basis of a vector-space complement to N. We identify members a of A with members $a \otimes 1$ of A_K. With this identification in force, we decompose each basis vector x_i for $i > t$ according to $A_K = S \oplus N_K$ as $x_i = y_i - z_i$ with $y_i \in S$ and $z_i \in N_K$. Since the x_i's for $i \le t$ are in $N \subseteq N_K$, the vectors y_i with $i > t$ form a vector-space basis of S over K. For $i > t$, write $z_i = \sum_{j=0}^s z_{ij} \otimes \rho_j$ with z_{ij} in N. Then we have

$$y_i = x_i + z_i = (x_i + z_{i0}) + \sum_{j=1}^s z_{ij} \otimes \rho_j \qquad \text{for } i > t.$$

Put

$$x_i' = x_i + z_{i0} \qquad \text{and} \qquad z_i' = \sum_{j=1}^s z_{ij} \otimes \rho_j \qquad \text{for } i > t.$$

Then $\{x_i\}_{i=1}^t \cup \{x_i'\}_{i=t+1}^n$ is a basis of A over F. We shall show that $S_0 = \sum_{i=t+1}^n F x_i'$ is a subalgebra of A, and then $A = S_0 \oplus N$ will be the required decomposition.

Let x_i' and x_j' be given with $i > t$ and $j > t$, and write

$$x_i' x_j' = \textstyle\sum_k \gamma_{kij} x_k' + v_{ij} \qquad \text{with } \gamma_{kij} \in F \text{ and } v_{ij} \in N.$$

Substituting $x_i' = y_i - z_i'$ and taking into account that N_K is an ideal in A_K, we have

$$y_i y_j \equiv \sum_k \gamma_{kij} x_k' \bmod N_K \equiv \sum_k \gamma_{kij} y_k \bmod N_K.$$

Then $y_i y_j = \sum_k \gamma_{kij} y_k + u_{ij}$ with each $u_{ij} \in N_K$. Since the y_i are in S and S is a subalgebra, $u_{ij} = 0$. Thus $y_i y_j = \sum_k \gamma_{kij} y_k$. Let us resubstitute into this equality from $y_i = x_i' + z_i'$. Taking into account that $z_i' z_j' = 0$ because $N_K^2 = 0$, we obtain

$$x_i' x_j' + x_i' z_j' + z_i' x_j' = \sum_k \gamma_{kij} x_k' + \sum_k \gamma_{kij} z_k'.$$

Substituting from $z_i' = \sum_{j=1}^s z_{ij} \otimes \rho_j$ gives

$$x_i' x_j' \otimes 1 + \sum_{l=1}^s x_i' z_{jl} \otimes \rho_l + \sum_{l=1}^s z_{il} x_j' \otimes \rho_l = \sum_k \gamma_{kij} x_k' \otimes 1 + \sum_k \sum_{l=1}^s \gamma_{kij} z_{kl} \otimes \rho_l.$$

The coefficients of $\rho_0 = 1$ must be equal, and therefore

$$x_i' x_j' = \sum_k \gamma_{kij} x_k'.$$

This equation shows that S_0 is a subalgebra and completes the proof under the hypothesis that $N^2 = 0$.

Now we drop the assumption that $N^2 = 0$. We shall prove the theorem by induction on $\dim_F A$, the base cases of the induction being $\dim_F A = 0$ and $\dim_F A = 1$, for which the theorem is immediate by inspection. For the inductive case, let A be given, and assume the theorem to be known for algebras of dimension $< \dim_F A$. If $N^2 = 0$, then we are done. Thus we may assume that the product ideal N^2 is nonzero and therefore that $\dim_F(A/N^2) < \dim_F A$. The First Isomorphism Theorem shows that $(A/N^2)\big/(N/N^2) \cong A/N = \overline{A}$. The quotient A/N is semisimple, and N/N^2 is a nilpotent ideal in A/N^2. By Lemma 2.34, $N/N^2 = \operatorname{rad}(A/N^2)$. The inductive hypothesis gives $A/N = S_1/N^2 \oplus N/N^2$ for a subalgebra S_1 of A with $S_1 \supseteq N^2$. This means that $A = S_1 + N$ and $S_1 \cap N = N^2$. Here

$$\begin{aligned}\dim_F A &= \dim_F(S_1 + N) = \dim_F S_1 + \dim_F N - \dim_F(S_1 \cap N) \\ &= \dim_F S_1 + \dim_F N - \dim_F N^2 = \dim_F S_1 + \dim_F(N/N^2),\end{aligned}$$

and $N/N^2 \neq 0$ implies $\dim_F S_1 < \dim_F A$. The Second Isomorphism Theorem gives $A/N = (S_1+N)/N \cong S_1/(S_1 \cap N) = S_1/N^2$. Thus S_1/N^2 is semisimple. Since N^2 is nilpotent, Lemma 2.34 shows that $N^2 = \operatorname{rad} S_1$. The inductive hypothesis gives $S_1 = S \oplus N^2$ for a semisimple subalgebra S. Substituting into $A = S_1 + N$, we obtain $A = (S \oplus N^2) + N = S + N$. Meanwhile, $S \cap N = (S \cap S_1) \cap N = S \cap (S_1 \cap N) = S \cap N^2 = 0$. Therefore $A = S \oplus N$, and the induction is complete. □

