Algebras

3

In many physical applications, a vector space $\mathcal{V}$ has a natural "product", i.e., a binary operation $\mathcal{V} \times \mathcal{V} \to \mathcal{V}$, which we call multiplication. The prime example of such a vector space is the vector space of matrices. It is therefore useful to consider vector spaces for which such a product exists.

3.1 From Vector Space to Algebra

In this section, we define an algebra, give some familiar examples of algebras, and discuss some of their basic properties.

algebra defined

Definition 3.1.1 An **algebra** $\mathcal{A}$ over $\mathbb{C}$ (or $\mathbb{R}$) is a vector space over $\mathbb{C}$ (or $\mathbb{R}$), together with a binary operation $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$, called **multiplication**. The image of $(\mathbf{a}, \mathbf{b}) \in \mathcal{A} \times \mathcal{A}$ under this mapping[1] is denoted by $\mathbf{ab}$, and it satisfies the following two relations

$$\mathbf{a}(\beta\mathbf{b} + \gamma\mathbf{c}) = \beta\mathbf{ab} + \gamma\mathbf{ac}$$
$$(\beta\mathbf{b} + \gamma\mathbf{c})\mathbf{a} = \beta\mathbf{ba} + \gamma\mathbf{ca}$$

dimension of the algebra; associativity; commutativity; identity; and right and left inverses

for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{A}$ and $\beta, \gamma \in \mathbb{C}$ (or $\mathbb{R}$). The dimension of the vector space is called the **dimension of the algebra**. The algebra is called **associative** if the product satisfies $\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c}$ and **commutative** if it satisfies $\mathbf{ab} = \mathbf{ba}$. An algebra with **identity** is an algebra that has an element $\mathbf{1}$ satisfying $\mathbf{a1} = \mathbf{1a} = \mathbf{a}$. An element $\mathbf{b}$ of an algebra with identity is said to be a **left inverse** of $\mathbf{a}$ if $\mathbf{ba} = \mathbf{1}$. **Right inverse** is defined similarly. The identity is also called **unit**, and an algebra with identity is also called a **unital algebra**.

It is sometimes necessary to use a different notation for the identity of an algebra. This happens especially when we are discussing several algebras at the same time. A common notation other than $\mathbf{1}$ is $\mathbf{e}$.

[1] We shall, for the most part, abandon the Dirac bra-and-ket notation in this chapter due to its clumsiness; instead we use boldface roman letters to denote vectors.

S. Hassani, *Mathematical Physics*, DOI 10.1007/978-3-319-01195-0_3,

3.1.1 General Properties

Taking $\beta = 1 = -\gamma$ and $\mathbf{b} = \mathbf{c}$ in the definition above leads immediately to

$$\mathbf{a0} = \mathbf{0a} = \mathbf{0} \quad \forall \mathbf{a} \in \mathcal{A}.$$

The identity of an algebra is unique. If there were two identities $\mathbf{1}$ and $\mathbf{e}$, then $\mathbf{1e} = \mathbf{e}$, because $\mathbf{1}$ is the identity, and $\mathbf{1e} = \mathbf{1}$, because $\mathbf{e}$ is the identity.

If $\mathcal{A}$ is an associative algebra and $\mathbf{a} \in \mathcal{A}$ has both a left inverse $\mathbf{b}$ and a right inverse $\mathbf{c}$, then the two are equal:

$$\mathbf{bac} = (\mathbf{ba})\mathbf{c} = \mathbf{1c} = \mathbf{c},$$

$$\mathbf{bac} = \mathbf{b}(\mathbf{ac}) = \mathbf{b1} = \mathbf{b}.$$

Therefore, in an associative algebra, we talk of an inverse without specifying right or left. Furthermore, it is trivial to show that the (two-sided) inverse is unique. Hence, we have

Theorem 3.1.2 *Let $\mathcal{A}$ be an associative algebra with identity. If $\mathbf{a} \in \mathcal{A}$ has a right and a left inverse, then they are equal and this single inverse is unique. We denote it by $\mathbf{a}^{-1}$. If $\mathbf{a}$ and $\mathbf{b}$ are invertible, then $\mathbf{ab}$ is also invertible, and*

$$(\mathbf{ab})^{-1} = \mathbf{b}^{-1}\mathbf{a}^{-1}.$$

The proof of the last statement is straightforward.

subalgebra of an algebra

Definition 3.1.3 Let $\mathcal{A}$ be an algebra and $\mathcal{A}'$ a linear subspace of $\mathcal{A}$. If $\mathcal{A}'$ is closed under multiplication, i.e., if $\mathbf{ab} \in \mathcal{A}'$ whenever $\mathbf{a} \in \mathcal{A}'$ and $\mathbf{b} \in \mathcal{A}'$, then $\mathcal{A}'$ is called a **subalgebra** of $\mathcal{A}$.

Clearly, a subalgebra of an associative (commutative) algebra is also associative (commutative).

subalgebra generated by a subset

Let $\mathcal{A}$ be an associative algebra and S a subset of $\mathcal{A}$. The **subalgebra generated by** S is the collection of all linear combinations of

$$\mathbf{s}_1\mathbf{s}_2 \ldots \mathbf{s}_k, \quad \mathbf{s}_i \in S.$$

If S consists of a single element $\mathbf{s}$, then the subalgebra generated by $\mathbf{s}$ is the set of polynomials in $\mathbf{s}$.

$\mathbb{C}$ is a subalgebra of any unital algebra.

Example 3.1.4 Let $\mathcal{A}$ be a unital algebra, then the vector space

$$\mathrm{Span}\{\mathbf{1}\} = \{\alpha\mathbf{1} \mid \alpha \in \mathbb{C}\}$$

is a subalgebra of $\mathcal{A}$. Since $\mathrm{Span}\{\mathbf{1}\}$ is indistinguishable from $\mathbb{C}$, we sometimes say that $\mathbb{C}$ is a subalgebra of $\mathcal{A}$.

center of an algebra

Definition 3.1.5 Let $\mathcal{A}$ be an algebra. The set of elements of $\mathcal{A}$ which commute with all elements of $\mathcal{A}$ is called the **center** of $\mathcal{A}$ and denoted by $\mathcal{Z}(\mathcal{A})$.

Table 3.1 The multiplication table for $\mathcal{S}$

	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$-\mathbf{e}_3$	$-\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$-\mathbf{e}_2$	$-\mathbf{e}_1$	$\mathbf{e}_0$

$\mathcal{Z}(\mathcal{A})$ is easily shown to be a subspace of $\mathcal{A}$, and if $\mathcal{A}$ is associative, then $\mathcal{Z}(\mathcal{A})$ is a subalgebra of $\mathcal{A}$.

Definition 3.1.6 A unital algebra $\mathcal{A}$ is called **central** if $\mathcal{Z}(\mathcal{A}) = \text{Span}\{\mathbf{1}\}$. central algebra

Example 3.1.7 Consider the algebra $\mathcal{S}$ with basis $\{\mathbf{e}_i\}_{i=0}^3$ and multiplication table given in Table 3.1, where for purely aesthetic reasons the identity has been denoted by $\mathbf{e}_0$.

We want to see which elements belong to the center. Let $\mathbf{a} \in \mathcal{Z}(\mathcal{S})$. Then for any arbitrary element $\mathbf{b} \in \mathcal{S}$, we must have $\mathbf{ab} = \mathbf{ba}$. Let

$$\mathbf{a} = \sum_{i=0}^{3} \alpha_i \mathbf{e}_i \quad \text{and} \quad \mathbf{b} = \sum_{i=0}^{3} \beta_i \mathbf{e}_i .$$

Then a straightforward calculation shows that

$$\begin{aligned} \mathbf{ab} = &(\alpha_0\beta_0 + \alpha_1\beta_1 - \alpha_2\beta_2 + \alpha_3\beta_3)\mathbf{e}_0 \\ &+ (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)\mathbf{e}_1 \\ &+ (\alpha_0\beta_2 + \alpha_1\beta_3 + \alpha_2\beta_0 - \alpha_3\beta_1)\mathbf{e}_2 \\ &+ (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)\mathbf{e}_3, \end{aligned}$$

with a similar expression for $\mathbf{ba}$, in which αs and βs are switched. It is easy to show that the two expressions are equal if and only if

$$\alpha_2\beta_3 = \alpha_3\beta_2 \quad \text{and} \quad \alpha_1\beta_3 = \alpha_3\beta_1 .$$

This can hold for arbitrary $\mathbf{b}$ only if $\alpha_1 = \alpha_2 = \alpha_3 = 0$, with α_0 arbitrary. Therefore, $\mathbf{a} \in \mathcal{Z}(\mathcal{S})$ if and only if $\mathbf{a}$ is a multiple of $\mathbf{e}_0$, i.e., if and only if $\mathbf{a} \in \text{Span}\{\mathbf{e}_0\}$. Therefore, $\mathcal{S}$ is central.

Let A and B be subsets of an algebra $\mathcal{A}$. We denote by AB the set of elements in $\mathcal{A}$ which can be written as the sum of products of an element in A by an element in B:

$$AB \equiv \left\{ \mathbf{x} \in \mathcal{A} \mid \mathbf{x} = \sum_k \mathbf{a}_k \mathbf{b}_k,\ \mathbf{a}_k \in A, \mathbf{b}_k \in B \right\}. \tag{3.1}$$

In particular,

$$\mathcal{A}^2 \equiv \left\{ \mathbf{x} \in \mathcal{A} \mid \mathbf{x} = \sum_k \mathbf{a}_k \mathbf{b}_k,\ \mathbf{a}_k, \mathbf{b}_k \in \mathcal{A} \right\} \tag{3.2}$$

derived algebra

is called the **derived algebra** of $\mathcal{A}$.

Algebra **opposite to** $\mathcal{A}$

Definition 3.1.8 Given any algebra $\mathcal{A}$, in which $(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{ab}$, we can obtain a second algebra $\mathcal{A}^{\text{op}}$ in which $(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{ba}$. We write

$$(\mathbf{ab})^{\text{op}} = \mathbf{ba}$$

and call $\mathcal{A}^{\text{op}}$ the algebra **opposite to** $\mathcal{A}$.

It is obvious that if $\mathcal{A}$ is associative, so is $\mathcal{A}^{\text{op}}$, and if $\mathcal{A}$ is commutative, then $\mathcal{A}^{\text{op}} = \mathcal{A}$.

Example 3.1.9 Here are some examples of algebra:

- Define the following product on $\mathbb{R}^2$:

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1).$$

  The reader is urged to verify that this product turns $\mathbb{R}^2$ into a commutative algebra.
- Similarly, the vector (cross) product on $\mathbb{R}^3$ turns it into a nonassociative, noncommutative algebra.
- The paradigm of all algebras is the **matrix algebra** whose binary operation is ordinary multiplication of $n \times n$ matrices. This algebra is associative but not commutative.
- Let $\mathcal{A}$ be the set of $n \times n$ matrices. Define the binary operation, denoted by $\bullet$, as

$$\mathsf{A} \bullet \mathsf{B} \equiv \mathsf{AB} - \mathsf{BA}, \tag{3.3}$$

  where the RHS is ordinary matrix multiplication. The reader may check that $\mathcal{A}$ together with this operation becomes a nonassociative, noncommutative algebra.
- Let $\mathcal{A}$ be the set of $n \times n$ upper triangular matrices, i.e., matrices all of whose elements below the diagonal are zero. With ordinary matrix multiplication, this set turns into an associative, noncommutative algebra, as the reader can verify.
- Let $\mathcal{A}$ be the set of $n \times n$ upper triangular matrices. Define the binary operation as in Eq. (3.3). The reader may check that $\mathcal{A}$ together with this operation becomes a nonassociative, noncommutative algebra. The derived algebra $\mathcal{A}^2$ of $\mathcal{A}$ is the set of $n \times n$ *strictly upper triangular matrices*, i.e., upper triangular matrices whose diagonal elements are all zero.
- We have already established that the set of linear transformations $L(\mathcal{V}, \mathcal{W})$ from $\mathcal{V}$ to $\mathcal{W}$ is a vector space. Let us attempt to define a multiplication as well. The best candidate is the composition of linear transformations. If $\mathbf{T} : \mathcal{V} \to \mathcal{U}$ and $\mathbf{S} : \mathcal{U} \to \mathcal{W}$ are linear operators, then the composition $\mathbf{S} \circ \mathbf{T} : \mathcal{V} \to \mathcal{W}$ is also a linear operator, as can easily be verified. This product, however, is not defined on a single vector space, but is such that it takes an element in $L(\mathcal{V}, \mathcal{U})$ and another element in

a second vector space $L(\mathcal{U}, \mathcal{W})$ to give an element in yet another vector space $L(\mathcal{V}, \mathcal{W})$. An algebra requires a single vector space. We can accomplish this by letting $\mathcal{V} = \mathcal{U} = \mathcal{W}$. Then the three spaces of linear transformations collapse to the single space $L(\mathcal{V}, \mathcal{V})$, the set of endomorphisms of $\mathcal{V}$, which we have abbreviated as $\mathcal{L}(\mathcal{V})$ or End$(\mathcal{V})$ and to which $\mathbf{T}$, $\mathbf{S}$, $\mathbf{ST} \equiv \mathbf{S} \circ \mathbf{T}$, and $\mathbf{TS} \equiv \mathbf{T} \circ \mathbf{S}$ belong.

- All the examples above are finite-dimensional algebras. An example of an infinite-dimensional algebra is $\mathcal{C}^r(a, b)$, the vector space of real-valued functions defined on a real interval (a, b), which have derivatives up to order r. The multiplication is defined pointwise: If $f \in \mathcal{C}^r(a, b)$ and $g \in \mathcal{C}^r(a, b)$, then

$$(fg)(t) \equiv f(t)g(t) \quad \forall t \in (a, b).$$

  This algebra is commutative and associative, and has the identity element $f(t) = 1$.
- Another example of an infinite dimensional algebra is the algebra of polynomials.[2] This algebra is a commutative and associative algebra with identity.

Definition 3.1.10 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras. Then the *vector* direct sum $\mathcal{A} \oplus \mathcal{B}$ becomes an **algebra direct sum** if we define the following product

algebra direct sum

$$(\mathbf{a}_1 \oplus \mathbf{b}_1)(\mathbf{a}_2 \oplus \mathbf{b}_2) = (\mathbf{a}_1\mathbf{a}_2 \oplus \mathbf{b}_1\mathbf{b}_2)$$

on $\mathcal{A} \oplus \mathcal{B}$.

Note that if an element $\mathbf{a}$ is in $\mathcal{A}$, then it can be represented by $\mathbf{a} \oplus \mathbf{0}$ as an element of $\mathcal{A} \oplus \mathcal{B}$. Similarly, an element $\mathbf{b}$ in $\mathcal{B}$ can be represented by $\mathbf{0} \oplus \mathbf{b}$. Thus the product of any element in $\mathcal{A}$ with any element in $\mathcal{B}$ is zero, i.e., $\mathcal{AB} = \mathcal{BA} = \{\mathbf{0}\}$. As we shall see later, this condition becomes necessary if a given algebra is to be the direct sum of its subalgebras.

In order for $\mathbf{a} \oplus \mathbf{b}$ to be in the center of $\mathcal{A} \oplus \mathcal{B}$, we must have

$$(\mathbf{a} \oplus \mathbf{b})(\mathbf{x} \oplus \mathbf{y}) = (\mathbf{x} \oplus \mathbf{y})(\mathbf{a} \oplus \mathbf{b}),$$

or

$$\mathbf{ax} \oplus \mathbf{by} = \mathbf{xa} \oplus \mathbf{yb} \quad \text{or} \quad (\mathbf{ax} - \mathbf{xa}) \oplus (\mathbf{by} - \mathbf{yb}) = \mathbf{0},$$

for all $\mathbf{x} \in \mathcal{A}$ and $\mathbf{y} \in \mathcal{B}$. For this to hold, we must have

$$\mathbf{ax} - \mathbf{xa} = \mathbf{0} \quad \text{and} \quad \mathbf{by} - \mathbf{yb} = \mathbf{0},$$

i.e., that $\mathbf{a} \in \mathcal{Z}(\mathcal{A})$ and $\mathbf{b} \in \mathcal{Z}(\mathcal{B})$. Hence,

$$\mathcal{Z}(\mathcal{A} \oplus \mathcal{B}) = \mathcal{Z}(\mathcal{A}) \oplus \mathcal{Z}(\mathcal{B}). \tag{3.4}$$

Definition 3.1.11 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras. Then the vector space tensor

algebra tensor product

[2] It should be clear that the algebra of polynomials cannot be finite dimensional.

product $\mathcal{A}\otimes\mathcal{B}$ becomes an **algebra tensor product** if we define the product

$$(\mathbf{a}_1\otimes\mathbf{b}_1)(\mathbf{a}_2\otimes\mathbf{b}_2)=\mathbf{a}_1\mathbf{a}_2\otimes\mathbf{b}_1\mathbf{b}_2$$

on $\mathcal{A}\otimes\mathcal{B}$. Because of the isomorphism, $\mathcal{A}\otimes\mathcal{B}\cong\mathcal{B}\otimes\mathcal{A}$, we demand that $\mathbf{a}\otimes\mathbf{b}=\mathbf{b}\otimes\mathbf{a}$ for all $\mathbf{a}\in\mathcal{A}$ and $\mathbf{b}\in\mathcal{B}$.