7. Skolem–Noether Theorem

In this section we begin an investigation of division algebras that are finite-dimensional over a given field F. A nonzero algebra A with identity over a field F will be called **central** if the center of A consists exactly of the scalar multiples of the identity, i.e., if $\operatorname{center}(A) = F$. Of special interest will be algebras with identity that are **central simple**, i.e., are both central and simple.

Lemma 2.35. Let A and B be algebras with identity over a field F, and suppose that B is central. Then

(a) the members of $A \otimes_F B$ commuting with $1 \otimes B$ are the members of $A \otimes 1$,
(b) $\operatorname{center}(A \otimes_F B) = (\operatorname{center} A) \otimes_F 1$.

PROOF. For (a), suppose that $z = \sum_i a_i \otimes b_i$ commutes with $1 \otimes B$ and that the a_i are linearly independent over F. If b is in B, then

$$0 = (1 \otimes b)z - z(1 \otimes b) = \sum_i a_i \otimes (bb_i - b_i b),$$

from which it follows that $bb_i - b_i b = 0$ for all b and all i. Since B is central, each b_i is in F, and we can write z as

$$z = \sum_i a_i \otimes b_i = \sum_i (a_i b_i \otimes 1) = \Big(\sum_i a_i b_i\Big) \otimes 1.$$

In other words, z is of the form $z = a \otimes 1$.

For (b), we need to prove the inclusion $\subseteq$. Thus let z be in center$(A \otimes_F B)$. By (a), z is of the form $z = a \otimes 1$ for some $a \in A$. Now suppose that a' is in A. Then $0 = (a' \otimes 1)z - z(a' \otimes 1) = (a'a - aa') \otimes 1$. Hence $a'a = aa'$, and we conclude that a is in center(A). □

Proposition 2.36. Let A and B be algebras with identity over a field F, and suppose that B is central simple. Then

(a) A simple implies $A \otimes_F B$ simple,
(b) A central simple implies $A \otimes_F B$ central simple.

PROOF. For (a), Proposition 2.31 shows that any two-sided ideal of $A \otimes_F B$ is of the form $I \otimes_F B$ for some two-sided ideal I of A. Since A is assumed simple, the only I's are 0 and A. Thus the only ideals in $A \otimes_F B$ are 0 and $A \otimes_F B$, and $A \otimes_F B$ is simple.

For (b), conclusion (a) shows that $A \otimes_F B$ is simple. By Lemma 2.35b the center of $A \otimes_F B$ is (center A) $\otimes 1 = F1 \otimes 1 = F(1 \otimes 1)$, and hence $A \otimes_F B$ is central. □

Corollary 2.37. If A and B are finite-dimensional semisimple algebras over a field F and at least one of them is separable over F, then $A \otimes_F B$ is semisimple.

REMARK. The definition of separability of A or B appears between Proposition 2.33 and Proposition 2.33′.

PROOF. Without loss of generality, we may assume that A and B are simple. For definiteness let us say that A is the given separable algebra over F. Let $K =$ center(B). Lemma 2.32 shows that K is a field, and associativity of tensor products allows us to write

$$A \otimes_F B \cong A \otimes_F (K \otimes_K B) \cong (A \otimes_F K) \otimes_K B.$$

Here $A \otimes_F K$ is semisimple by Proposition 2.33′, and B is central simple over K. Thus Proposition 2.36a applies and shows that $(A \otimes_F K) \otimes_K B$ is simple. □

Corollary 2.38. Let A be a central simple algebra of finite dimension n over a field F, and let A^o be the opposite algebra. Then $A \otimes_F A^o \cong M_n(F)$.

EXAMPLE. Take $F = \mathbb{R}$ and $A = \mathbb{H}$, the algebra of quaternions. Then conjugation, with $1 \mapsto 1$ and $i, j, k \mapsto -i, -j, -k$, is an antiautomorphism of $\mathbb{H}$. Consequently $H^o \cong H$. The corollary says in this case that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$.

PROOF. Let V be A considered as a vector space. For each $a_0 \in A$, we associate the members $l(a_0)$ and $r(a_0)$ of $\mathrm{End}_F(V)$ given by $l(a_0)a = a_0 a$ and $r(a_0)a = aa_0$. Then $l(a_0 a_0') = l(a_0)l(a_0')$ and $r(a_0 a_0') = r(a_0')r(a_0)$, and it follows that $l : A \to \mathrm{End}_F(V)$ and $r : A^o \to \mathrm{End}_F(V)$ are algebra homomorphisms sending 1 to 1.