The last condition of the definition becomes an important requirement when we write a given algebra $\mathcal{A}$ as the tensor product of two of its subalgebras $\mathcal{B}$ and $\mathcal{C}$. In such a case, $\otimes$ coincides with the multiplication in $\mathcal{A}$, and the condition becomes the requirement that all elements of $\mathcal{B}$ commute with all elements of $\mathcal{C}$, i.e., $\mathcal{BC}=\mathcal{CB}$.

structure constants of an algebra

Definition 3.1.12 Given an algebra $\mathcal{A}$ and a basis $B=\{\mathbf{e}_i\}_{i=1}^N$ for the underlying vector space, one can write

$$\mathbf{e}_i\mathbf{e}_j=\sum_{k=1}^N c_{ij}^k\mathbf{e}_k,\qquad c_{ij}^k\in\mathbb{C}. \tag{3.5}$$

The complex numbers c_{ij}^k, the components of the vector $\mathbf{e}_i\mathbf{e}_j$ in the basis B, are called the **structure constants** of $\mathcal{A}$.

The structure constants determine the product of any two vectors once they are expressed in terms of the basis vectors of B. Conversely, given any N-dimensional vector space $\mathcal{V}$, one can turn it into an algebra by choosing a basis and a set of N^3 numbers $\{c_{ij}^k\}$ and defining the product of basis vectors by Eq. (3.5).

Example 3.1.13 Let the structure constants in algebras $\mathcal{A}$ and $\mathcal{B}$ be $\{a_{ij}^k\}_{i,j,k=1}^M$ and $\{b_{mn}^l\}_{l,m,n=1}^N$ in their bases $\{\mathbf{e}_i\}_{i=1}^M$ and $\{\mathbf{f}_n\}_{n=1}^N$, respectively. So that

$$\mathbf{e}_i\mathbf{e}_j=\sum_{i,j=1}^M a_{ij}^k\mathbf{e}_k\quad\text{and}\quad\mathbf{f}_m\mathbf{f}_n=\sum_{m,n=1}^N b_{mn}^l\mathbf{f}_l.$$

Construct the MN dimensional algebra $\mathcal{C}$ by defining its structure constants as $c_{im,jn}^{kl}=a_{ij}^k b_{mn}^l$ in a basis $\{\mathbf{v}_{kl}\}_{k,l=1}^{M,N}$, so that

$$\mathbf{v}_{im}\mathbf{v}_{jn}=\sum_{i,j=1}^M\sum_{m,n=1}^N c_{im,jn}^{kl}\mathbf{v}_{kl}=\sum_{i,j=1}^M\sum_{m,n=1}^N a_{ij}^k b_{mn}^l\mathbf{v}_{kl}.$$

This algebra is isomorphic to the algebra $\mathcal{A}\otimes\mathcal{B}$. In fact, if we identify $\mathbf{v}_{kl}$ on the right-hand side as $\mathbf{e}_k\otimes\mathbf{f}_l$, then

$$\begin{aligned}\mathbf{v}_{im}\mathbf{v}_{jn}&=\sum_{i,j=1}^M\sum_{m,n=1}^N c_{im,jn}^{kl}\mathbf{e}_k\otimes\mathbf{f}_l=\sum_{i,j=1}^M\sum_{m,n=1}^N a_{ij}^k b_{mn}^l\mathbf{e}_k\otimes\mathbf{f}_l\\&=\left(\sum_{i,j=1}^M a_{ij}^k\mathbf{e}_k\right)\otimes\left(\sum_{m,n=1}^N b_{mn}^l\mathbf{f}_l\right)=(\mathbf{e}_i\mathbf{e}_j)\otimes(\mathbf{f}_m\mathbf{f}_n),\end{aligned}$$

which is consistent with $\mathbf{v}_{im} \equiv \mathbf{e}_i \otimes \mathbf{f}_m$ and $\mathbf{v}_{jn} \equiv \mathbf{e}_j \otimes \mathbf{f}_n$, and the rule of multiplication of the tensor product of two algebras.

Definition 3.1.14 A unital algebra all of whose nonzero elements have inverses is called a **division algebra**.

division algebra

Example 3.1.15 Let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be a basis of $\mathbb{R}^2$. Let the structure constants be

$$c_{11}^1 = -c_{22}^1 = c_{12}^2 = c_{21}^2 = 1$$
$$c_{12}^1 = -c_{21}^1 = c_{11}^2 = c_{22}^2 = 0,$$

i.e., let

$$\mathbf{e}_1^2 = -\mathbf{e}_2^2 = \mathbf{e}_1, \qquad \mathbf{e}_1\mathbf{e}_2 = \mathbf{e}_2\mathbf{e}_1 = \mathbf{e}_2.$$

Then, it is easy to prove that the algebra so constructed is just $\mathbb{C}$. All that needs to be done is to identify $\mathbf{e}_1$ with 1 and $\mathbf{e}_2$ with $\sqrt{-1}$. Clearly, $\mathbb{C}$ is a division algebra.

Example 3.1.16 In the standard basis $\{\mathbf{e}_i\}_{i=0}^3$ of $\mathbb{R}^4$, choose the structure constants as follows:

$$\mathbf{e}_0^2 = -\mathbf{e}_1^2 = -\mathbf{e}_2^2 = -\mathbf{e}_3^2 = \mathbf{e}_0,$$
$$\mathbf{e}_0\mathbf{e}_i = \mathbf{e}_i\mathbf{e}_0 = \mathbf{e}_i \quad \text{for } i = 1, 2, 3,$$
$$\mathbf{e}_i\mathbf{e}_j = \sum_{k=1}^{3} \epsilon_{ijk}\mathbf{e}_k \quad \text{for } i, j = 1, 2, 3,\ i \neq j,$$

where ϵ_{ijk} is completely antisymmetric in all its indices (therefore vanishing if any two of its indices are equal) and $\epsilon_{123} = 1$. The reader may verify that these relations turn $\mathbb{R}^4$ into an associative, but noncommutative, algebra. This algebra is called the **algebra of quaternions** and denoted by $\mathbb{H}$. In this context, $\mathbf{e}_0$ is usually denoted by 1, and $\mathbf{e}_1$, $\mathbf{e}_2$, and $\mathbf{e}_3$ by i, j, and k, respectively, and one writes $q = x + iy + jz + kw$ for an element of $\mathbb{H}$. It then becomes evident that $\mathbb{H}$ is a generalization of $\mathbb{C}$. In analogy with $\mathbb{C}$, x is called the **real part** of q, and (y, z, w) the **pure part** of q. Similarly, the **conjugate** of q is $q^* = x - iy - jz - kw$.

algebra of quaternions

It is convenient to write $q = x_0 + \mathbf{x}$, where $\mathbf{x}$ is a three-dimensional vector. Then $q^* = x_0 - \mathbf{x}$. Furthermore, one can show that, with $q = x_0 + \mathbf{x}$ and $p = y_0 + \mathbf{y}$,

$$qp = \underbrace{x_0y_0 - \mathbf{x}\cdot\mathbf{y}}_{\text{real part of } qp} + \underbrace{x_0\mathbf{y} + y_0\mathbf{x} + \mathbf{x}\times\mathbf{y}}_{\text{pure part of } qp}. \tag{3.6}$$

Changing $\mathbf{x}$ to $-\mathbf{x}$ and $\mathbf{y}$ to $-\mathbf{y}$ in the expression above, one gets

$$q^*p^* = x_0y_0 - \mathbf{x}\cdot\mathbf{y} - x_0\mathbf{y} - y_0\mathbf{x} + \mathbf{x}\times\mathbf{y},$$

which is not equal to $(qp)^*$. However, it is easy to show that $(qp)^* = p^*q^*$.

Substituting q^* for p in (3.6), we get $qq^* = x_0^2 + |\mathbf{x}|^2$. The **absolute value** of q, denoted by $|q|$ is—similar to the absolute value of a complex number—given by $|q| = \sqrt{qq^*}$. If $q \neq 0$, then $q^*/(x_0^2 + |\mathbf{x}|^2)$ is the inverse of q. Thus, the algebra of quaternions is a division algebra.

It is not hard to show that

$$q^n = \sum_{k=0}^{[n]/2} (-1)^k \binom{n}{2k} x_0^{n-2k} |\mathbf{x}|^{2k} + \sum_{k=0}^{[n]/2} (-1)^k \binom{n}{2k+1} x_0^{n-2k-1} |\mathbf{x}|^{2k} \mathbf{x}, \tag{3.7}$$

where $[n] = n$ if n is even and $[n] = n - 1$ if n is odd.

In order for $\mathbf{a} \otimes \mathbf{b}$ to be in the center of $\mathcal{A} \otimes \mathcal{B}$, we must have

$$(\mathbf{a} \otimes \mathbf{b})(\mathbf{x} \otimes \mathbf{y}) = (\mathbf{x} \otimes \mathbf{y})(\mathbf{a} \otimes \mathbf{b}),$$

or

$$\mathbf{ax} \otimes \mathbf{by} = \mathbf{xa} \otimes \mathbf{yb}$$

for all $\mathbf{x} \in \mathcal{A}$ and $\mathbf{y} \in \mathcal{B}$. For this to hold, we must have

$$\mathbf{ax} = \mathbf{xa} \quad \text{and} \quad \mathbf{by} = \mathbf{yb},$$

i.e., that $\mathbf{a} \in \mathcal{Z}(\mathcal{A})$ and $\mathbf{b} \in \mathcal{Z}(\mathcal{B})$. Hence,

$$\mathcal{Z}(\mathcal{A} \otimes \mathcal{B}) = \mathcal{Z}(\mathcal{A}) \otimes \mathcal{Z}(\mathcal{B}). \tag{3.8}$$

Generator of an algebra

Let $\mathcal{A}$ be an associative algebra. A subset $S \subset \mathcal{A}$ is called the **generator** of $\mathcal{A}$ if every element of $\mathcal{A}$ can be expressed as a linear combination of the products of elements in S. A basis of the *vector space* $\mathcal{A}$ is clearly a generator of $\mathcal{A}$. However, it is not the smallest generator, because it may be possible to obtain the entire basis vectors by multiplying a subset of them. For example, $(\mathbb{R}^3, \times)$, the algebra of vectors under cross product, has the basis $\{\hat{\mathbf{e}}_x, \hat{\mathbf{e}}_y, \hat{\mathbf{e}}_z\}$, but $\{\hat{\mathbf{e}}_x, \hat{\mathbf{e}}_y\}$—or any other *pair* of unit vectors—is a generator because $\hat{\mathbf{e}}_z = \hat{\mathbf{e}}_x \times \hat{\mathbf{e}}_y$.

3.1.2 Homomorphisms

The linear transformations connecting vector spaces can be modified slightly to accommodate the binary operation of multiplication of the corresponding algebras:

Homomorphism, monomorphism, epimorphism, and isomorphism of algebras

Definition 3.1.17 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras. A linear map[3] $\phi : \mathcal{A} \to \mathcal{B}$ is called an **algebra homomorphism** if $\phi(\mathbf{ab}) = \phi(\mathbf{a})\phi(\mathbf{b})$. An injective, surjective, or bijective algebra homomorphism is called, respectively, a **monomorphism**, an **epimorphism**, or an **isomorphism**. An isomorphism of an algebra onto itself is called an **automorphism**.

[3] It is more common to use ϕ, ψ etc. instead of $\mathbf{T}$, $\mathbf{U}$, etc. for linear maps of *algebras*.

Example 3.1.18 Let $\mathcal{A}$ be $\mathbb{R}^3$, and $\mathcal{B}$ the set of 3×3 matrices of the form

$$\mathsf{A} = \begin{pmatrix} 0 & a_1 & -a_2 \\ -a_1 & 0 & a_3 \\ a_2 & -a_3 & 0 \end{pmatrix}.$$

Then the map $\phi : \mathcal{A} \to \mathcal{B}$ defined by

$$\phi(\mathbf{a}) = \phi(a_1, a_2, a_3) = \begin{pmatrix} 0 & a_1 & -a_2 \\ -a_1 & 0 & a_3 \\ a_2 & -a_3 & 0 \end{pmatrix}$$

can be shown to be a *linear* isomorphism. Let the cross product be the binary operation on $\mathcal{A}$, turning it into an algebra. For $\mathcal{B}$, define the binary operation of Eq. (3.3). The reader may check that, with these operations, ϕ is extended to an *algebra* isomorphism.

Proposition 3.1.19 *Let $\mathcal{A}$ and $\mathcal{B}$ be algebras. Let $\{\mathbf{e}_i\}$ be a basis of $\mathcal{A}$ and $\phi : \mathcal{A} \to \mathcal{B}$ a linear transformation. Then ϕ is an algebra homomorphism if and only if*

$$\phi(\mathbf{e}_i \mathbf{e}_j) = \phi(\mathbf{e}_i)\phi(\mathbf{e}_j).$$

Proof If $\mathbf{a} = \sum_i \alpha_i \mathbf{e}_i$ and $\mathbf{b} = \sum_j \beta_j \mathbf{e}_j$, then

$$\begin{aligned} \phi(\mathbf{ab}) &= \phi\left(\left(\sum_i \alpha_i \mathbf{e}_i\right)\left(\sum_j \beta_j \mathbf{e}_j\right)\right) = \phi\left(\sum_i \alpha_i \sum_j \beta_j \mathbf{e}_i \mathbf{e}_j\right) \\ &= \sum_i \alpha_i \sum_j \beta_j \phi(\mathbf{e}_i \mathbf{e}_j) = \sum_i \alpha_i \sum_j \beta_j \phi(\mathbf{e}_i)\phi(\mathbf{e}_j) \\ &= \sum_i \alpha_i \phi(\mathbf{e}_i) \sum_j \beta_j \phi(\mathbf{e}_j) = \phi\left(\sum_i \alpha_i \mathbf{e}_i\right)\phi\left(\sum_j \beta_j \mathbf{e}_j\right) \\ &= \phi(\mathbf{a})\phi(\mathbf{b}). \end{aligned}$$

The converse is trivial. □

Example 3.1.20 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras and $\phi : \mathcal{A} \to \mathcal{B}$ a homomorphism. Theorem 2.3.10 ensures that $\phi(\mathcal{A})$ is a sub*space* of $\mathcal{B}$. Now let $\mathbf{b}_1, \mathbf{b}_2 \in \phi(\mathcal{A})$. Then there exist $\mathbf{a}_1, \mathbf{a}_2 \in \mathcal{A}$ such that $\mathbf{b}_1 = \phi(\mathbf{a}_1)$ and $\mathbf{b}_2 = \phi(\mathbf{a}_2)$. Furthermore,

$$\mathbf{b}_1 \mathbf{b}_2 = \phi(\mathbf{a}_1)\phi(\mathbf{a}_2) = \phi(\mathbf{a}_1 \mathbf{a}_2), \quad \Rightarrow \quad \mathbf{b}_1 \mathbf{b}_2 \in \phi(\mathcal{A}).$$

Hence, $\phi(\mathcal{A})$ is a subalgebra of $\mathcal{B}$.

Example 3.1.21 Let $\mathcal{A}$ be a real algebra with identity $\mathbf{1}$. Let $\phi : \mathbb{R} \to \mathcal{A}$ be the linear mapping given by $\phi(\alpha) = \alpha\mathbf{1}$. Considering $\mathbb{R}$ as an algebra over itself, we have

$\mathbb{R}$ (or $\mathbb{C}$) is a subalgebra of any unital algebra.

$$\phi(\alpha\beta) = \alpha\beta\mathbf{1} = (\alpha\mathbf{1})(\beta\mathbf{1}) = \phi(\alpha)\phi(\beta).$$

This shows that ϕ is an algebra homomorphism. Furthermore,

$$\phi(\alpha_1) = \phi(\alpha_2) \quad \Rightarrow \quad \alpha_1 \mathbf{1} = \alpha_2 \mathbf{1} \quad \Rightarrow \quad (\alpha_1 - \alpha_2)\mathbf{1} = 0 \quad \Rightarrow \quad \alpha_1 = \alpha_2.$$

Hence, ϕ is a monomorphism. Therefore, we can identify $\mathbb{R}$ with $\phi(\mathbb{R})$, and consider $\mathbb{R}$ as a subalgebra of $\mathcal{A}$. This is the same conclusion we arrived at in Example 3.1.4.

Definition 3.1.22 Let $\mathcal{A}$ and $\mathcal{B}$ be unital algebras. A homomorphism $\phi : \mathcal{A} \to \mathcal{B}$ is called **unital** if $\phi(\mathbf{1}_A) = \mathbf{1}_B$.

One can show the following:

Proposition 3.1.23 *Let $\mathcal{A}$ and $\mathcal{B}$ be unital algebras. If $\phi : \mathcal{A} \to \mathcal{B}$ is an epimorphism, then ϕ is unital.*

Example 3.1.9 introduced the algebra $\mathcal{L}(\mathcal{V})$ of endomorphisms (operators) on $\mathcal{V}$. This algebra has an identity $\mathbf{1}$ which maps every vector to itself.

involution

Definition 3.1.24 An endomorphism ω of $\mathcal{V}$ whose square is $\mathbf{1}$ is called an **involution**.

In particular, $\mathbf{1} \in \text{End}(\mathcal{V})$ is an involution. If ω_1 and ω_2 are involutions such that $\omega_1 \circ \omega_2 = \omega_2 \circ \omega_1$, then $\omega_1 \circ \omega_2$ is also an involution.

Involutions do not affect the identity of the algebra.

For an algebra, we require that an involution be a homomorphism, not just a linear map. Let $\mathcal{A}$ be an algebra and let $\mathcal{H}(\mathcal{A})$ denote the set of homomorphisms of $\mathcal{A}$. An involution $\omega \in \mathcal{H}(\mathcal{A})$ satisfies $\omega \circ \omega = \iota \in \mathcal{H}(\mathcal{A})$, of course.[4] Now, if $\mathcal{A}$ has an identity $\mathbf{e}$, then $\omega(\mathbf{e})$ must be equal to $\mathbf{e}$. Indeed, let $\omega(\mathbf{e}) = \mathbf{a}$, then, since $\omega \circ \omega = \iota$, we must have $\omega(\mathbf{a}) = \mathbf{e}$ and

$$\omega(\mathbf{ea}) = \omega(\mathbf{e})\omega(\mathbf{a}) = \omega(\mathbf{e})\mathbf{e} = \omega(\mathbf{e})$$

applying ω to both sides, we get $\mathbf{ea} = \mathbf{e}$. This can happen only if $\mathbf{a} = \mathbf{e}$.

Theorem 3.1.25 *Let $\mathcal{U}$ and $\mathcal{V}$ be two isomorphic vector spaces. Then the algebras $\mathcal{L}(\mathcal{U})$ and $\mathcal{L}(\mathcal{V})$ are isomorphic as algebras.*

Proof Let $\phi : \mathcal{U} \to \mathcal{V}$ be a vector-space isomorphism. Define $\Phi : \mathcal{L}(\mathcal{U}) \to \mathcal{L}(\mathcal{V})$ by

$$\Phi(\mathbf{T}) = \phi \circ \mathbf{T} \circ \phi^{-1}.$$

It is easy to show that Φ is an algebra isomorphism. □

A consequence of this theorem and Theorem 2.3.20 is that $\mathcal{L}(\mathcal{V})$, the algebra of the linear transformations of any real vector space $\mathcal{V}$, is isomorphic to $\mathcal{L}(\mathbb{R}^N)$, where N is the dimension of $\mathcal{V}$. Similarly, $\mathcal{L}(\mathcal{V})$ is isomorphic to $\mathcal{L}(\mathbb{C}^N)$ if $\mathcal{V}$ is an N-dimensional complex vector space.

[4] In keeping with our notation, we use ι for the identity homomorphism of the algebra $\mathcal{A}$.

3.2 Ideals

Subalgebras are subspaces which are stable under multiplication of their elements; i.e., the product of elements of a subalgebra do not leave the subalgebra. Of more importance in algebra theory are those subspaces which are stable under multiplication of its elements by the entire algebra.

Definition 3.2.1 Let $\mathcal{A}$ be an algebra. A subspace $\mathcal{B}$ of $\mathcal{A}$ is called a **left ideal** of $\mathcal{A}$ if it contains **ab** for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$. Using Eq. (3.1), we write this as $\mathcal{AB} \subset \mathcal{B}$. A **right ideal** is defined similarly with $\mathcal{BA} \subset \mathcal{B}$. A **two-sided ideal**, or simply an **ideal**, is a subspace that is both a left ideal and a right ideal.

left, right, and two-sided ideals

It is clear from the definition that an ideal is automatically a subalgebra, and that the only ideal of a unital algebra containing the identity, or an invertible element, is the algebra itself.

an ideal is a subalgebra

Example 3.2.2 Let $\mathcal{A}$ be an associative algebra and $\mathbf{a} \in \mathcal{A}$. Let $\mathcal{L}(\mathbf{a})$ be the set of elements $\mathbf{x} \in \mathcal{A}$ such that $\mathbf{xa} = \mathbf{0}$. For any $\mathbf{x} \in \mathcal{L}(\mathbf{a})$ and any $\mathbf{y} \in \mathcal{A}$, we have

left and right annihilators

$$(\mathbf{yx})\mathbf{a} = \mathbf{y}(\mathbf{xa}) = \mathbf{0},$$

i.e., $\mathbf{yx} \in \mathcal{L}(\mathbf{a})$. So, $\mathcal{L}(\mathbf{a})$ is a left ideal in $\mathcal{A}$. It is called the **left annihilator of a**. Similarly, one can construct $\mathcal{R}(\mathbf{a})$, the right annihilator of **a**.

Example 3.2.3 Let $\mathcal{C}^r(a, b)$ be the algebra of all r times differentiable real-valued functions on an interval (a, b) (see Example 3.1.9). The set of functions that vanish at a given fixed point $c \in (a, b)$ constitutes an ideal in $\mathcal{C}^r(a, b)$. Since the algebra is commutative, the ideal is two-sided.

More generally, let $\mathcal{M}_n$ be the (noncommutative) algebra of matrices with entries $f_{ij} \in \mathcal{C}^r(a, b)$. Then the set of matrices whose entries vanish at a given fixed point $c \in (a, b)$ constitutes a two-sided ideal in $\mathcal{M}_n$.

Let $\mathcal{A}$ and $\mathcal{B}$ be algebras and $\phi : \mathcal{A} \to \mathcal{B}$ a homomorphism. By Theorem 2.3.9, $\ker\phi$ is a sub*space* of $\mathcal{A}$. Now let $\mathbf{x} \in \ker\phi$ and $\mathbf{a} \in \mathcal{A}$. Then

$$\phi(\mathbf{xa}) = \phi(\mathbf{x})\phi(\mathbf{a}) = \mathbf{0}\phi(\mathbf{a}) = \mathbf{0},$$

i.e., $\mathbf{xa} \in \ker\phi$. This shows that $\ker\phi$ is a right ideal in $\mathcal{A}$. Similarly, one can show that $\ker\phi$ is a left ideal in $\mathcal{A}$.

Theorem 3.2.4 *Let $\phi : \mathcal{A} \to \mathcal{B}$ be a homomorphism of algebras. Then* $\ker\phi$ *is a (two-sided) ideal of $\mathcal{A}$.*

One can easily construct left ideals for an associative algebra $\mathcal{A}$: Take any element $\mathbf{x} \in \mathcal{A}$ and consider the set

ideals generated by an element of an associative algebra

$$\mathcal{A}\mathbf{x} \equiv \{\mathbf{ax} \mid \mathbf{a} \in \mathcal{A}\}.$$

The reader may check that $\mathcal{A}\mathbf{x}$ is a left ideal. Similarly, $\mathbf{x}\mathcal{A}$ is a right ideal, and the set

$$\mathcal{A}\mathbf{x}\mathcal{A} \equiv \{\mathbf{axb} \mid \mathbf{a}, \mathbf{b} \in \mathcal{A}\}$$

is a two-sided ideal. These are all called left, right, and two-sided **ideals generated by x**.

minimal left, right, and two-sided ideals

Definition 3.2.5 A left (right, two-sided) ideal $\mathcal{M}$ of an algebra $\mathcal{A}$ is called **minimal** if every left (right, two-sided) ideal of $\mathcal{A}$ contained in $\mathcal{M}$ coincides with $\mathcal{M}$.

Theorem 3.2.6 *Let $\mathcal{L}$ be a left ideal of $\mathcal{A}$. Then the following statements are equivalent*:

(a) $\mathcal{L}$ *is a minimal left ideal.*
(b) $\mathcal{A}\mathbf{x} = \mathcal{L}$ *for all* $\mathbf{x} \in \mathcal{L}$.
(c) $\mathcal{L}\mathbf{x} = \mathcal{L}$ *for all* $\mathbf{x} \in \mathcal{L}$.

Similar conditions hold for a minimal right ideal.

Proof The proof follows directly from the definition of ideals and minimal ideals. □

Theorem 3.2.7 *Let $\mathcal{A}$ and $\mathcal{B}$ be algebras, $\phi : \mathcal{A} \to \mathcal{B}$ an epimorphism, and $\mathcal{L}$ a (minimal) left ideal of $\mathcal{A}$. Then $\phi(\mathcal{L})$ is a (minimal) left ideal of $\mathcal{B}$. In particular, any automorphism of an algebra is an isomorphism among its minimal ideals.*

Proof Let $\mathbf{b}$ be any element of $\mathcal{B}$ and $\mathbf{y}$ any element of $\phi(\mathcal{L})$. Then there exist elements $\mathbf{a}$ and $\mathbf{x}$ of $\mathcal{A}$ and $\mathcal{L}$, respectively, such that $\mathbf{b} = \phi(\mathbf{a})$ and $\mathbf{y} = \phi(\mathbf{x})$. Furthermore,

$$\mathbf{by} = \phi(\mathbf{a})\phi(\mathbf{x}) = \phi(\mathbf{ax}) \in \phi(\mathcal{L})$$

because $\mathbf{ax} \in \mathcal{L}$. Hence, $\phi(\mathcal{L})$ is an ideal in $\mathcal{B}$.

Now suppose $\mathcal{L}$ is minimal. To show that $\phi(\mathcal{L})$ is minimal, we use (b) of Theorem 3.2.6. Since ϕ is an epimorphism, we have $\mathcal{B} = \phi(\mathcal{A})$. Therefore, let $\mathbf{u} \in \phi(\mathcal{L})$. Then there exists $\mathbf{t} \in \mathcal{L}$ such that $\mathbf{u} = \phi(\mathbf{t})$ and

$$\mathcal{B}\mathbf{u} = \phi(\mathcal{A})\phi(\mathbf{t}) = \phi(\mathcal{A}\mathbf{t}) = \phi(\mathcal{L}).$$

The last statement of the theorem follows from the fact that $\ker\phi$ is an ideal of $\mathcal{A}$. □

algebra direct sums

Definition 3.2.8 $\mathcal{A}$ is the **direct sum** of its subalgebras $\mathcal{B}$ and $\mathcal{C}$ if $\mathcal{A} = \mathcal{B} \oplus \mathcal{C}$ as a vector space and $\mathcal{B}\mathcal{C} = \mathcal{C}\mathcal{B} = \{\mathbf{0}\}$. $\mathcal{B}$ and $\mathcal{C}$ are called **components** of $\mathcal{A}$. Obviously, an algebra can have several components. An algebra is called **reducible** if it is the direct sum of subalgebras.

Table 3.2 The multiplication table for $\mathcal{S}$

	$\mathbf{f}_1$	$\mathbf{f}_2$	$\mathbf{f}_3$	$\mathbf{f}_4$
$\mathbf{f}_1$	$\mathbf{f}_1$	$\mathbf{f}_2$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{f}_2$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{f}_2$	$\mathbf{f}_1$
$\mathbf{f}_3$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{f}_3$	$\mathbf{f}_4$
$\mathbf{f}_4$	$\mathbf{f}_4$	$\mathbf{f}_3$	$\mathbf{0}$	$\mathbf{0}$

As we saw in Definition 3.1.10, the condition $\mathcal{BC} = \mathcal{CB} = \{\mathbf{0}\}$ is necessary if $\mathcal{B}$ and $\mathcal{C}$ are to be naturally identified as $\mathcal{B} \oplus \{\mathbf{0}\}$ and $\mathcal{C} \oplus \{\mathbf{0}\}$, respectively.

Proposition 3.2.9 *A central algebra is not reducible.*

Proof Suppose that the (necessarily unital) central algebra $\mathcal{A}$ is reducible. Then the identity has components in each of the subalgebras of which $\mathcal{A}$ is composed. Clearly, these components are linearly independent and all belong to the center. This is a contradiction. □

Example 3.2.10 Consider $\mathcal{S}$, the algebra introduced in Example 3.1.7. Construct a new basis $\{\mathbf{f}_i\}_{i=1}^4$ as follows:[5]

$$\begin{aligned} \mathbf{f}_1 &= \frac{1}{2}(\mathbf{e}_0 + \mathbf{e}_3), \qquad & \mathbf{f}_2 &= \frac{1}{2}(\mathbf{e}_1 - \mathbf{e}_2), \\ \mathbf{f}_3 &= \frac{1}{2}(\mathbf{e}_0 - \mathbf{e}_3), \qquad & \mathbf{f}_4 &= \frac{1}{2}(\mathbf{e}_1 + \mathbf{e}_2). \end{aligned} \tag{3.9}$$

The multiplication table for $\mathcal{S}$ in terms of the new basis vectors is given in Table 3.2, as the reader may verify.

Multiplying both sides of the identity $\mathbf{e}_0 = \mathbf{f}_1 + \mathbf{f}_3$ by an arbitrary element of $\mathcal{S}$, we see that any such element can be written as a vector in the left ideal $\mathcal{L}_1 \equiv \mathcal{S}\mathbf{f}_1$ plus a vector in the left ideal $\mathcal{L}_3 \equiv \mathcal{S}\mathbf{f}_3$. Any vector in $\mathcal{L}_1$ can be written as a product of some vector in $\mathcal{S}$ and $\mathbf{f}_1$. Let $\mathbf{a} = \sum_{i=1}^4 \alpha_i \mathbf{f}_i$ be an arbitrary element of $\mathcal{S}$. Then any vector in $\mathcal{L}_1$ is of the form

$$\mathbf{a}\mathbf{f}_1 = (\alpha_1\mathbf{f}_1 + \alpha_2\mathbf{f}_2 + \alpha_3\mathbf{f}_3 + \alpha_4\mathbf{f}_4)\mathbf{f}_1 = \alpha_1\mathbf{f}_1 + \alpha_4\mathbf{f}_4,$$

i.e., that $\mathbf{f}_1$ and $\mathbf{f}_4$ span $\mathcal{L}_1$. Similarly, $\mathbf{f}_2$ and $\mathbf{f}_3$ span $\mathcal{L}_3$. It follows that $\mathcal{L}_1 \cap \mathcal{L}_3 = \{\mathbf{0}\}$. Therefore, we have

$$\mathcal{S} = \mathcal{L}_1 \oplus_V \mathcal{L}_3, \qquad \mathcal{L}_1 = \mathrm{Span}\{\mathbf{f}_1, \mathbf{f}_4\}, \qquad \mathcal{L}_3 = \mathrm{Span}\{\mathbf{f}_2, \mathbf{f}_3\},$$

where $\oplus_V$ indicates a vector space direct sum. Note that there is no contradiction between this direct sum decomposition and the fact that $\mathcal{S}$ is central because the direct sum above is not an algebra direct sum since $\mathcal{L}_1\mathcal{L}_3 \neq \{\mathbf{0}\}$.

[5] The reader is advised to show that $\{\mathbf{f}_i\}_{i=1}^4$ is a linearly independent set of vectors.

Let $\mathbf{x} = \gamma_1\mathbf{f}_1 + \gamma_4\mathbf{f}_4$ be an arbitrary nonzero element of $\mathcal{L}_1$. Then clearly, $\mathcal{S}\mathbf{x} \subseteq \mathcal{L}_1$. To show that $\mathcal{L}_1 \subseteq \mathcal{S}\mathbf{x}$, let $\mathbf{y} = \beta_1\mathbf{f}_1 + \beta_4\mathbf{f}_4$ be in $\mathcal{L}_1$. Can we find $\mathbf{z} \in \mathcal{S}$ such that $\mathbf{y} = \mathbf{z}\mathbf{x}$? Let $\mathbf{z} = \sum_{i=1}^{4} \eta_i\mathbf{f}_i$ and note that

$$\begin{aligned}\mathbf{z}\mathbf{x} &= (\eta_1\mathbf{f}_1 + \eta_2\mathbf{f}_2 + \eta_3\mathbf{f}_3 + \eta_4\mathbf{f}_4)(\gamma_1\mathbf{f}_1 + \gamma_4\mathbf{f}_4)\\ &= (\eta_1\gamma_1 + \eta_2\gamma_4)\mathbf{f}_1 + (\eta_3\gamma_4 + \eta_4\gamma_1)\mathbf{f}_4.\end{aligned}$$

We are looking for a set of η's satisfying

$$\eta_1\gamma_1 + \eta_2\gamma_4 = \beta_1 \quad \text{and} \quad \eta_3\gamma_4 + \eta_4\gamma_1 = \beta_4.$$

If $\gamma_1 \neq 0$, then $\eta_1 = \beta_1/\gamma_1$, $\eta_2 = 0 = \eta_3$, $\eta_4 = \beta_4/\gamma_1$ yields a solution for $\mathbf{z}$. If $\gamma_4 \neq 0$, then $\eta_2 = \beta_1/\gamma_4$, $\eta_1 = 0 = \eta_4$, $\eta_3 = \beta_4/\gamma_4$ yields a solution for $\mathbf{z}$. Therefore, $\mathcal{L}_1 = \mathcal{S}\mathbf{x}$, and by Theorem 3.2.6, $\mathcal{L}_1$ is minimal. Similarly, $\mathcal{L}_3$ is also minimal.