Meanwhile, the map $A \times A^o \to \mathrm{End}_F(V)$ given by $(a, a') \mapsto l(a)r(a')$ is F bilinear and extends to an F linear map $\varphi : A \otimes_F A^o \to \mathrm{End}_F(V)$. Because of the homomorphism properties of l and r, the mapping φ is an algebra homomorphism sending 1 to 1. Proposition 2.36 shows that $A \otimes_F A^o$ is simple, and it follows that φ is one-one. Since $\dim_F(A \otimes_F A^o) = (\dim_F A)^2 = \dim_F \mathrm{End}_F(V)$, φ is onto. □

Corollary 2.39. Let A be a central simple algebra of finite dimension d over a field F. Then d is the square of an integer.

PROOF. Let $\overline{F}$ be an algebraic closure of F. Proposition 2.36a shows that the algebra $\overline{F} \otimes_F A$ is simple, and its dimension over $\overline{F}$ is d. A simple finite-dimensional algebra over an algebraically closed field is a full matrix algebra over that field, and thus $\overline{F} \otimes_F A \cong M_n(\overline{F})$. Comparing dimensions over $\overline{F}$, we see that $d = n^2$. □

Corollary 2.40. If D is a division algebra finite-dimensional over its center F, then $\dim_F D$ is the square of an integer.

PROOF. The algebra D is central simple over its center F, and the result is immediate from Corollary 2.39. □

Theorem 2.41 (Skolem–Noether Theorem). Let A be a finite-dimensional central simple algebra over the field F, and let B be any simple algebra over F. Suppose that f and g are F algebra homomorphisms of B into A carrying the identity to the identity. Then there exists an $x \in A$ with $f(b) = xg(b)x^{-1}$ for all b in B.

PROOF. Let us observe that the homomorphisms f and g are one-one because B is simple, and the finite dimensionality of A therefore forces B to be finite-dimensional.

We consider first the special case that $A = M_n(F)$ for some n. The homomorphism f makes the space F^n of column vectors into a unital left B module by the definition $bv = f(b)v$, and similarly the homomorphism g makes F^n into a unital left B module. Since B is finite-dimensional and simple, an argument given with Example 1 of semisimple rings in Section 2 shows that there is only one simple left B module up to isomorphism and that every unital left B module is a direct sum of copies of this simple left B module. Consequently the isomorphism classes of the B modules determined by f and g depend only on their dimension. The dimension is n in both cases, and hence there exists an invertible F linear map $L : F^n \to F^n$ such that $Lf(b)v = g(b)Lv$ for all $v \in F^n$. If L is given by the matrix x^{-1} in $M_n(F)$, then $x^{-1}f(b) = g(b)x^{-1}$, and the theorem is therefore proved in this special case.

For the general case we form the tensor products $B \otimes_F A^o$ and $A \otimes_F A^o$. The maps $f \otimes 1$ and $g \otimes 1$ are F algebra homomorphisms between these algebras, $B \otimes_F A^o$ is simple by Proposition 2.36a, and Corollary 2.38 shows that $A \otimes_F A^o$ is isomorphic to $M_n(F)$ for the integer $n = \dim A$. The special case is applicable, and we obtain an invertible element X of $A \otimes_F A^o$ such that

$$(f \otimes 1)(b \otimes a^o) = X(g \otimes 1)(b \otimes a^o)X^{-1} \quad \text{for all } b \in B \text{ and } a^o \in A^o. \quad (*)$$

Taking $b = 1$, we see that $1 \otimes a^o = X(1 \otimes a^o)X^{-1}$ for all $a^o \in A^o$. By Lemma 2.35a, X lies in $A \otimes 1$, hence is of the form $X = x \otimes 1$ for some x in A. Substituting for X in $(*)$, we obtain $f(b) = xg(b)x^{-1}$ as required. □

Corollary 2.42. If A is a finite-dimensional central simple algebra over the field F, then every F automorphism of A is inner in the sense of being given by conjugation by an invertible element of A.

PROOF. This is the special case of Theorem 2.41 in which $B = A$ and g is the identity map on B. □

8. Double Centralizer Theorem

We saw in Corollary 2.40 that if D is a division algebra finite-dimensional over its center F, then $\dim_F D$ is the square of an integer. In this section we shall prove a theorem from which we can conclude that the positive integer of which $\dim_F D$ is the square is the dimension of any maximal subfield of D. We state the theorem, establish two lemmas, prove the theorem, and then derive two corollaries concerning maximal subfields of division algebras.

If A is an algebra with identity and B is a subalgebra containing the identity, then the **centralizer** of B in A is the subalgebra of all members of A commuting with every element of B.

Theorem 2.43 (Double Centralizer Theorem). Let A be a finite-dimensional central simple algebra over a field F, let B be a simple subalgebra of A, and let C be the centralizer of B in A. Then C is simple, B is the centralizer of C in A, and $(\dim_F B)(\dim_F C) = \dim_F A$.

Lemma 2.44. Let A and A' be algebras with identity over a field F, let B and B' be subalgebras of them, and let C and C' be the centralizers of B and B' in A and A', respectively. Then the centralizer of $B \otimes_F B'$ in $A \otimes_F A'$ is $C \otimes_F C'$.

PROOF. Expand an element of $A \otimes_F A'$ for the moment as $x = \sum_i a_i \otimes a_i'$ with the elements a_i' linearly independent over F. If x satisfies $x(b \otimes 1) = (b \otimes 1)x$ for all b in B, then $\sum_i (a_i b - b a_i) \otimes a_i' = 0$. Since the a_i''s are independent, $a_i b - b a_i = 0$ for all i, and each a_i is in C. Thus the centralizer of $B \otimes_F 1$ is $C \otimes_F A'$.

Rewriting x with the a_i's assumed independent, we see similarly that the centralizer of $1 \otimes_F B'$ is $A \otimes_F C'$. Putting these conclusions together, we see that

$$\begin{aligned}\text{centralizer}(B \otimes_F B') &\subseteq \text{centralizer}(B \otimes_F 1) \cap \text{centralizer}(1 \otimes_F B') \\ &= (C \otimes_F A') \cap (A \otimes_F C') = C \otimes_F C'.\end{aligned}$$

The reverse inclusion, namely $\text{centralizer}(B \otimes_F B') \supseteq C \otimes_F C'$, is immediate, and the lemma follows. □

Lemma 2.45. Let B be a finite-dimensional simple algebra over a field F, and write V for the algebra B considered as a vector space. For b in B and v in V, define members $l(b)$ and $r(b)$ of $\text{End}_F(V)$ by $l(b)v = bv$ and $r(b)v = vb$. Then the centralizer in $\text{End}_F(V)$ of $l(B)$ is $r(B)$.

PROOF. Let K be the center of B. This is an extension field of F by Lemma 2.32, and B is central simple over K. Let us see that any member a of $\text{End}_F(V)$ that centralizes $l(B)$ is actually in $\text{End}_K(V)$. If c is in K, then c is in particular in B, and therefore $al(c) = l(c)a$. Applying this equality to $v \in V$ yields $a(cv) = ca(v)$, and this equality for all $c \in K$ says that a is in $\text{End}_K(V)$.

Thus it is enough to show that the centralizer of $l(B)$ in $\text{End}_K(V)$ is $r(B)$. We argue as in the proof of Corollary 2.38: The definitions of l and r make V into a unital left B module and a unital right B module, and the members of K operate consistently on either side of V because K lies in the center of B. The function $(b, b') \mapsto l(b)r(b')$ is therefore K bilinear, and it extends to the tensor product $B \otimes_K B^o$ as an algebra homomorphism $\varphi : B \otimes_K B^o \mapsto \text{End}_K(V)$. The homomorphism φ is one-one, since Proposition 2.36a shows $B \otimes_K B^o$ to be simple. The dimensional equality $\dim_K(B \otimes_K B^o) = (\dim_K B)^2 = \dim_K(\text{End}_K(V))$ allows us to conclude that φ is onto, hence is an isomorphism.

Lemma 2.35a shows that the centralizer of $B \otimes_K 1$ in $B \otimes_K B^o$ is $1 \otimes_K B^o$. If this statement is translated from the context of $B \otimes_K B^o$ into the isomorphic context of $\mathrm{End}_K(V)$, then the centralizer of $l(B)$ in $\mathrm{End}_K(V)$ is $r(B)$, and we saw that this fact is sufficient to imply the lemma. □

PROOF OF THEOREM 2.43. Let V be the algebra B considered as a vector space over F, and let $l(B)$ and $r(B)$ be the sets of those members of $\mathrm{End}_F(V)$ that are given by left multiplication and right multiplication by members of B. The algebra A is central simple by assumption, and $\mathrm{End}_F(V)$ is central simple, being isomorphic to $M_n(F)$ for the integer $n = \dim_F(V)$. By Proposition 2.36b, $A \otimes_F \mathrm{End}_F(V)$ is central simple. We define two algebra homomorphisms f and g of B into $A \otimes_F \mathrm{End}_F(V)$ by $f(b) = l(b) \otimes 1$ and $g(b) = 1 \otimes l(b)$.

The Skolem–Noether Theorem (Theorem 2.41) produces an element x of $A \otimes_F \mathrm{End}_F(V)$ with $f(b) = xg(b)x^{-1}$ for all $b \in B$. Hence

$$B \otimes_F 1 = x(1 \otimes_F l(B))x^{-1}. \tag{$*$}$$

Lemma 2.44 shows that the centralizer of $B \otimes_F 1$ in $A \otimes_F \mathrm{End}_F(V)$ is $C \otimes_F \mathrm{End}_F(V)$ and that the centralizer of $1 \otimes_F l(B)$ is $A \otimes_F r(B)$. From the latter identification the centralizer of $x(1 \otimes_F l(B))x^{-1}$ is $x(A \otimes_F r(B))x^{-1}$. Combining $(*)$ with these computations of centralizers, we see that

$$C \otimes_F \mathrm{End}_F(V) = x(A \otimes_F r(B))x^{-1}. \tag{$**$}$$

The algebra $A \otimes_F r(B)$ is isomorphic to $A \otimes_F B^o$, which is simple by Proposition 2.36a. Therefore $C \otimes_F \mathrm{End}_F(V)$ is simple, and C has to be simple.