If $\mathcal{A} = \mathcal{B} \oplus \mathcal{C}$, then multiplying both sides on the right by $\mathcal{B}$, we get

$$\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{B} \oplus \mathcal{C}\mathcal{B} = \mathcal{B}\mathcal{B} \oplus \{\mathbf{0}\} = \mathcal{B}\mathcal{B} \subset \mathcal{B},$$

showing that $\mathcal{B}$ is a left ideal of $\mathcal{A}$. Likewise, multiplying on the left leads to the fact that $\mathcal{B}$ is a right ideal of $\mathcal{A}$. Thus it is an ideal of $\mathcal{A}$. Similarly, $\mathcal{C}$ is an ideal of $\mathcal{A}$. Moreover, since the subalgebras do not share any nonzero elements, any other ideal of $\mathcal{A}$ must be contained in the subalgebras. We thus have

Proposition 3.2.11 *If $\mathcal{A}$ is the direct sum of algebras, then each component (or the direct sum of several components) is an ideal of $\mathcal{A}$. Furthermore, any other ideal of $\mathcal{A}$ is contained entirely in one of the components.*

simple algebra

Algebras which have no proper ideals are important in the classification of all algebras.

Definition 3.2.12 An algebra $\mathcal{A}$ is called **simple** if its only ideals are $\mathcal{A}$ and $\{\mathbf{0}\}$.

Recall that by ideal we mean two-sided ideal. Therefore, a simple algebra can have proper left ideals and proper right ideals. In fact, the following example illustrates this point.

Example 3.2.13 Let's go back to algebra $\mathcal{S}$ of Example 3.2.10, where we saw that $\mathcal{S} = \mathcal{L}_1 \oplus_V \mathcal{L}_3$ in which $\mathcal{L}_1$ and $\mathcal{L}_3$ are minimal left ideals and $\oplus_V$ indicates direct sum of vector spaces. Can $\mathcal{S}$ have a proper two-sided ideal? Let $\mathcal{I}$ be such an ideal and let $\mathbf{a} \in \mathcal{I}$ be nonzero. By the decomposition of $\mathcal{S}$, $\mathbf{a} = \mathbf{a}_1 + \mathbf{a}_3$ with $\mathbf{a}_1 \in \mathcal{L}_1$ and $\mathbf{a}_3 \in \mathcal{L}_3$, at least one of which must be nonzero. Suppose $\mathbf{a}_1 \neq \mathbf{0}$. Then $\mathcal{S}\mathbf{a}_1$ is a nonzero left ideal which is contained in $\mathcal{L}_1$. Since $\mathcal{L}_1$ is minimal, $\mathcal{S}\mathbf{a}_1 = \mathcal{L}_1$. Since $\mathbf{f}_1 \in \mathcal{L}_1$ there must exist

$\mathbf{b} \in \mathcal{S}$ such that $\mathbf{ba}_1 = \mathbf{f}_1$, and hence,

$$\mathbf{ba} = \mathbf{ba}_1 + \mathbf{ba}_3 = \mathbf{f}_1 + \mathbf{ba}_3.$$

Multiplying both sides on the right by $\mathbf{f}_1$ and noting that $\mathbf{f}_1^2 = \mathbf{f}_1$ and $\mathcal{L}_3\mathbf{f}_1 = \{\mathbf{0}\}$ by the multiplication table of Example 3.2.10, we obtain $\mathbf{baf}_1 = \mathbf{f}_1$. Since $\mathcal{I}$ is a two-sided ideal and $\mathbf{a} \in \mathcal{I}$, $\mathbf{baf}_1 \in \mathcal{I}$, and therefore, $\mathbf{f}_1 \in \mathcal{I}$.

The equality $\mathcal{S}\mathbf{a}_1 = \mathcal{L}_1$, also implies that there exists $\mathbf{c} \in \mathcal{S}$ such that $\mathbf{ca}_1 = \mathbf{f}_4$, and hence,

$$\mathbf{ca} = \mathbf{ca}_1 + \mathbf{ca}_3 = \mathbf{f}_4 + \mathbf{ca}_3.$$

Multiplying both sides on the right by $\mathbf{f}_1$ and noting that $\mathbf{f}_4\mathbf{f}_1 = \mathbf{f}_4$ and $\mathcal{L}_3\mathbf{f}_1 = \{\mathbf{0}\}$, we obtain $\mathbf{caf}_1 = \mathbf{f}_4$. Since $\mathcal{I}$ is a two-sided ideal, we must have $\mathbf{f}_4 \in \mathcal{I}$. Since $\mathbf{f}_1\mathbf{f}_2 = \mathbf{f}_2$ and $\mathbf{f}_4\mathbf{f}_2 = \mathbf{f}_3$, all the basis vectors are in $\mathcal{I}$. Hence, $\mathcal{I} = \mathcal{S}$. The case where $\mathbf{a}_3 \neq \mathbf{0}$ leads to the same conclusion. Therefore, $\mathcal{S}$ has no *proper* ideal, i.e., $\mathcal{S}$ is simple.

An immediate consequence of Definition 3.2.12 and Theorem 3.2.4 is

Proposition 3.2.14 *A nontrivial homomorphism of a simple algebra $\mathcal{A}$ with any other algebra $\mathcal{B}$ is necessarily injective.*

Proof For any $\phi : \mathcal{A} \to \mathcal{B}$, the kernel of ϕ is an ideal of $\mathcal{A}$. Since $\mathcal{A}$ has no proper ideal, $\ker\phi = \mathcal{A}$ or $\ker\phi = \{\mathbf{0}\}$. If ϕ is nontrivial, then $\ker\phi = \{\mathbf{0}\}$, i.e., ϕ is injective. □

3.2.1 Factor Algebras

Let $\mathcal{A}$ be an algebra and $\mathcal{B}$ a subspace of $\mathcal{A}$. Section 2.1.2 showed how to construct the factor space $\mathcal{A}/\mathcal{B}$. Can this space be turned into an algebra? Let $[\![\mathbf{a}]\!]$ and $[\![\mathbf{a}']\!]$ be in $\mathcal{A}/\mathcal{B}$. Then the natural product rule for making $\mathcal{A}/\mathcal{B}$ an algebra is

$$[\![\mathbf{a}]\!][\![\mathbf{a}']\!] = [\![\mathbf{aa}']\!]. \tag{3.10}$$

Under what conditions does this multiplication make sense? Since $[\![\mathbf{a}]\!] = [\![\mathbf{a} + \mathbf{b}]\!]$ and $[\![\mathbf{a}']\!] = [\![\mathbf{a}' + \mathbf{b}']\!]$ for all $\mathbf{b}, \mathbf{b}' \in \mathcal{B}$, for (3.10) to make sense, we must have

$$(\mathbf{a} + \mathbf{b})(\mathbf{a}' + \mathbf{b}') = \mathbf{aa}' + \mathbf{b}''$$

for some $\mathbf{b}''$ in $\mathcal{B}$. Taking $\mathbf{a} = \mathbf{0} = \mathbf{a}'$ yields $\mathbf{bb}' = \mathbf{b}''$. This means that $\mathcal{B}$ must be a subalgebra of $\mathcal{A}$. Taking $\mathbf{a}' = \mathbf{0}$ yields $\mathbf{ab}' + \mathbf{bb}' = \mathbf{b}''$ for all $\mathbf{a} \in \mathcal{A}$, $\mathbf{b}, \mathbf{b}' \in \mathcal{B}$ and some $\mathbf{b}'' \in \mathcal{B}$. This means that $\mathcal{B}$ must be a left ideal of $\mathcal{A}$. Similarly, by setting $\mathbf{a} = \mathbf{0}$ we conclude that $\mathcal{B}$ must be a right ideal of $\mathcal{A}$. We thus have

Proposition 3.2.15 *Let $\mathcal{A}$ be an algebra and $\mathcal{B}$ a subspace of $\mathcal{A}$. Then the factor space $\mathcal{A}/\mathcal{B}$ can be turned into an algebra with multiplication $[\![\mathbf{a}]\!][\![\mathbf{a}']\!] = [\![\mathbf{aa}']\!]$, if and only if $\mathcal{B}$ is an ideal in $\mathcal{A}$. The algebra so constructed is called the **factor algebra** of $\mathcal{A}$ with respect to the ideal $\mathcal{B}$.*

factor algebra

Example 3.2.16 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras and $\phi : \mathcal{A} \to \mathcal{B}$ an algebra homomorphism. Example 3.1.20 and Theorem 3.2.4 showed that $\phi(\mathcal{A})$ is a subalgebra of $\mathcal{B}$ and $\ker\phi$ is an ideal in $\mathcal{A}$. Now consider the linear map $\bar{\phi} : \mathcal{A}/\ker\phi \to \phi(\mathcal{A})$ defined in Example 2.3.22 by $\bar{\phi}([\![\mathbf{a}]\!]) = \phi(\mathbf{a})$. It is straightforward to show that $\bar{\phi}$ is an algebra homomorphism. Using this and Example 2.3.22 where it was shown that $\bar{\phi}$ is a *linear* isomorphism, we conclude that $\bar{\phi}$ is an *algebra* isomorphism.

3.3 Total Matrix Algebra

Consider the vector space of $n \times n$ matrices with its standard basis $\{\mathbf{e}_{ij}\}_{i,j=1}^{n}$, where $\mathbf{e}_{ij}$ has a 1 at the ijth position and zero everywhere else. This means that $(\mathbf{e}_{ij})_{lk} = \delta_{il}\delta_{jk}$, and

$$\begin{aligned}(\mathbf{e}_{ij}\mathbf{e}_{kl})_{mn} &= \sum_{r=1}^{n}(\mathbf{e}_{ij})_{mr}(\mathbf{e}_{kl})_{rn}\\ &= \sum_{r=1}^{n}\delta_{im}\delta_{jr}\delta_{kr}\delta_{ln} = \delta_{im}\delta_{jk}\delta_{ln} = \delta_{jk}(\mathbf{e}_{il})_{mn},\end{aligned}$$

or

$$\mathbf{e}_{ij}\mathbf{e}_{kl} = \delta_{jk}\mathbf{e}_{il}.$$

The structure constants are $c_{ij,kl}^{mn} = \delta_{im}\delta_{jk}\delta_{ln}$. Note that one needs a double index to label these constants.

total matrix algebra
$\mathbb{F} \otimes \mathcal{M}_n$ or $\mathcal{M}_n(\mathbb{F})$

The abstract algebra whose basis is $\{\mathbf{e}_{ij}\}_{i,j=1}^{n}$ with multiplication rules and structure constants given above is called the **total matrix algebra**. Let $\mathbb{F}$ denote either $\mathbb{R}$ or $\mathbb{C}$. Then the total matrix algebra over $\mathbb{F}$ is denoted by $\mathbb{F} \otimes \mathcal{M}_n$ or $\mathcal{M}_n(\mathbb{F})$. It is an associative algebra isomorphic with the real or complex matrix algebra, but its elements are not necessarily $n \times n$ matrices. When the dimension of the matrices is not specified, one writes simply $\mathbb{F} \otimes \mathcal{M}$ or $\mathcal{M}(\mathbb{F})$.

We now construct a left ideal of this algebra. Take $\mathbf{e}_{pq}$ and multiply it on the left by $\sum_{i,j=1}^{n}\alpha_{ij}\mathbf{e}_{ij}$, a general element of $\mathcal{M}_n(\mathbb{F})$. This yields

$$\left(\sum_{i,j=1}^{n}\alpha_{ij}\mathbf{e}_{ij}\right)\mathbf{e}_{pq} = \sum_{i,j=1}^{n}\alpha_{ij}\mathbf{e}_{ij}\mathbf{e}_{pq} = \sum_{i,j=1}^{n}\alpha_{ij}\delta_{jp}\mathbf{e}_{iq} = \sum_{i=1}^{n}\alpha_{ip}\mathbf{e}_{iq},$$

which corresponds to a matrix all of whose columns are zero except the qth column. Let $\mathcal{L}$ be the set of all such matrices. Multiplying an element of $\mathcal{L}$ by a general matrix $\sum_{l,m=1}^{n}\beta_{lm}\mathbf{e}_{lm}$, we obtain[6]

$$\left(\sum_{l,m=1}^{n}\beta_{lm}\mathbf{e}_{lm}\right)\left(\sum_{i=1}^{n}\gamma_{i}\mathbf{e}_{iq}\right) = \sum_{i,l,m=1}^{n}\beta_{lm}\gamma_{i}\mathbf{e}_{lm}\mathbf{e}_{iq} = \sum_{i,l,m=1}^{n}\beta_{lm}\gamma_{i}\delta_{mi}\mathbf{e}_{lq}$$

[6]The index p has no significance in the final answer because all the $\mathbf{e}_{pq}$ with varying p but a fixed q generate the same matrices.

$$= \sum_{l,m=1}^{n} \beta_{lm}\gamma_m \mathbf{e}_{lq} = \sum_{l=1}^{n} \underbrace{\left(\sum_{m=1}^{n} \beta_{lm}\gamma_m \right)}_{\equiv \eta_l} \mathbf{e}_{lq}$$

$$= \sum_{l=1}^{n} \eta_l \mathbf{e}_{lq}.$$

It follows that $\mathcal{L}$ is a left ideal. Furthermore, the very construction of $\mathcal{L}$ implies that it satisfies condition (b) of Theorem 3.2.6. Had we multiplied $\mathbf{e}_{pq}$ on the right, we would have obtained a right ideal consisting of matrices all of whose rows equaled zero except the pth row; and this right ideal would satisfy condition (b) of Theorem 3.2.6 for right minimal ideals. We thus have

Theorem 3.3.1 *The minimal left (right) ideals of $\mathbb{R} \otimes \mathcal{M}$ or $\mathbb{C} \otimes \mathcal{M}$ consist of matrices with all their columns (rows) zero except one.*

Multiplying $\mathbf{e}_{pq}$ on the left and the right by a pair of arbitrary matrices, the reader can easily show that one recovers the entire total matrix algebra. This indicates that the algebra has no proper two-sided ideal. Example 3.3.3 below finds the center of $\mathcal{M}_n(\mathbb{F})$ to be Span$\{\mathbf{1}_n\}$, where $\mathbf{1}_n$ is the identity of $\mathcal{M}_n(\mathbb{F})$. We thus have

Theorem 3.3.2 *The total matrix algebra $\mathcal{M}_n(\mathbb{F})$ is central simple.*

finding the center of $\mathbb{F} \otimes \mathcal{M}_n$

Example 3.3.3 Let $\mathbf{a} = \sum_{i,j=1}^{n} \alpha_{ij}\mathbf{e}_{ij}$ be in the center of $\mathbb{F} \otimes \mathcal{M}_n$. Then

$$\mathbf{a}\mathbf{e}_{kl} = \sum_{i,j=1}^{n} \alpha_{ij}\mathbf{e}_{ij}\mathbf{e}_{kl} = \sum_{i,j=1}^{n} \alpha_{ij}\delta_{jk}\mathbf{e}_{il} = \sum_{i=1}^{n} \alpha_{ik}\mathbf{e}_{il}$$

$$\mathbf{e}_{kl}\mathbf{a} = \sum_{i,j=1}^{n} \mathbf{e}_{kl}\alpha_{ij}\mathbf{e}_{ij} = \sum_{i,j=1}^{n} \alpha_{ij}\delta_{il}\mathbf{e}_{kj} = \sum_{j=1}^{n} \alpha_{lj}\mathbf{e}_{kj}.$$

For these two expressions to be equal, we must have

$$\sum_{i=1}^{n} (\alpha_{ik}\mathbf{e}_{il} - \alpha_{li}\mathbf{e}_{ki}) = 0.$$

By letting $l = k$ in the sum above and invoking the linear independence of $\mathbf{e}_{ij}$, we conclude that $\alpha_{ik} = 0$ if $i \neq k$. Therefore, $\mathbf{a}$ must be a diagonal matrix. Write $\mathbf{a} = \sum_{k=1}^{n} \lambda_k \mathbf{e}_{kk}$ and let $\mathbf{b} = \sum_{i,j=1}^{n} \beta_{ij}\mathbf{e}_{ij}$ be an arbitrary element of $\mathbb{F} \otimes \mathcal{M}_n$. Then

$$\mathbf{a}\mathbf{b} = \sum_{i,j,k=1}^{n} \lambda_k \beta_{ij}\mathbf{e}_{kk}\mathbf{e}_{ij} = \sum_{i,j,k=1}^{n} \lambda_k \beta_{ij}\delta_{ik}\mathbf{e}_{kj} = \sum_{i,j=1}^{n} \lambda_i \beta_{ij}\mathbf{e}_{ij}$$

$$\mathbf{ba} = \sum_{i,j,k=1}^{n} \lambda_k \beta_{ij} \mathbf{e}_{ij} \mathbf{e}_{kk} = \sum_{i,j,k=1}^{n} \lambda_k \beta_{ij} \delta_{jk} \mathbf{e}_{ik} = \sum_{i,j=1}^{n} \lambda_j \beta_{ij} \mathbf{e}_{ij}.$$

Again, because of the linear independence of $\mathbf{e}_{ij}$, for these two expressions to be equal, we must have $\lambda_j \beta_{ij} = \lambda_i \beta_{ij}$ for all i and j and all β_{ij}. The only way this can happen is for λ_i to be equal to λ_j for all i and j. It follows that $\mathbf{a} = \lambda \mathbf{1}_n$, where $\mathbf{1}_n = \sum_{k=1}^{n} \mathbf{e}_{kk}$ is the identity element of $\mathcal{M}_n(\mathbb{F})$. Therefore, $\mathcal{M}_n(\mathbb{F})$ is central.

3.4 Derivation of an Algebra

The last two items in Example 3.1.9 have a feature that turns out to be of great significance in all algebras, the product rule for differentiation.

derivation

Definition 3.4.1 A vector space endomorphism $\mathbf{D} : \mathcal{A} \to \mathcal{A}$ is called a **derivation** on $\mathcal{A}$ if it has the additional property

$$\mathbf{D}(\mathbf{ab}) = \big[\mathbf{D}(\mathbf{a})\big]\mathbf{b} + \mathbf{a}\big[\mathbf{D}(\mathbf{b})\big].$$

Example 3.4.2 Let $\mathcal{C}^r(a, b)$ be as in Example 3.1.9, and let $\mathbf{D}$ be ordinary differentiation: $\mathbf{D} : f \mapsto f'$ where f' is the derivative of f. Then ordinary differentiation rules show that $\mathbf{D}$ is a derivation of the algebra $\mathcal{C}^r(a, b)$.

Example 3.4.3 Consider the algebra of $n \times n$ matrices with multiplication as defined in Eq. (3.3). Let A be a fixed matrix, and define the linear transformation

$$\mathbf{D}_\mathsf{A}(\mathsf{B}) = \mathsf{A} \bullet \mathsf{B}.$$

Then we note that

$$\begin{aligned}\mathbf{D}_\mathsf{A}(\mathsf{B} \bullet \mathsf{C}) &= \mathsf{A} \bullet (\mathsf{B} \bullet \mathsf{C}) = \mathsf{A}(\mathsf{B} \bullet \mathsf{C}) - (\mathsf{B} \bullet \mathsf{C})\mathsf{A} \\ &= \mathsf{A}(\mathsf{BC} - \mathsf{CB}) - (\mathsf{BC} - \mathsf{CB})\mathsf{A} \\ &= \mathsf{ABC} - \mathsf{ACB} - \mathsf{BCA} + \mathsf{CBA}.\end{aligned}$$

On the other hand,

$$\begin{aligned}(\mathbf{D}_\mathsf{A}\mathsf{B}) \bullet \mathsf{C} + \mathsf{B} \bullet (\mathbf{D}_\mathsf{A}\mathsf{C}) &= (\mathsf{A} \bullet \mathsf{B}) \bullet \mathsf{C} + \mathsf{B} \bullet (\mathsf{A} \bullet \mathsf{C}) \\ &= (\mathsf{AB} - \mathsf{BA}) \bullet \mathsf{C} + \mathsf{B} \bullet (\mathsf{AC} - \mathsf{CA}) \\ &= (\mathsf{AB} - \mathsf{BA})\mathsf{C} - \mathsf{C}(\mathsf{AB} - \mathsf{BA}) + \mathsf{B}(\mathsf{AC} - \mathsf{CA}) \\ &\quad - (\mathsf{AC} - \mathsf{CA})\mathsf{B} \\ &= \mathsf{ABC} + \mathsf{CBA} - \mathsf{BCA} - \mathsf{ACB}.\end{aligned}$$

So, $\mathbf{D}_\mathsf{A}$ is a derivation on $\mathcal{A}$.

Theorem 3.4.4 *Let $\{\mathbf{e}_i\}_{i=1}^N$ be a basis of the algebra $\mathcal{A}$. Then a vector space endomorphism $\mathbf{D}:\mathcal{A}\to\mathcal{A}$ is a derivation on $\mathcal{A}$ iff*

$$\mathbf{D}(\mathbf{e}_i\mathbf{e}_j)=\mathbf{D}(\mathbf{e}_i)\cdot\mathbf{e}_j+\mathbf{e}_i\cdot\mathbf{D}(\mathbf{e}_j)\quad \textit{for } i,j=1,2,\ldots,N.$$

Proof The simple proof is left as an exercise for the reader. □

If $\mathcal{A}$ has an identity $\mathbf{e}$, then $\mathbf{D}(\mathbf{e})=\mathbf{0}$, because

$$\mathbf{D}(\mathbf{e})=\mathbf{D}(\mathbf{ee})=\mathbf{D}(\mathbf{e})\mathbf{e}+\mathbf{e}\mathbf{D}(\mathbf{e})=2\mathbf{D}(\mathbf{e}).$$

This shows that $\mathbf{e}\in\ker\mathbf{D}$. In general, one can show that $\ker\mathbf{D}$ is a subalgebra of $\mathcal{A}$.

Proposition 3.4.5 *Every derivation $\mathbf{D}$ satisfies the **Leibniz formula***

Leibniz formula

$$\mathbf{D}^n(\mathbf{ab})=\sum_{k=0}^{n}\binom{n}{k}\mathbf{D}^k(\mathbf{a})\cdot\mathbf{D}^{n-k}(\mathbf{b}). \tag{3.11}$$

Proof The proof by mathematical induction is very similar to the proof of the binomial theorem of Example 1.5.2. The details are left as an exercise for the reader. □

Derivations of $\mathcal{A}$, being endomorphisms of the *vector space* $\mathcal{A}$, are subsets of $\mathrm{End}(\mathcal{A})$. If $\mathbf{D}_1$ and $\mathbf{D}_2$ are derivations, then it is straightforward to show that any linear combination $\alpha\mathbf{D}_1+\beta\mathbf{D}_2$ is also a derivation. Thus, the set of derivations $\mathcal{D}(\mathcal{A})$ on an algebra $\mathcal{A}$ forms a vector space [a subspace of $\mathrm{End}(\mathcal{A})$]. Do they form a sub*algebra* of $\mathrm{End}(\mathcal{A})$? Is $\mathbf{D}_1\mathbf{D}_2$ a derivation? Let's find out!

$$\begin{aligned}\mathbf{D}_1\mathbf{D}_2(\mathbf{ab})&=\mathbf{D}_1\big(\big[\mathbf{D}_2(\mathbf{a})\big]\mathbf{b}+\mathbf{a}\big[\mathbf{D}_2(\mathbf{b})\big]\big)\\&=\big[\mathbf{D}_1\mathbf{D}_2(\mathbf{a})\big]\mathbf{b}+\mathbf{D}_2(\mathbf{a})\mathbf{D}_1(\mathbf{b})+\mathbf{D}_1(\mathbf{a})\mathbf{D}_2(\mathbf{b})+\mathbf{a}\big[\mathbf{D}_1\mathbf{D}_2(\mathbf{b})\big].\end{aligned}$$

So, the product of two derivations is not a derivation, because of the two terms in the middle. However, since these terms are symmetric in their subscripts, we can subtract them away by taking the difference $\mathbf{D}_1\mathbf{D}_2-\mathbf{D}_2\mathbf{D}_1$. The question is whether the result will be a derivation. Switching the order of the subscripts, we obtain

$$\mathbf{D}_2\mathbf{D}_1(\mathbf{ab})=\big[\mathbf{D}_2\mathbf{D}_1(\mathbf{a})\big]\mathbf{b}+\mathbf{D}_1(\mathbf{a})\mathbf{D}_2(\mathbf{b})+\mathbf{D}_2(\mathbf{a})\mathbf{D}_1(\mathbf{b})+\mathbf{a}\big[\mathbf{D}_2\mathbf{D}_1(\mathbf{b})\big].$$

Subtracting this from the previous expression yields

$$\begin{aligned}&(\mathbf{D}_1\mathbf{D}_2-\mathbf{D}_2\mathbf{D}_1)(\mathbf{ab})\\&\quad=\big[\mathbf{D}_1\mathbf{D}_2(\mathbf{a})\big]\mathbf{b}+\mathbf{a}\big[\mathbf{D}_1\mathbf{D}_2(\mathbf{b})\big]-\big[\mathbf{D}_2\mathbf{D}_1(\mathbf{a})\big]\mathbf{b}-\mathbf{a}\big[\mathbf{D}_2\mathbf{D}_1(\mathbf{b})\big]\\&\quad=\big[(\mathbf{D}_1\mathbf{D}_2-\mathbf{D}_2\mathbf{D}_1)(\mathbf{a})\big]\mathbf{b}+\mathbf{a}\big[(\mathbf{D}_1\mathbf{D}_2-\mathbf{D}_2\mathbf{D}_1)(\mathbf{b})\big].\end{aligned}$$

Thus, if we define a new product

$$\mathbf{D}_1\bullet\mathbf{D}_2\equiv\mathbf{D}_1\mathbf{D}_2-\mathbf{D}_2\mathbf{D}_1, \tag{3.12}$$

then $\mathcal{D}(\mathcal{A})$ becomes an algebra.

derivation algebra

Theorem 3.4.6 *The set $\mathcal{D}(\mathcal{A})$ of derivations of $\mathcal{A}$ forms an algebra, the* ***derivation algebra*** *of $\mathcal{A}$ under the product* (3.12).

ϕ-**derivation**

Definition 3.4.7 Let $\mathcal{A}$ and $\mathcal{B}$ be algebras, and $\phi : \mathcal{A} \to \mathcal{B}$ a homomorphism. Then $\mathbf{D} : \mathcal{A} \to \mathcal{B}$ is called a ϕ-**derivation** if

$$\mathbf{D}(\mathbf{a}_1\mathbf{a}_2) = \mathbf{D}(\mathbf{a}_1)\phi(\mathbf{a}_2) + \phi(\mathbf{a}_1)\mathbf{D}(\mathbf{a}_2), \quad \mathbf{a}_1, \mathbf{a}_2 \in \mathcal{A}.$$

Example 3.4.8 As an example, let $\mathbf{D}_A$ be a derivation in $\mathcal{A}$. Then $\mathbf{D} = \phi \circ \mathbf{D}_A$ is a ϕ-derivation, because

$$\begin{aligned}\phi \circ \mathbf{D}_A(\mathbf{a}_1\mathbf{a}_2) &= \phi\big[\mathbf{D}_A(\mathbf{a}_1)\mathbf{a}_2 + \mathbf{a}_1\mathbf{D}_A(\mathbf{a}_2)\big] \\ &= \phi\big[\mathbf{D}_A(\mathbf{a}_1)\big]\phi(\mathbf{a}_2) + \phi(\mathbf{a}_1)\phi\big[\mathbf{D}_A(\mathbf{a}_2)\big] \\ &= \phi \circ \mathbf{D}_A(\mathbf{a}_1)\phi(\mathbf{a}_2) + \phi(\mathbf{a}_1)\phi \circ \mathbf{D}_A(\mathbf{a}_2).\end{aligned}$$

Similarly, if $\mathbf{D}_B$ is a derivation in $\mathcal{B}$, then $\mathbf{D}_B \circ \phi$ is a ϕ-derivation.

More specifically, let $\mathcal{A}$ be the algebra $\mathcal{C}^r(a, b)$ of r-time differentiable functions, and $\mathcal{B}$ be the algebra $\mathbb{R}$ of real numbers. Let $\phi_c : \mathcal{C}^r(a, b) \to \mathbb{R}$ be the evaluation at a fixed point $c \in (a, b)$, so that $\phi_c(f) = f(c)$. If $\mathbf{D}_c : \mathcal{C}^r(a, b) \to \mathbb{R}$ is defined as $\mathbf{D}_c(f) = f'(c)$, then one can readily show that $\mathbf{D}_c$ is a ϕ_c-derivation.

antiderivation

Definition 3.4.9 Let $\mathcal{A}$ be an algebra with identity and ω an involution of $\mathcal{A}$. A linear transformation $\mathbf{\Omega} \in \mathcal{L}(\mathcal{A})$ is called an **antiderivation** of $\mathcal{A}$ with respect to ω if

$$\mathbf{\Omega}(\mathbf{a}_1\mathbf{a}_2) = \mathbf{\Omega}(\mathbf{a}_1) \cdot \mathbf{a}_2 + \omega(\mathbf{a}_1) \cdot \mathbf{\Omega}(\mathbf{a}_2).$$

In particular, a derivation is an antiderivation with respect to to the identity.

As in the case of the derivation, one can show that $\ker\mathbf{\Omega}$ is a subalgebra of $\mathcal{A}$, $\mathbf{\Omega}(\mathbf{e}) = \mathbf{0}$ if $\mathcal{A}$ has an identity $\mathbf{e}$, and $\mathbf{\Omega}$ is determined entirely by its action on the generators of $\mathcal{A}$.

Theorem 3.4.10 *Let $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$ be antiderivations with respect to two involutions ω_1 and ω_2. Suppose that $\omega_1 \circ \omega_2 = \omega_2 \circ \omega_1$. Furthermore assume that*

$$\omega_1\mathbf{\Omega}_2 = \pm\mathbf{\Omega}_2\omega_1 \quad \textit{and} \quad \omega_2\mathbf{\Omega}_1 = \pm\mathbf{\Omega}_1\omega_2.$$

Then $\mathbf{\Omega}_1\mathbf{\Omega}_2 \mp \mathbf{\Omega}_2\mathbf{\Omega}_1$ is an antiderivation with respect to the involution $\omega_1 \circ \omega_2$.

Proof The proof consists of evaluating $\mathbf{\Omega}_1\mathbf{\Omega}_2 \mp \mathbf{\Omega}_2\mathbf{\Omega}_1$ using Definition 3.4.9 for $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$. We leave the straightforward proof for the reader. □

Some particular cases of this theorem are of interest:

- Let $\mathbf{\Omega}$ be an antiderivation with respect to ω and $\mathbf{D}$ a derivation such that $\omega\mathbf{D} = \mathbf{D}\omega$. Then $\mathbf{D\Omega} - \mathbf{\Omega D}$ is an antiderivation with respect to ω.

- Let $\mathbf{\Omega}_1$ and $\mathbf{\Omega}_2$ be antiderivations with respect to the same involution ω such that $\omega\mathbf{\Omega}_i = -\mathbf{\Omega}_i\omega$ for $i = 1, 2$. Then $\mathbf{\Omega}_1\mathbf{\Omega}_2 + \mathbf{\Omega}_2\mathbf{\Omega}_1$ is a derivation.
- A particular example of the second case is when $\mathbf{\Omega}$ is an antiderivation with respect to an involution ω such that $\omega\mathbf{\Omega} = -\mathbf{\Omega}\omega$. Then $\mathbf{\Omega}^2$ is a derivation.

3.5 Decomposition of Algebras

In Sect. 2.1.3, we decomposed a vector space into smaller vector spaces. The decomposition of algebras into "smaller" algebras is also useful. In this section we investigate properties and conditions which allow such a decomposition. All algebras in this section are assumed to be associative.

nilpotent, index, nil, and idempotent

Definition 3.5.1 A nonzero element $\mathbf{a} \in \mathcal{A}$ is called **nilpotent** if $\mathbf{a}^k = \mathbf{0}$ for some positive integer k. The smallest such integer is called the **index** of $\mathbf{a}$. A subalgebra $\mathcal{B}$ of $\mathcal{A}$ is called **nil** if all elements of $\mathcal{B}$ are nilpotent. $\mathcal{B}$ is called nilpotent of index ν if $\mathcal{B}^\nu = \{\mathbf{0}\}$ and $\mathcal{B}^{\nu-1} \neq \{\mathbf{0}\}$.[7] A nonzero element $\mathbf{P} \in \mathcal{A}$ is called **idempotent** if $\mathbf{P}^2 = \mathbf{P}$.