Equating the dimensions of the two sides of $(**)$ gives

$$\begin{aligned}(\dim_F C)(\dim_F B)^2 &= (\dim_F C)(\dim_F \mathrm{End}_F(V)) = \dim_F(C \otimes_F \mathrm{End}_F(V)) \\ &= \dim_F(A \otimes_F r(B)) = (\dim_F A)(\dim_F B),\end{aligned}$$

and hence

$$(\dim_F C)(\dim_F B) = \dim_F A.$$

Finally the centralizer D of C contains B, and two applications of the dimensional equality gives

$$(\dim_F D)(\dim_F C) = \dim_F A = (\dim_F C)(\dim_F B).$$

Thus $\dim_F D = \dim_F B$, and we must have $D = B$. In other words, B is the centralizer of C. □

Corollary 2.46. Let D be a central finite-dimensional division algebra over the field F. If K is any maximal subfield of D, then $\dim_F D = (\dim_F K)^2$.

PROOF. Apply the Double Centralizer Theorem (Theorem 2.43) with $A = D$. Let $Z(K)$ be the centralizer of the simple subalgebra K in D. Since K is commutative, $K \subseteq Z(K)$. If a is in $Z(K)$ but not K, then $K(a)$ is a field in D properly containing K, in contradiction to the assumption that K is a maximal subfield of D. Hence $K = Z(K)$. The dimensional equality in the theorem therefore gives $\dim_F D = (\dim_F K)(\dim_F Z(K)) = (\dim_F K)^2$. □

Corollary 2.47. Let A be a finite-dimensional central simple algebra over a field F, and let K be a subfield of A. Then the following are equivalent:

(a) K is its own centralizer,
(b) $\dim_F A = (\dim_F K)^2$,
(c) K is a maximal commutative subalgebra of A.

PROOF. Let $Z(K)$ be the centralizer of K in A. The Double Centralizer Theorem (Theorem 2.43) gives the equality

$$\dim_F A = (\dim_F K)(\dim_F Z(K)). \qquad (*)$$

If (a) holds, then $Z(K) = K$, and $(*)$ yields (b).

If (b) holds, then $(*)$ and the equality $\dim_F A = (\dim_F K)^2$ together imply that $\dim_F Z(K) = \dim_F K$. Since K is commutative, $Z(K) \supseteq K$. The equality of dimensions implies that $Z(K) = K$, and then (c) follows.

If (c) holds, we start from the inclusion $K \subseteq Z(K)$. If x is in $Z(K)$ but not K, then $K(x)$ is a field strictly larger than K, in contradiction to (c). Thus $K = Z(K)$, and (a) holds. □

9. Wedderburn's Theorem about Finite Division Rings

The theorem of this section is as follows.

Theorem 2.48 (Wedderburn). Every finite division ring is a field.

The proof will be preceded by a lemma.

Lemma 2.49. If G is a finite group and H is a proper subgroup, then $\bigcup_{g \in G} gHg^{-1}$ does not exhaust G.

PROOF. In the union $\bigcup_{g\in G} gHg^{-1}$, the terms corresponding to g and to gh, for h in H, are the same because $(gh)H(gh)^{-1} = g(hHh^{-1})g^{-1} = gHg^{-1}$. Thus the union can be rewritten as $\bigcup_{gH} gHg^{-1}$, it being understood that only one g is used from each coset gH. From this rewritten form of the union, we see that the number of elements other than the identity in the union is

$$\leq [G : H](|H| - 1) = [G : H]|H| - [G : H] = |G| - [G : H] < |G| - 1,$$

and the lemma follows. □

PROOF OF THEOREM 2.48. Let D be a finite division ring, and let F be the center. Then F is a field, say of q elements. Maximal subfields of D certainly exist. Any such subfield K has $\dim_F D = (\dim_F K)^2$ by Corollary 2.46, and hence any two such subfields K and K' are isomorphic. The Skolem–Noether Theorem (Theorem 2.41) shows that $K' = xKx^{-1}$ for some invertible x in the group $D^\times$ of invertible elements of D.