Proposition 3.5.2 *The identity element is the only idempotent in a division algebra.*

Proof The proof is trivial. □

If $\mathbf{P}$ is an idempotent, then $\mathbf{P}^k = \mathbf{P}$ for any positive integer k. Therefore, a nilpotent subalgebra cannot contain an idempotent.

The following theorem, whose rather technical proof can be found in [Bly 90, p. 191], is very useful:

Theorem 3.5.3 *A nil ideal is nilpotent.*

Example 3.5.4 The set of $n \times n$ upper triangular matrices is a subalgebra of the algebra of $n \times n$ matrices, because the product of two upper triangular matrices is an upper triangular matrix, as can be easily verified.

A strictly upper triangular matrix is nilpotent. Let's illustrate this for a 4×4 matrix. With

$$\mathsf{A} = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ 0 & 0 & a_{23} & a_{24} \\ 0 & 0 & 0 & a_{34} \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

[7] Recall that $\mathcal{B}^k$ is the collection of products $\mathbf{a}_1 \dots \mathbf{a}_k$ of elements in $\mathcal{B}$.

it is easily seen that

$$\mathsf{A}^2 = \begin{pmatrix} 0 & 0 & a_{12}a_{23} & a_{12}a_{24} + a_{13}a_{34} \\ 0 & 0 & 0 & a_{23}a_{34} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathsf{A}^3 = \begin{pmatrix} 0 & 0 & 0 & a_{12}a_{23}a_{34} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and

$$\mathsf{A}^4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, the strictly upper triangular 4×4 matrices are nilpotent of index 4. In fact, one can show that the *subalgebra* of the strictly upper triangular 4×4 matrices has index 4.

The reader can convince him/herself that strictly upper triangular $n \times n$ matrices are nilpotent of index n, and that the subalgebra of the strictly upper triangular $n \times n$ matrices is nilpotent of index n.

3.5.1 The Radical

Nilpotent subalgebras play a fundamental role in the classification of algebras. It is remarkable that all the left, right, and two-sided nilpotent ideals of an algebra are contained is a single nilpotent ideal, which we shall explore now.

Lemma 3.5.5 *Let $\mathcal{L}$ and $\mathcal{M}$ be two nilpotent left (right) ideals of the algebra $\mathcal{A}$. Let λ and μ be the indices of $\mathcal{L}$ and $\mathcal{M}$, respectively. Then $\mathcal{L} + \mathcal{M}$ is a left (right) ideal of $\mathcal{A}$ of index at most $\lambda + \mu - 1$.*

Proof We prove the Lemma for left ideals. Clearly, $\mathcal{L} + \mathcal{M}$ is a left ideal. Any element of $\mathcal{L} + \mathcal{M}$ raised to the kth power can be written as a linear combination of elements of the form $\mathbf{a}_1\mathbf{a}_2 \ldots \mathbf{a}_k$ with $\mathbf{a}_i$ belonging to either $\mathcal{L}$ or $\mathcal{M}$. Suppose that l terms of this product are in $\mathcal{L}$ and m terms in $\mathcal{M}$. Let j be the largest integer such that $\mathbf{a}_j \in \mathcal{L}$. Starting with $\mathbf{a}_j$ move to the left until you reach another element of $\mathcal{L}$, say $\mathbf{a}_r$. All the terms $\mathbf{a}_{r+1}$ to $\mathbf{a}_{j-1}$ are in $\mathcal{M}$. Since $\mathcal{L}$ is a left ideal,

$$\underbrace{\mathbf{a}_{r+1} \ldots \mathbf{a}_{j-1}}_{\in \mathcal{A}} \mathbf{a}_j \equiv \mathbf{a}'_j \in \mathcal{L}.$$

This contracts the product $\mathbf{a}_r\mathbf{a}_{r+1}\ldots\mathbf{a}_{j-1}\mathbf{a}_j$ to $\mathbf{a}_r\mathbf{a}'_j$ with both factors in $\mathcal{L}$. Continuing this process, we obtain

$$\mathbf{a}_1\mathbf{a}_2\ldots\mathbf{a}_k = \mathbf{b}_1\mathbf{b}_2\ldots\mathbf{b}_l\mathbf{c}, \quad \mathbf{b}_i \in \mathcal{L},\ \mathbf{c} \in \mathcal{M}.$$

Similarly,

$$\mathbf{a}_1\mathbf{a}_2\ldots\mathbf{a}_k = \mathbf{c}_1\mathbf{c}_2\ldots\mathbf{c}_m\mathbf{b}, \quad \mathbf{b} \in \mathcal{L},\ \mathbf{c}_i \in \mathcal{M}.$$

Since $k = l+m$, if $k = \mu+\lambda-1$, then $(\mu-m)+(\lambda-l) = 1$. This shows that if $m < \mu$, then $l \geq \lambda$ and if $l < \lambda$, then $m \geq \mu$. In either case, $\mathbf{a}_1\ldots\mathbf{a}_k = \mathbf{0}$, by one of the last two equations above. Hence, $\mathcal{L}+\mathcal{M}$ is nilpotent with an index of at most $\mu+\lambda-1$. The proof for the right ideals is identical to this proof. □

Lemma 3.5.6 *Let $\mathcal{L}$ be a nilpotent left ideal of the algebra $\mathcal{A}$. Then the sum $\mathcal{I} = \mathcal{L}+\mathcal{L}\mathcal{A}$ is a nilpotent two-sided ideal.*

Proof Since $\mathcal{L}$ is a left ideal, $\mathcal{A}\mathcal{L} \subseteq \mathcal{L}$. Therefore,

$$\mathcal{A}\mathcal{I} = \mathcal{A}\mathcal{L}+\mathcal{A}\mathcal{L}\mathcal{A} \subseteq \mathcal{L}+\mathcal{L}\mathcal{A} = \mathcal{I},$$

showing that $\mathcal{I}$ is a left ideal. On the other hand,

$$\mathcal{I}\mathcal{A} = \mathcal{L}\mathcal{A}+\mathcal{L}\mathcal{A}\mathcal{A} \subseteq \mathcal{L}\mathcal{A}+\mathcal{L}\mathcal{A} = \mathcal{L}\mathcal{A} \subset \mathcal{I}$$

showing that $\mathcal{I}$ is a right ideal.

Now consider a product of k elements of $\mathcal{L}\mathcal{A}$:

$$\mathbf{l}_1\mathbf{a}_1\mathbf{l}_2\mathbf{a}_2\ldots\mathbf{l}_k\mathbf{a}_k = \mathbf{l}_1\mathbf{l}'_2\mathbf{l}'_3\ldots\mathbf{l}'_k\mathbf{a}_k, \quad \mathbf{l}_j \in \mathcal{L},\ \mathbf{a}_j \in \mathcal{A}$$

where $\mathbf{l}'_i \equiv \mathbf{a}_{i-1}\mathbf{l}_i \in \mathcal{L}$. This shows that if k is equal to the index of $\mathcal{L}$, then the product is zero and hence, $\mathcal{L}\mathcal{A}$ is nilpotent. Note that since some of the $\mathbf{a}$'s may be in $\mathcal{L}$, the index of $\mathcal{L}\mathcal{A}$ is at most equal to the index of $\mathcal{L}$. Invoking Lemma 3.5.5 completes the proof. □

The preceding two lemmas were introduced for the following:

Theorem 3.5.7 *There exists a unique nilpotent ideal in $\mathcal{A}$ which contains every nilpotent left, right, and two-sided ideal of $\mathcal{A}$.*

Proof Let $\mathcal{N}$ be a nilpotent ideal of maximum dimension. Let $\mathcal{M}$ be any nilpotent ideal. By Lemma 3.5.5, $\mathcal{N}+\mathcal{M}$ is both a left and a right nilpotent ideal, hence, a nilpotent ideal. By assumption $\mathcal{N}+\mathcal{M} \subset \mathcal{N}$, and therefore, $\mathcal{M} \subset \mathcal{N}$, proving that $\mathcal{N}$ contains all ideals. If there were another maximal ideal $\mathcal{N}'$, then $\mathcal{N}' \subset \mathcal{N}$ and $\mathcal{N} \subset \mathcal{N}'$, implying that $\mathcal{N}' = \mathcal{N}$, and that $\mathcal{N}$ is unique.

If $\mathcal{L}$ is a left nilpotent ideal, then by Lemma 3.5.6, $\mathcal{L} \subset \mathcal{I} = \mathcal{L}+\mathcal{L}\mathcal{A} \subset \mathcal{N}$, because $\mathcal{I}$ is an ideal. Thus, $\mathcal{N}$ contains all the nilpotent left ideals. Similarly, $\mathcal{N}$ contains all the nilpotent right ideals. □

radical of an algebra

Definition 3.5.8 The unique maximal ideal of an algebra $\mathcal{A}$ guaranteed by Theorem 3.5.7 is called the **radical** of $\mathcal{A}$ and denoted by $\text{Rad}(\mathcal{A})$.

We have seen that a nilpotent algebra cannot contain an idempotent. In fact, the reverse implication is also true. To show that, we need the following

Lemma 3.5.9 *Suppose that $\mathcal{A}$ contains an element $\mathbf{a}$ such that $\mathcal{A}\mathbf{a}^k = \mathcal{A}\mathbf{a}^{k-1}$ for some positive integer k. Then $\mathcal{A}$ contains an idempotent.*

Proof Let $\mathcal{B} \equiv \mathcal{A}\mathbf{a}^{k-1}$. Then $\mathcal{B}$ is a left ideal of $\mathcal{A}$ satisfying $\mathcal{B}\mathbf{a} = \mathcal{B}$. Multiplying both sides by $\mathbf{a}$, we see that

$$\mathcal{B}\mathbf{a}^2 = \mathcal{B}\mathbf{a} = \mathcal{B}, \qquad \mathcal{B}\mathbf{a}^3 = \mathcal{B}\mathbf{a} = \mathcal{B},$$

and $\mathcal{B}\mathbf{a}^k = \mathcal{B}$. But $\mathbf{a}^k \in \mathcal{B}$ because $\mathcal{B} \equiv \mathcal{A}\mathbf{a}^{k-1}$. Thus, with $\mathbf{b} = \mathbf{a}^k$, we get $\mathcal{B}\mathbf{b} = \mathcal{B}$. This means that there must exist an element $\mathbf{P} \in \mathcal{B}$ such that $\mathbf{P}\mathbf{b} = \mathbf{b}$, or $(\mathbf{P}^2 - \mathbf{P})\mathbf{b} = \mathbf{0}$. By Problem 3.32, $\mathbf{P}^2 = \mathbf{P}$. Hence, $\mathcal{B}$, and therefore $\mathcal{A}$ has an idempotent. □

Proposition 3.5.10 *An algebra is nilpotent if and only if it contains no idempotent.*

Proof The "only if" part was shown after Definition 3.5.1. We now show that if $\mathcal{A}$ has no idempotent, then it must be nilpotent. To begin, we note that in general, $\mathcal{A}\mathbf{a} \subseteq \mathcal{A}$, and therefore, $\mathcal{A}\mathbf{a}^k \subseteq \mathcal{A}\mathbf{a}^{k-1}$ for all k. If $\mathcal{A}$ has no idempotent, then the equality is ruled out by Lemma 3.5.9. Hence, $\mathcal{A}\mathbf{a}^k \subset \mathcal{A}\mathbf{a}^{k-1}$. This being true for all k, we have

$$\mathcal{A} \supset \mathcal{A}\mathbf{a} \supset \mathcal{A}\mathbf{a}^2 \supset \cdots \supset \mathcal{A}\mathbf{a}^k \supset \cdots .$$

Since $\mathcal{A}$ has a finite dimension, there must exist an integer r such that $\mathcal{A}\mathbf{a}^r = \{\mathbf{0}\}$ for all $\mathbf{a} \in \mathcal{A}$. In particular, $\mathbf{a}^{r+1} = \mathbf{0}$ for all $\mathbf{a} \in \mathcal{A}$. This shows that $\mathcal{A}$ is nil, and by Theorem 3.5.3, nilpotent. □

Let $\mathbf{P}$ be an idempotent of $\mathcal{A}$. Consider $\mathcal{L}(\mathbf{P})$, the left annihilator of $\mathbf{P}$ (see Example 3.2.2), and note that $(\mathbf{a} - \mathbf{a}\mathbf{P}) \in \mathcal{L}(\mathbf{P})$ for any $\mathbf{a} \in \mathcal{A}$. Furthermore, if $\mathbf{a} \in \mathbf{P}\mathcal{L}(\mathbf{P})$, then $\mathbf{a} = \mathbf{P}\mathbf{x}$ for some $\mathbf{x} \in \mathcal{L}(\mathbf{P})$. Thus, $\mathbf{a}$ has the property that $\mathbf{P}\mathbf{a} = \mathbf{a}$ and $\mathbf{a}\mathbf{P} = \mathbf{0}$.

Similarly, consider $\mathcal{R}(\mathbf{P})$, the right annihilator of $\mathbf{P}$, and note that $(\mathbf{a} - \mathbf{P}\mathbf{a}) \in \mathcal{R}(\mathbf{P})$ for any $\mathbf{a} \in \mathcal{A}$. Furthermore, if $\mathbf{a} \in \mathcal{R}(\mathbf{P})\mathbf{P}$, then $\mathbf{a} = \mathbf{x}\mathbf{P}$ for some $\mathbf{x} \in \mathcal{R}(\mathbf{P})$. Thus, $\mathbf{a}$ has the property that $\mathbf{a}\mathbf{P} = \mathbf{a}$ and $\mathbf{P}\mathbf{a} = \mathbf{0}$.

Let $\mathcal{I}(\mathbf{P}) = \mathcal{L}(\mathbf{P}) \cap \mathcal{R}(\mathbf{P})$. Then, clearly $\mathcal{I}(\mathbf{P})$ is a two-sided ideal consisting of elements $\mathbf{a} \in \mathcal{A}$ such that $\mathbf{a}\mathbf{P} = \mathbf{P}\mathbf{a} = \mathbf{0}$. To these, we add the subalgebra $\mathbf{P}\mathcal{A}\mathbf{P}$, whose elements $\mathbf{a}$ can be shown to have the property $\mathbf{P}\mathbf{a} = \mathbf{a}\mathbf{P} = \mathbf{a}$.

We thus have

$$\begin{aligned}\mathbf{P}\mathcal{A}\mathbf{P} &= \{\mathbf{a}\in\mathcal{A}\mid \mathbf{Pa}=\mathbf{aP}=\mathbf{a}\},\\ \mathbf{P}\mathcal{L}(\mathbf{P}) &= \{\mathbf{a}\in\mathcal{A}\mid \mathbf{Pa}=\mathbf{a},\ \mathbf{aP}=\mathbf{0}\},\\ \mathcal{R}(\mathbf{P})\mathbf{P} &= \{\mathbf{a}\in\mathcal{A}\mid \mathbf{aP}=\mathbf{a},\ \mathbf{Pa}=\mathbf{0}\},\\ \mathcal{I}(\mathbf{P}) &= \{\mathbf{a}\in\mathcal{A}\mid \mathbf{aP}=\mathbf{Pa}=\mathbf{0}\},\end{aligned} \tag{3.13}$$

and the following

Theorem 3.5.11 *Let $\mathcal{A}$ be any algebra with an idempotent $\mathbf{P}$. Then we have the **Peirce decomposition** of $\mathcal{A}$:*

Peirce decomposition

$$\mathcal{A} = \mathbf{P}\mathcal{A}\mathbf{P}\oplus_V \mathbf{P}\mathcal{L}(\mathbf{P})\oplus_V \mathcal{R}(\mathbf{P})\mathbf{P}\oplus_V \mathcal{I}(\mathbf{P}),$$

where $\oplus_V$ indicates a vector space direct sum, and each factor is a subalgebra.

Proof By Eq. (3.13), each summand is actually an algebra. Furthermore, it is not hard to show that the only vector common to any two of the summands is the zero vector. Thus the sum is indeed a direct sum of subspaces. Next note that for any $\mathbf{a}\in\mathcal{A}$,

$$\mathbf{a} = \mathbf{PaP} + \mathbf{P}\underbrace{(\mathbf{a}-\mathbf{aP})}_{\in\mathcal{L}(\mathbf{P})} + \underbrace{(\mathbf{a}-\mathbf{Pa})}_{\in\mathcal{R}(\mathbf{P})}\mathbf{P} + \underbrace{(\mathbf{a}-\mathbf{Pa}-\mathbf{aP}+\mathbf{PaP})}_{\in\mathcal{I}(\mathbf{P})}$$

Problem 3.33 provides the details of the proof. □

Definition 3.5.12 An element $\mathbf{a}\in\mathcal{A}$ is **orthogonal** to an idempotent $\mathbf{P}$ if $\mathbf{aP}=\mathbf{Pa}=\mathbf{0}$. Thus $\mathcal{I}(\mathbf{P})$ houses such elements. An idempotent $\mathbf{P}$ is called **principal** if $\mathcal{I}(\mathbf{P})$ contains no idempotent.

principal idempotent and elements orthogonal to an idempotent

Let $\mathbf{P}_0$ be an idempotent. If it is not principal, then $\mathcal{I}(\mathbf{P}_0)$ contains an idempotent $\mathbf{q}$. Let $\mathbf{P}_1=\mathbf{P}_0+\mathbf{q}$. Then using the fact that $\mathbf{P}_0\mathbf{q}=\mathbf{qP}_0=\mathbf{0}$, we can show that $\mathbf{P}_1$ is an idempotent and that

$$\mathbf{P}_1\mathbf{P}_0=\mathbf{P}_0\mathbf{P}_1=\mathbf{P}_0 \quad\text{and}\quad \mathbf{P}_1\mathbf{q}=\mathbf{qP}_1=\mathbf{q}. \tag{3.14}$$

If $\mathbf{x}\in\mathcal{I}(\mathbf{P}_1)$, then $\mathbf{xP}_1=\mathbf{P}_1\mathbf{x}=\mathbf{0}$, and the first equation in (3.14) gives $\mathbf{xP}_0=\mathbf{P}_0\mathbf{x}=\mathbf{0}$, i.e., $\mathbf{x}\in\mathcal{I}(\mathbf{P}_0)$, demonstrating that $\mathcal{I}(\mathbf{P}_1)\subseteq\mathcal{I}(\mathbf{P}_0)$. Since $\mathbf{q}\in\mathcal{I}(\mathbf{P}_0)$, but $\mathbf{q}\notin\mathcal{I}(\mathbf{P}_1)$, $\mathcal{I}(\mathbf{P}_1)$ is a proper subset of $\mathcal{I}(\mathbf{P}_0)$. If $\mathcal{I}(\mathbf{P}_1)$ is not principal, then $\mathcal{I}(\mathbf{P}_1)$ contains an idempotent $\mathbf{r}$. Let $\mathbf{P}_2=\mathbf{P}_1+\mathbf{r}$. Then $\mathbf{P}_2$ is an idempotent and, as before, $\mathcal{I}(\mathbf{P}_2)$ is a proper subset of $\mathcal{I}(\mathbf{P}_1)$. We continue this process and obtain

$$\mathcal{I}(\mathbf{P}_0)\supset\mathcal{I}(\mathbf{P}_1)\supset\mathcal{I}(\mathbf{P}_2)\supset\cdots\supset\mathcal{I}(\mathbf{P}_k)\supset\cdots.$$

However, we cannot continue this chain indefinitely, because $\mathcal{I}(\mathbf{P}_0)$ has finite dimension. This means that there is a positive integer n such that $\mathcal{I}(\mathbf{P}_n)$ has no idempotent, i.e., $\mathbf{P}_n$ is principal. We have just proved

Proposition 3.5.13 *Every algebra that is not nilpotent has a principal idempotent.*

primitive idempotent

Definition 3.5.14 An idempotent is **primitive** if it is not the sum of two orthogonal idempotents.

Proposition 3.5.15 $\mathbf{P}$ *is primitive if and only if it is the only idempotent of* $\mathbf{P}\mathcal{A}\mathbf{P}$.

Proof Suppose that $\mathbf{P}$ is not primitive. Then there are orthogonal idempotents $\mathbf{P}_1$ and $\mathbf{P}_2$ such that $\mathbf{P} = \mathbf{P}_1 + \mathbf{P}_2$. It is easy to show that $\mathbf{P}\mathbf{P}_i = \mathbf{P}_i\mathbf{P} = \mathbf{P}_i$ for $i = 1, 2$. Hence, by the first equation in (3.13), $\mathbf{P}_i \in \mathbf{P}\mathcal{A}\mathbf{P}$, and $\mathbf{P}$ is not the only idempotent of $\mathbf{P}\mathcal{A}\mathbf{P}$.

Conversely, suppose that $\mathbf{P}$ is not the only idempotent in $\mathbf{P}\mathcal{A}\mathbf{P}$, so that $\mathbf{P}\mathcal{A}\mathbf{P}$ contains another idempotent, say $\mathbf{P}'$. Then by the first equation in (3.13), $\mathbf{P}\mathbf{P}' = \mathbf{P}'\mathbf{P} = \mathbf{P}'$. This shows that

$$(\mathbf{P} - \mathbf{P}')\mathbf{P}' = \mathbf{P}'(\mathbf{P} - \mathbf{P}') = \mathbf{0} \quad \text{and} \quad (\mathbf{P} - \mathbf{P}')\mathbf{P} = \mathbf{P}(\mathbf{P} - \mathbf{P}') = \mathbf{P} - \mathbf{P}',$$

i.e., that $(\mathbf{P} - \mathbf{P}') \in \mathbf{P}\mathcal{A}\mathbf{P}$ and it is orthogonal to $\mathbf{P}'$. Furthermore, $\mathbf{P} = (\mathbf{P} - \mathbf{P}') + \mathbf{P}'$, i.e., $\mathbf{P}$ is the sum of two primitive idempotents, and thus not primitive. □

Let $\mathbf{P}$ be an idempotent that is not primitive. Write $\mathbf{P} = \mathbf{P}_1 + \mathbf{Q}$, with $\mathbf{P}_1$ and $\mathbf{Q}$ orthogonal. If either of the two, say $\mathbf{Q}$, is not primitive, write it as $\mathbf{Q} = \mathbf{P}_2 + \mathbf{P}_3$, with $\mathbf{P}_2$ and $\mathbf{P}_3$ orthogonal. By Problem 3.34, the set $\{\mathbf{P}_i\}_{i=1}^3$ are mutually orthogonal idempotents and $\mathbf{P} = \mathbf{P}_1 + \mathbf{P}_2 + \mathbf{P}_3$. We can continue this process until all $\mathbf{P}_i$s are primitive. Therefore, we have

Theorem 3.5.16 *Every idempotent of an algebra* $\mathcal{A}$ *can be expressed as the sum of a finite number of mutually orthogonal primitive idempotents.*

3.5.2 Semi-simple Algebras

semi-simple algebras

Algebras which have no nilpotent ideals play an important role in the classification of algebras.

Definition 3.5.17 An algebra whose radical is zero is called **semi-simple**.

Since $\text{Rad}(\mathcal{A})$ contains all nilpotent left, right, and two-sided ideals of an algebra, if $\mathcal{A}$ is semi-simple, it can have no nilpotent left, right, or two-sided ideals.

Proposition 3.5.18 *A simple algebra is semi-simple.*

Proof If the simple algebra $\mathcal{A}$ is not semi-simple, then it has a nilpotent ideal. Since the only ideal is $\mathcal{A}$ itself, we must show that $\mathcal{A}$ is not nilpotent. Assume otherwise, and note that $\mathcal{A}^2$ is a *proper* ideal of $\mathcal{A}$, because if $\mathcal{A}^2 = \mathcal{A}$, then $\mathcal{A}^k = \mathcal{A}$ for any k. This contradicts our assumption that $\mathcal{A}$ is nilpotent. Since the only ideals of $\mathcal{A}$ are $\mathcal{A}$ and $\{\mathbf{0}\}$, we must have $\mathcal{A}^2 = \{\mathbf{0}\}$. It then follows that any proper subspace of $\mathcal{A}$ is trivially a nonzero proper ideal of $\mathcal{A}$, which cannot happen because of the simplicity of $\mathcal{A}$. □

Lemma 3.5.19 *If $\mathcal{A}$ is semi-simple and $\mathbf{P}$ is any principal idempotent in $\mathcal{A}$, then $\mathcal{A} = \mathbf{P}\mathcal{A}\mathbf{P}$.*

Proof Since $\mathcal{A}$ is not nilpotent, it has a principal idempotent $\mathbf{P}$ by Proposition 3.5.13. Since $\mathbf{P}$ is principal, $\mathcal{I}(\mathbf{P})$ of Theorem 3.5.11 contains no idempotent and by Proposition 3.5.10 must be nilpotent. Since $\mathcal{A}$ has no nilpotent ideal, $\mathcal{I}(\mathbf{P}) = \{\mathbf{0}\}$. Now note that $\mathcal{R}(\mathbf{P})\mathcal{L}(\mathbf{P})$ of Theorem 3.5.11 consists of all elements annihilated by both the right and left multiplication by $\mathbf{P}$. Therefore, $\mathcal{R}(\mathbf{P})\mathcal{L}(\mathbf{P})$ is a subset of $\mathcal{I}(\mathbf{P})$. Hence, $\mathcal{R}(\mathbf{P})\mathcal{L}(\mathbf{P}) = \{\mathbf{0}\}$. This shows that if $\mathbf{r} \in \mathcal{R}(\mathbf{P})$ and $\mathbf{l} \in \mathcal{L}(\mathbf{P})$, then $\mathbf{rl} = \mathbf{0}$. On the other hand, for any $\mathbf{l} \in \mathcal{L}(\mathbf{P})$ and $\mathbf{r} \in \mathcal{R}(\mathbf{P})$, we have

$$(\mathbf{lr})^2 = \mathbf{l}\underbrace{(\mathbf{rl})}_{=\mathbf{0}}\mathbf{r} = \mathbf{0}.$$

It follows that the ideal $\mathcal{L}(\mathbf{P})\mathcal{R}(\mathbf{P})$ (see Problem 3.10) is nil of index 2, and by Theorem 3.5.3, it is nilpotent. The semi-simplicity of $\mathcal{A}$ implies that $\mathcal{L}(\mathbf{P})\mathcal{R}(\mathbf{P}) = \{\mathbf{0}\}$. Multiplying the Peirce decomposition on the left by $\mathcal{L}(\mathbf{P})$, and using these results and the fact that $\mathcal{L}(\mathbf{P})\mathbf{P} = \{\mathbf{0}\}$, we obtain

$$\mathcal{L}(\mathbf{P})\mathcal{A} = \mathcal{L}(\mathbf{P})\mathcal{R}(\mathbf{P})\mathbf{P} = \{\mathbf{0}\}.$$

In particular $\mathcal{L}(\mathbf{P})\mathcal{L}(\mathbf{P}) = \{\mathbf{0}\}$, and thus $\mathcal{L}(\mathbf{P})$ is nilpotent, hence zero. Similarly, $\mathcal{R}(\mathbf{P})$ is also zero. Therefore, the Peirce decomposition of $\mathcal{A}$ reduces to the first term. □

Theorem 3.5.20 *A semi-simple algebra $\mathcal{A}$ is necessarily unital. Furthermore, the unit is the only principal idempotent of $\mathcal{A}$.*

semi-simple algebras are unital

Proof Let $\mathbf{P}$ be a principal idempotent of $\mathcal{A}$. If $\mathbf{b} \in \mathcal{A}$, then by Lemma 3.5.19 $\mathbf{b} \in \mathbf{P}\mathcal{A}\mathbf{P}$, and $\mathbf{b} = \mathbf{PaP}$ for some $\mathbf{a} \in \mathcal{A}$. Therefore,

$$\mathbf{Pb} = \mathbf{P}^2\mathbf{aP} = \mathbf{PaP} = \mathbf{b}$$

$$\mathbf{bP} = \mathbf{PaP}^2 = \mathbf{PaP} = \mathbf{b}.$$

Since this holds for all $\mathbf{b} \in \mathcal{A}$, we conclude that $\mathbf{P}$ is the identity of $\mathcal{A}$. □

Idempotents preserve the semi-simplicity of algebras in the following sense:

Proposition 3.5.21 *If $\mathcal{A}$ is semi-simple, then $\mathbf{P}\mathcal{A}\mathbf{P}$ is also semi-simple for any idempotent $\mathbf{P} \in \mathcal{A}$.*

Proof Let $\mathcal{N} = \text{Rad}(\mathbf{P}\mathcal{A}\mathbf{P})$ and $\mathbf{x} \in \mathcal{N} \subset \mathbf{P}\mathcal{A}\mathbf{P}$. Construct the left ideal $\mathcal{A}\mathbf{x}$ in $\mathcal{A}$ and note that by Eq. (3.13), $\mathbf{xP} = \mathbf{Px} = \mathbf{x}$. Then we have the following set identities:

$$\begin{aligned}(\mathcal{A}\mathbf{x})^{\nu+1} &= \mathcal{A}\mathbf{x}\mathcal{A}\mathbf{x}\ldots\mathcal{A}\mathbf{x}\mathcal{A}\mathbf{x} = \mathcal{A}\mathbf{x}\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x}\ldots\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x}\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x} \\ &= \mathcal{A}\mathbf{x}(\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x})^{\nu}.\end{aligned}$$

Since $\mathcal{N}$ is an ideal in $\mathbf{P}\mathcal{A}\mathbf{P}$, we have $\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x} \subset \mathcal{N}$, and if ν is the index of $\mathcal{N}$, then $(\mathbf{P}\mathcal{A}\mathbf{P}\mathbf{x})^{\nu} = \{\mathbf{0}\}$. Thus, $\mathcal{A}\mathbf{x}$ is nilpotent. Since $\mathcal{A}$ is semi-simple, we must have $\mathcal{A}\mathbf{x} = \{\mathbf{0}\}$. Thus, for any nonzero $\mathbf{a} \in \mathcal{A}$, $\mathbf{ax} = \mathbf{0}$. In particular, $\mathbf{Px} = \mathbf{x} = \mathbf{0}$. Since $\mathbf{x}$ was an arbitrary element of $\text{Rad}(\mathbf{P}\mathcal{A}\mathbf{P})$, we must have $\text{Rad}(\mathbf{P}\mathcal{A}\mathbf{P}) = \{\mathbf{0}\}$. Hence, $\mathbf{P}\mathcal{A}\mathbf{P}$ is semi-simple. □

Proposition 3.5.22 *Let $\mathcal{A}$ be a semi-simple algebra and $\mathbf{P}$ an idempotent in $\mathcal{A}$. Then $\mathbf{P}\mathcal{A}\mathbf{P}$ is a division algebra if and only if $\mathbf{P}$ is primitive.*

Proof Suppose that $\mathbf{P}\mathcal{A}\mathbf{P}$ is a division algebra. By Proposition 3.5.2, identity is the only idempotent of $\mathbf{P}\mathcal{A}\mathbf{P}$. But $\mathbf{P}$ is the identity of $\mathbf{P}\mathcal{A}\mathbf{P}$. Hence, $\mathbf{P}$ is the only idempotent of $\mathbf{P}\mathcal{A}\mathbf{P}$, and by Proposition 3.5.15 $\mathbf{P}$ is primitive.

Conversely, assume that $\mathbf{P}$ is primitive. Let $\mathbf{x} \in \mathbf{P}\mathcal{A}\mathbf{P}$ be nonzero. The left ideal $\mathcal{L} \equiv (\mathbf{P}\mathcal{A}\mathbf{P})\mathbf{x}$ cannot be nilpotent because $\mathbf{P}\mathcal{A}\mathbf{P}$ is semi-simple by Proposition 3.5.21. Hence, it must contain an idempotent by Proposition 3.5.13. But an idempotent in $\mathcal{L}$ is an idempotent in $\mathbf{P}\mathcal{A}\mathbf{P}$. Proposition 3.5.15 identifies $\mathbf{P}$ as the sole idempotent in $\mathbf{P}\mathcal{A}\mathbf{P}$, and thus, in $\mathcal{L}$. As an element of $\mathcal{L}$, we can write $\mathbf{P}$ as $\mathbf{P} = \mathbf{ax}$ with $\mathbf{a} \in \mathbf{P}\mathcal{A}\mathbf{P}$. Since, $\mathbf{P}$ is the identity in $\mathbf{P}\mathcal{A}\mathbf{P}$, $\mathbf{x}$ has an inverse. It follows that any element in $\mathbf{P}\mathcal{A}\mathbf{P}$ has an inverse. Thus it is a division algebra. □

It is intuitively obvious that a simple algebra is somehow more fundamental than a semi-simple algebra. We have seen that a simple algebra is semi-simple. But the converse is of course not true. If simple algebras are more fundamental, then semi-simple algebras should be "built up" from simple ones. To see this we first need some preliminaries.