On the other hand, F and any element of D generate a subfield of D, and this subfield is contained in a maximal subfield. Consequently any element of D is contained in some such K', and $D = \bigcup_{x\in D^\times} xKx^{-1}$. Discarding the element 0 from both sides, we obtain $D^\times = \bigcup_{x\in D^\times} xK^\times x^{-1}$. Applying Lemma 2.49 to the group $G = D^\times$ and the subgroup $H = K^\times$, we see that $K^\times$ cannot be a proper subgroup of $D^\times$. Therefore $D = K$, and D is commutative. □

10. Frobenius's Theorem about Division Algebras over the Reals

We conclude this chapter by bringing together our results to prove the following celebrated theorem of Frobenius.

Theorem 2.50 (Frobenius). Up to $\mathbb{R}$ isomorphism the only finite-dimensional associative division algebras over $\mathbb{R}$ are the algebras $\mathbb{R}$ of reals, $\mathbb{C}$ of complex numbers, and $\mathbb{H}$ of quaternions.

REMARKS. The text of this chapter has not produced any concrete examples of noncommutative division rings other than the quaternions. Problems 12–16 at the end of the chapter produce generalized quaternion algebras in which $\mathbb{R}$ can be replaced by many other fields; there are infinitely many nonisomorphic such examples when the field is $\mathbb{Q}$. In addition, Problems 17–19 produce examples of central division algebras of dimension 9 over suitable base fields. The next chapter will give further insight into the construction of division algebras.

PROOF. Let D be such a division algebra, and let F be the center. Then F is a finite extension field of $\mathbb{R}$ and must be $\mathbb{R}$ or $\mathbb{C}$, since $\mathbb{C}$ is algebraically closed. If $F = \mathbb{C}$, then we have seen that $D = \mathbb{C}$. Thus we may assume that $\text{center}(D) = \mathbb{R}$.

Let K be a maximal subfield of D (existence by finite dimensionality), and let $n = \dim_{\mathbb{R}} K$. Corollary 2.46 shows that $\dim_{\mathbb{R}} D = n^2$. Since K has to be $\mathbb{R}$ or $\mathbb{C}$, n has to be 1 or 2. If $n = 1$, we obtain $D \cong \mathbb{R}$. Thus we may assume that $n = 2$, $K = \mathbb{C}$, and $\dim_{\mathbb{R}} D = 4$.

The map $f : K \to D$ given by $f(a + bi) = a - bi$, where i is the member of K corresponding to $\sqrt{-1}$ in $\mathbb{C}$, is an algebra homomorphism into a central simple algebra over $\mathbb{R}$, and so is the map $g : K \to D$ given by $g(a+bi) = a+bi$. By the Skolem–Noether Theorem (Theorem 2.41), there exists some x in D with $x(a + bi)x^{-1} = a - bi$ for all a and b in $\mathbb{R}$.

This element x has the property that x^2 commutes with every element of K and must lie in K, by Corollary 2.47. Let us see that x^2 lies in $\text{center}(D) = \mathbb{R}$. In fact, otherwise 1 and x^2 would generate K as an $\mathbb{R}$ algebra, and every member of D commuting with 1 and x^2 would commute with all of K; since x commutes with 1 and x^2, x would have to commute with K, contradiction. Thus x^2 lies in $\mathbb{R}$.

If $x^2 > 0$, then $x^2 = r^2$ for some $r \in \mathbb{R}$. The elements x and r together lie in some subfield K' of D, and K' has no zero divisors. Since $(x - r)(x + r) = 0$ within K', we conclude that $x = \pm r$. Then x commutes with the maximal subfield K above, and we arrive at a contradiction.

Thus $x^2 < 0$. Write $x^2 = -y^2$ for some $y \in \mathbb{R}$, and put $j = y^{-1}x$. The equation $x(a+bi)x^{-1} = a-bi$ says that $j(a+bi)j^{-1} = a-bi$ and in particular that $jij^{-1} = -i$. Define $k = ij$.

We have $j^2 = y^{-2}x^2 = -1$. Hence $k^2 = ijij = i(jij^{-1})j^2 = i(-i)(-1) = i^2 = -1$. Then $ijk = -1$, and $k = -1(j^{-1})(i^{-1}) = -1(-j)(-i) = -ji$; hence $ij + ji = 0$.

Let us show that $\{1, i, j, k\}$ is a linearly independent set over $\mathbb{R}$. Certainly j is not an $\mathbb{R}$ linear combination of 1 and i. If $k = a + bi + cj$ for some $a, b, c \in \mathbb{R}$, then squaring gives

$$\begin{aligned} -1 = k^2 &= a^2 + b^2i^2 + c^2j^2 + 2abi + 2acj + bc(ij + ji) \\ &= a^2 - b^2 - c^2 + 2abi + 2acj. \end{aligned}$$

Equating coefficients of 1, i, and j, we obtain $-1 = a^2 - b^2 - c^2$, $ab = 0$, and $ac = 0$. We cannot have $-1 = a^2$, and thus at least one of b and c is nonzero. Then $a = 0$, and $ij = k = bi + cj$. Left multiplication by i gives $-j = -b + cij = -b + c(bi + cj)$; equating coefficients shows that $b = 0$. Hence $ij = cj$, and we arrive at the contradiction $i = c \in \mathbb{R}$. We conclude that $\{1, i, j, k\}$ is linearly independent over $\mathbb{R}$.

To complete the proof that D is isomorphic to $\mathbb{H}$, we have only to verify that $\{1, i, j, k\}$ satisfies the usual multiplication table for $\mathbb{H}$. We know that $i^2 = j^2 = k^2 = -1$, that $k = ij$, and that $k = -ji$. The last of these says that $ji = -k$. The other verifications are

$$\begin{aligned} jk &= jij = (jij^{-1})j^2 = (-i)(-1) = i, \\ kj &= ijj = i(-1) = -i, \\ ki &= iji = i(jij^{-1})j = i(-i)j = j, \\ ik &= iij = (-1)j = -j, \end{aligned}$$

and the proof is complete. □

11. Problems

In all the problems below, all algebras are assumed to be associative.

1. Let G be a finite group, and let $\mathbb{C}G$ be its complex group algebra. Prove that $\mathbb{C}G$ is a semisimple ring, and identify the constituent matrix algebras that arise for $\mathbb{C}G$ in Theorem 2.2 in terms of the irreducible representations of G.
2. Wedderburn's Main Theorem (Theorem 2.17) decomposes finite-dimensional algebras A in characteristic 0 as $A = S \oplus \operatorname{rad} A$ for some subalgebra S.
   (a) What explicitly is a decomposition $A = S \oplus \operatorname{rad} A$ for the complex algebra $\mathbb{C}[X]/(X^2+1)^2$?
   (b) Is the subalgebra S in (a) unique? Prove that it is, or give a counterexample.
   (c) Answer the same questions as for (a) and (b) in the case of the real algebra $\mathbb{R}[X]/(X^2+1)^2$.
3. Let A and B be finite-dimensional algebras with identity over a field F, and suppose that B is central simple. Prove that $\operatorname{rad}(A \otimes_F B) = (\operatorname{rad} A) \otimes_F B$.

Problems 4–7 concern commutative Artinian rings. Let R be such a ring.

4. Prove that
   (a) R has only finitely many maximal ideals,
   (b) $\operatorname{rad} R$ is the set of all nilpotent elements in R,
   (c) R is semisimple if and only if it has no nonzero nilpotent elements,
   (d) R semisimple implies that R is the direct product of fields.
5. Let $\bar{e}$ be an idempotent in $R/\operatorname{rad} R$. Prove that the idempotent $e \in R$ in Proposition 2.23 with $\bar{e} = e + \operatorname{rad} R$ is unique.
6. Problem 4a shows that R has only finitely many maximal ideals. Let N be their product. Use Nakayama's Lemma (Lemma 8.51 of *Basic Algebra*, restated in the present book on page xxv) to prove that N is a nilpotent ideal in R.
7. Deduce from the previous problem that any prime ideal in R contains one of the finitely many maximal ideals, hence that every prime ideal in R is maximal.

Problems 8–11 concern triangular rings, which were introduced in an example after Proposition 2.5. The problems ask for verifications for some assertions that were made in that example without proof. The notation is as follows: R and S are rings with identity, and M is a unital (R, S) bimodule. Define a set A and operations of addition and multiplication symbolically by

$$A = \begin{pmatrix} R & M \\ 0 & S \end{pmatrix} = \left\{ \begin{pmatrix} r & m \\ 0 & s \end{pmatrix} \,\middle|\, r \in R,\ m \in M,\ s \in S \right\}$$

with

$$\begin{pmatrix} r & m \\ 0 & s \end{pmatrix} \begin{pmatrix} r' & m' \\ 0 & s' \end{pmatrix} = \begin{pmatrix} rr' & rm' + ms' \\ 0 & ss' \end{pmatrix}.$$

8. Prove that the left ideals in A are of the form $I_1 \oplus I_2$, where I_2 is a left ideal in S and I_1 is a left R submodule of $R \oplus M$ containing MI_2. (Educational note: Then similarly the right ideals in A are of the form $J_1 \oplus J_2$, where J_1 is a right ideal in R and J_2 is a right S submodule of $M \oplus S$ containing $J_1 M$.)

9. (a) Prove that the ring A is left Noetherian if and only if R and S are left Noetherian and M satisfies the ascending chain condition for its left R submodules.
   (b) Prove that the ring A is right Noetherian if and only if R and S are right Noetherian and M satisfies the ascending chain condition for its right S submodules. (Educational note: By similar arguments the conclusions of (a) and (b) remain valid if "Noetherian" is replaced by "Artinian" and "ascending" is replaced by "descending.")

10. If $A = \left(\begin{smallmatrix} R & R \\ 0 & S \end{smallmatrix}\right)$ is any ring such as $\left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$ in which S is a (commutative) Noetherian integral domain with field of fractions R and if $S \neq R$, prove that A is left Noetherian and not right Noetherian, and A is neither left nor right Artinian.

11. If $A = \left(\begin{smallmatrix} R & R \\ 0 & S \end{smallmatrix}\right)$ is a ring such as $\left(\begin{smallmatrix} \mathbb{Q}(x) & \mathbb{Q}(x) \\ 0 & \mathbb{Q} \end{smallmatrix}\right)$ in which R and S are fields with $S \subseteq R$ and $\dim_S R$ is infinite, prove that A is left Noetherian and left Artinian, and A is neither right Noetherian nor right Artinian.

Problems 12–16 concern **generalized quaternion algebras**. Let F be a field of characteristic other than 2, let K be a quadratic extension field, and let σ be the nontrivial element in the Galois group. The field K is necessarily of the form $K = F(\sqrt{m})$ for some nonsquare $m \in F$, and the elements c of K for which $\sigma(c) = -c$ are the F multiples of $\sqrt{m}$. Fix an element $r \neq 0$ of F, and let A be the subset of $M_2(K)$ given by $\left(\begin{smallmatrix} a & b \\ r\sigma(b) & \sigma(a) \end{smallmatrix}\right)$.

12. (a) Prove that A is a 4-dimensional algebra over F.
   (b) Prove that A is central simple by examining $cx - xc$ for $c = \left(\begin{smallmatrix} \sqrt{m} & 0 \\ 0 & -\sqrt{m} \end{smallmatrix}\right)$ when $x \neq 0$ is in a two-sided ideal I and is not in $K \cong \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & \sigma(a) \end{smallmatrix}\right) \right\}$.

13. Prove that A is a division algebra if and only if r is not of the form $N_{K/F}(c)$ for some $c \in K$. Why must A be isomorphic to $M_2(F)$ when A is not a division algebra?
14. Prove that if r and r' are two members of F such that $r = r'N_{K/F}(c)$ for some c in K, then the algebra A associated to r is isomorphic to the algebra associated to r'.
15. Let $\{1, i, j, k\}$ be the F basis of A consisting of the matrices
$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} \sqrt{m} & 0 \\ 0 & -\sqrt{m} \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{m} \\ -r\sqrt{m} & 0 \end{pmatrix}.$$
Prove that these satisfy $i^2 = m1$, $j^2 = r1$, $k^2 = -rm1$, $ij = k = -ji$, $jk = -ri = -kj$, and $ki = -mj = -ik$.
16. By going over the proof of Theorem 2.50 and using the relations of the previous problem, prove that every central simple algebra of dimension 4 over F is of the same kind as A for some quadratic extension $K = F(\sqrt{m})$ and some member $r \neq 0$ of F.

Problems 17–19 concern **cyclic algebras**, which were introduced by L. E. Dickson. These extend the theory of generalized quaternion algebras to other sizes of matrices. The analogy with the theory in Problems 12–16 is tightest when the size is a prime. For notational simplicity this set of problems asks about size 3. Let F be any field, and let K be a finite Galois extension of F with cyclic Galois group. It is assumed in these problems that K has degree 3 over F and that $\{1, \sigma, \sigma^2\}$ is the Galois group. Fix an element $r \neq 0$ of F, and let A be the subset of $M_3(K)$ given by $\begin{pmatrix} a & b & c \\ r\sigma(c) & \sigma(a) & \sigma(b) \\ r\sigma^2(b) & r\sigma^2(c) & \sigma^2(a) \end{pmatrix}$. Identifying $a \in K$ with the member $\begin{pmatrix} a & 0 & 0 \\ 0 & \sigma(a) & 0 \\ 0 & 0 & \sigma^2(a) \end{pmatrix}$ of A and letting j be the member $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ r & 0 & 0 \end{pmatrix}$ of A allows one to view A as the set of all matrices $a + bj + cj^2$ with $a, b, c \in K$. The element j satisfies $jaj^{-1} = \sigma(a)$ for $a \in K$ and $j^3 = r$.

17. Arguing as for Problem 12, show that A is an algebra over F and that it is central simple of dimension 9.
18. Using the general theory, prove that A either is a division algebra over F or is isomorphic to $M_3(F)$, and that $A \cong M_3(F)$ if and only if there is a 3-dimensional vector subspace of A that is a left A submodule of A. (Educational note: This problem makes crucial use of the fact that the size 3 is a prime.)
19. (a) Prove that if $r = N_{K/F}(d)$ for some $d \in K$, then the 3-dimensional vector subspace $K(1 + d^{-1}j + d^{-1}\sigma(d)^{-1}j^2)$ of A is a left A submodule.
    (b) Prove that any 3-dimensional left K submodule of A is necessarily of the form $K(a_0 + b_0 j + c_0 j^2)$ for some nonzero $a_0 + b_0 j + c_0 j^2$ in A and that this left K submodule is a left A submodule only if there exists an element $d \in K$ with $N_{K/F}(d) = r$, $da_0 = r\sigma(c_0)$, $db_0 = \sigma(a_0)$, and $dc_0 = \sigma(b_0)$.