Lemma 3.5.23 *If $\mathcal{A}$ has an ideal $\mathcal{B}$ with unit $\mathbf{1}_B$, then $\mathcal{A} = \mathcal{B} \oplus \mathcal{I}(\mathbf{1}_B)$, where $\mathcal{I}(\mathbf{1}_B)$ is the ideal in the Peirce decomposition of $\mathcal{A}$.*

Proof Since $\mathbf{1}_B$ is an idempotent[8] of $\mathcal{A}$, we can write the following Peirce decomposition:

$$\mathcal{A} = \mathbf{1}_B\mathcal{A}\mathbf{1}_B \oplus_V \mathbf{1}_B\mathcal{L}(\mathbf{1}_B) \oplus_V \mathcal{R}(\mathbf{1}_B)\mathbf{1}_B \oplus_V \mathcal{I}(\mathbf{1}_B) \equiv \mathcal{S}(\mathbf{1}_B) \oplus_V \mathcal{I}(\mathbf{1}_B)$$

[8]Note that $\mathbf{1}_B$ is *not* the identity of $\mathcal{A}$. It satisfies $\mathbf{x}\mathbf{1}_B = \mathbf{1}_B\mathbf{x} = \mathbf{x}$ only if $\mathbf{x} \in \mathcal{B}$.

where $\mathcal{S}(\mathbf{1}_B) = \mathbf{1}_B\mathcal{A}\mathbf{1}_B \oplus_V \mathbf{1}_B\mathcal{L}(\mathbf{1}_B) \oplus_V \mathcal{R}(\mathbf{1}_B)\mathbf{1}_B$. Since, $\mathcal{B}$ is an ideal, each component of $\mathcal{S}(\mathbf{1}_B)$ is a subset of $\mathcal{B}$, and therefore, $\mathcal{S}(\mathbf{1}_B) \subseteq \mathcal{B}$. If $\mathbf{b} \in \mathcal{B}$, then $\mathbf{b} \in \mathcal{A}$, and by the above decomposition, $\mathbf{b} = \mathbf{b}_1 + \mathbf{b}_2$, with $\mathbf{b}_1 \in \mathcal{S}(\mathbf{1}_B)$ and $\mathbf{b}_2 \in \mathcal{I}(\mathbf{1}_B)$. Multiplying both sides by $\mathbf{1}_B$, we get

$$\mathbf{b}\mathbf{1}_B = \mathbf{b}_1\mathbf{1}_B + \mathbf{b}_2\mathbf{1}_B \quad \text{or} \quad \mathbf{b} = \mathbf{b}_1$$

because $\mathbf{1}_B$ is the identity in $\mathcal{B}$ and $\mathcal{I}(\mathbf{1}_B)$ is orthogonal to $\mathbf{1}_B$. It follows that $\mathbf{b} \in \mathcal{S}(\mathbf{1}_B)$ and, therefore, $\mathcal{B} \subseteq \mathcal{S}(\mathbf{1}_B)$. Hence, $\mathcal{B} = \mathcal{S}(\mathbf{1}_B)$ and $\mathcal{A} = \mathcal{B} \oplus_V \mathcal{I}(\mathbf{1}_B)$. Since $\mathcal{I}(\mathbf{1}_B)\mathcal{B} = \mathcal{B}\mathcal{I}(\mathbf{1}_B) = \{\mathbf{0}\}$, we can change $\oplus_V$ to $\oplus$. □

Lemma 3.5.24 *A nonzero ideal of a semi-simple algebra is semi-simple.*

Proof Let $\mathcal{A}$ be a semi-simple algebra and $\mathcal{B}$ be a nonzero ideal of $\mathcal{A}$. Then $\mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B} \subset \mathrm{Rad}(\mathcal{B})$ because $\mathrm{Rad}(\mathcal{B})$ is an ideal in $\mathcal{B}$. Furthermore, since $\mathcal{B}$ is an ideal in $\mathcal{A}$, $\mathcal{A}\mathcal{B} \subset \mathcal{B}$ and $\mathcal{B}\mathcal{A} \subset \mathcal{B}$. It follow that $\mathcal{A}(\mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B})\mathcal{A} = (\mathcal{A}\mathcal{B})\,\mathrm{Rad}(\mathcal{B})(\mathcal{B}\mathcal{A}) \subset \mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B}$, i.e., that $\mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B}$ is an ideal in $\mathcal{A}$. Furthermore, it is nilpotent because it is contained in $\mathrm{Rad}(\mathcal{B})$. Semi-simplicity of $\mathcal{A}$ implies that $\mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B} = \{\mathbf{0}\}$. Since $\mathrm{Rad}(\mathcal{B}) \subset \mathcal{B}$, $\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A} \subset \mathcal{B}$, and $\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A} \subset \mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B}$. Now note that

$$\begin{aligned}\big(\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\big)^3 &= \mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\\ &\subset \mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}\\ &\subset \mathcal{B}\,\mathrm{Rad}(\mathcal{B})\mathcal{B} = \{\mathbf{0}\},\end{aligned}$$

indicating that $\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A}$ is nilpotent. Since it is an ideal in $\mathcal{A}$, and $\mathcal{A}$ is semi-simple, $\mathcal{A}\,\mathrm{Rad}(\mathcal{B})\mathcal{A} = \{\mathbf{0}\}$, and since $\mathcal{A}$ has an identity by Theorem 3.5.20, $\mathrm{Rad}(\mathcal{B}) = \{\mathbf{0}\}$, and $\mathcal{B}$ is semi-simple. □

Theorem 3.5.25 *An algebra is semi-simple iff it is the direct sum of simple algebras.*

Proof If the algebra $\mathcal{A}$ is the direct sum of simple algebras, then by Proposition 3.2.11, the only ideals of $\mathcal{A}$ are either direct sums of the components or contained in them. In either case, these ideals cannot be nilpotent because a simple algebra is semi-simple. Therefore, $\mathcal{A}$ is semi-simple.

Conversely, assume that $\mathcal{A}$ is semi-simple. If it has no proper ideal, then it is simple and therefore semi-simple, and we are done. So, suppose $\mathcal{B}$ is a proper nonzero ideal of $\mathcal{A}$. By Lemma 3.5.24 $\mathcal{B}$ is semi-simple, and by Theorem 3.5.20 $\mathcal{B}$ has a unit $\mathbf{1}_B$. Invoking Lemma 3.5.23, we can write $\mathcal{A} = \mathcal{B} \oplus \mathcal{I}(\mathbf{1}_B)$. If either of the two components is not simple, we continue the process. □

Theorem 3.5.26 *The reduction of a semi-simple algebra to simple subalgebras is unique up to an ordering of the components.*

Proof Let $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$ with $\mathcal{A}_i$ simple. The unit of $\mathcal{A}$ is a sum of the units of the components: $\mathbf{1} = \mathbf{1}_1 + \cdots + \mathbf{1}_r$. Let $\mathcal{A} = \mathcal{A}'_1 \oplus \cdots \oplus \mathcal{A}'_s$ be another reduction. Multiply both sides of the identity decomposition on the left by $\mathcal{A}'_j$ to obtain

$$\mathcal{A}'_j = \mathcal{A}'_j\mathbf{1}_1 + \cdots + \mathcal{A}'_j\mathbf{1}_r \equiv \mathcal{A}'_{j1} + \cdots + \mathcal{A}'_{jr} = \sum_{i=1}^{r} \mathcal{A}'_{ji}.$$

Since $\mathbf{1}_i \in \mathcal{A}_i$, and $\mathcal{A}_i$ is an ideal of $\mathcal{A}$, $\mathcal{A}'_{ji} \subset \mathcal{A}_i$. Since $\mathcal{A}_i$ are disjoint, $\mathcal{A}'_{ji}$ are disjoint. Since $\mathcal{A}'_j$ is an ideal, $\mathcal{A}'_j\mathbf{1}_i$ is an algebra as can be easily verified. Furthermore, since $\mathbf{1}_i\mathbf{1}_k = \mathbf{0}$ for $i \neq k$, the sum is a direct sum of algebras. Hence, by Proposition 3.2.11, $\mathcal{A}'_{ji}$ is an ideal, and since it is a subset of $\mathcal{A}_i$, it is a subideal of $\mathcal{A}_i$. The simplicity of $\mathcal{A}_i$ implies that $\mathcal{A}'_{ji} = \mathcal{A}_i$ or $\mathcal{A}'_{ji} = \{\mathbf{0}\}$. Since $\mathcal{A}'_j$ is simple, only one of its components is nonzero, and it is one of the $\mathcal{A}_i$. □

3.5.3 Classification of Simple Algebras

Wedderburn principal structure theorem
Wedderburn decomposition theorem

Theorems 3.5.25 and 3.5.26 classify all the semi-simple algebras, i.e., algebras with zero radicals, in terms of simple algebras. Can a general algebra be written as its radical and a semi-simple algebra? It turns out that an algebra $\mathcal{A}$ with nonzero radical $\mathrm{Rad}(\mathcal{A})$ is the direct sum $\mathcal{A} = \mathrm{Rad}(\mathcal{A}) \oplus (\mathcal{A}/\mathrm{Rad}(\mathcal{A}))$, i.e., the radical plus the factor algebra modulo the radical. Since, in $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$, the radical has been "factored out" of $\mathcal{A}$, the quotient is indeed semi-simple. This result is known as **Wedderburn principal structure theorem**, and reduces the study of all algebras to that of simple algebras. Simple algebras can be further decomposed (for a proof, see [Benn 87, pp. 330–332]):

Theorem 3.5.27 (Wedderburn decomposition) *An algebra $\mathcal{A}$ is simple if and only if*

$$\mathcal{A} \cong \mathcal{D} \otimes \mathcal{M}_n \cong \mathcal{M}_n(\mathcal{D}),$$

where $\mathcal{D}$ is a division algebra and $\mathcal{M}_n(\mathcal{D})$ is a total matrix algebra over $\mathcal{D}$ for some non-negative integer n. $\mathcal{D}$ and $\mathcal{M}_n(\mathcal{D})$ are unique up to a similarity transformation.

Denote by $\mathcal{Z}_n$ the center of $\mathcal{M}_n$. Since $\mathcal{M}_n$ is central, by Theorem 3.3.2, $\mathcal{Z}_n = \mathrm{Span}\{\mathbf{1}_n\}$. On the other hand, Eq. (3.8) gives

$$\mathcal{Z}(\mathcal{A}) = \mathcal{Z}(\mathcal{D}) \otimes \mathcal{Z}_n \cong \mathcal{Z}(\mathcal{D}), \tag{3.15}$$

which is a relation that determines $\mathcal{D}$ from a knowledge of the center of the algebra $\mathcal{A}$.

Proposition 3.5.28 *The only division algebra over $\mathbb{C}$ is $\mathbb{C}$ itself.*

Proof Let $\mathcal{D}$ be a division algebra over $\mathbb{C}$ and $\mathbf{x}$ a nonzero element of $\mathcal{D}$. Since $\mathcal{D}$ is finite-dimensional, there must exist a polynomial in $\mathbf{x}$ such that (why?)

$$f(\mathbf{x}) = \mathbf{x}^n + \alpha_{n-1}\mathbf{x}^{n-1} + \cdots + \alpha_1\mathbf{x} + \alpha_0\mathbf{1} = \mathbf{0}.$$

Let n be the smallest integer such that this holds. By the fundamental theorem of algebra (see Sect. 10.5), $f(\mathbf{x})$ has at least one root λ. Then we have

$$f(\mathbf{x}) = (\mathbf{x} - \lambda\mathbf{1})g(\mathbf{x}) = \mathbf{0}.$$

Now, $g(\mathbf{x})$ has degree at most $n-1$ and by assumption cannot be zero. Hence, it has an inverse because $\mathcal{D}$ is a division algebra. Therefore, $\mathbf{x} - \lambda\mathbf{1} = \mathbf{0}$, and every element of $\mathcal{D}$ is a multiple of $\mathbf{1}$. This completes the proof. □

Proposition 3.5.28 and Theorem 3.5.27, plus the fact that $\mathcal{M}_n(\mathbb{C})$ is central (Theorem 3.3.2) give the following:

Theorem 3.5.29 *Any simple algebra $\mathcal{A}$ over $\mathbb{C}$ is isomorphic to $\mathcal{M}_n(\mathbb{C})$ for some n, and therefore $\mathcal{A}$ is necessarily central simple.*

The centrality of a complex algebra can also be deduced from Eq. (3.15) and Proposition 3.5.28.

There is a theorem in abstract algebra, called the **Frobenius Theorem**, which states that the only division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$, and since the tensor product of two division algebras is a division algebra, also $\mathbb{C} \otimes \mathbb{H}$.[9] Furthermore, the center of $\mathbb{C}$ is the entire $\mathbb{C}$, because it is a commutative algebra. On the other hand, $\mathbb{H}$ is central, i.e., its center is the span of its identity (reader, please verify), therefore, isomorphic to $\mathbb{R}$.

Frobenius Theorem

Now consider a simple algebra $\mathcal{A}$ over $\mathbb{R}$. If $\mathcal{A}$ is central, i.e., if $\mathcal{Z}(\mathcal{A}) = \mathbb{R}$, then Eq. (3.15) yields

$$\mathbb{R} \cong \mathcal{Z}(\mathcal{D}) \quad \Rightarrow \quad \mathcal{D} = \mathbb{R} \text{ or } \mathbb{H}.$$

If $\mathcal{Z}(\mathcal{A}) = \mathbb{C}$, then

$$\mathbb{C} \cong \mathcal{Z}(\mathcal{D}) \quad \Rightarrow \quad \mathcal{D} = \mathbb{C} \text{ or } \mathbb{C} \otimes \mathbb{H}.$$

These results, plus the theorems of Frobenius and Wedderburn yield

[9] Since $\mathbb{C}$ is a subalgebra of $\mathbb{H}$, the tensor product is actually redundant. However, in the classification of the Clifford algebras discussed later in the book, $\mathbb{C}$ is sometimes explicitly factored out.

Theorem 3.5.30 *Any simple algebra $\mathcal{A}$ over $\mathbb{R}$ is isomorphic to $\mathcal{D} \otimes \mathcal{M}_n$ for some n. If the center of $\mathcal{A}$ is isomorphic to $\mathbb{C}$, then $\mathcal{D}$ is either $\mathbb{C}$ or $\mathbb{C} \otimes \mathbb{H}$. If $\mathcal{A}$ is central (i.e., its center is isomorphic to $\mathbb{R}$), then $\mathcal{D}$ is $\mathbb{R}$ or $\mathbb{H}$.*

We conclude our discussion of the decomposition of an algebra by a further characterization of a simple algebra and the connection between primitive idempotents andminimal left ideals.

similar idempotents

Definition 3.5.31 Two idempotents $\mathbf{P}$ and $\mathbf{P}'$ of an algebra $\mathcal{A}$ are called **similar** if there exists an invertible element $\mathbf{s} \in \mathcal{A}$ such that $\mathbf{P}' = \mathbf{s}\mathbf{P}\mathbf{s}^{-1}$.

The proof of the following theorem can be found in [Benn 87, pp. 332–334]:

rank of an idempotent of a simple algebra

Theorem 3.5.32 *If $\mathbf{P}$ is an idempotent of a simple algebra $\mathcal{A}$, then there exist mutually orthogonal primitive idempotents $\{\mathbf{P}_i\}_{i=1}^r$ such that $\mathbf{P} = \sum_{i=1}^r \mathbf{P}_i$. The integer r is unique and is called the **rank** of $\mathbf{P}$. Two idempotents are similar if and only if they have the same rank.*

Theorem 3.5.33 *Let $\mathbf{P}$ be a primitive idempotent of a semi-simple algebra $\mathcal{A}$. Then $\mathcal{A}\mathbf{P}$ (respectively $\mathbf{P}\mathcal{A}$) is a minimal left (respectively right) ideal of $\mathcal{A}$.*

Proof Since a semi-simple algebra is a direct sum of simple algebras each independent of the others, without loss of generality, we can assume that $\mathcal{A}$ is simple. Suppose $\mathcal{L} \equiv \mathcal{A}\mathbf{P}$ is not minimal. Then $\mathcal{L}$ contains a nonzero left ideal $\mathcal{L}_1$ of $\mathcal{A}$. Since $\mathcal{A}$ is (semi-)simple, $\mathcal{L}_1$ is not nilpotent. Hence by Proposition 3.5.10 it contains an idempotent $\mathbf{P}_1$. If $\mathbf{P}_1 = \mathbf{P}$, then

$$\mathcal{L} = \mathcal{A}\mathbf{P} = \mathcal{A}\mathbf{P}_1 \subseteq \mathcal{L}_1,$$

and therefore $\mathcal{L} = \mathcal{L}_1$, and we are done. So suppose that $\mathbf{P}_1 \neq \mathbf{P}$. Then, by Theorem 3.5.16

$$\mathbf{P}_1 = \mathbf{Q}_1 + \cdots + \mathbf{Q}_r,$$

where $\mathbf{Q}_i$ are all primitive and orthogonal to each other. Since $\mathbf{Q}_1$ and $\mathbf{P}$ have rank 1, by Theorem 3.5.32 they are similar, i.e., there exists an invertible element $\mathbf{s} \in \mathcal{A}$ such that $\mathbf{P} = \mathbf{s}\mathbf{Q}_1\mathbf{s}^{-1}$. So, by choosing $\mathbf{s}\mathbf{P}_1\mathbf{s}^{-1}$ instead of $\mathbf{P}_1$ if we have to,[10] we can assume that $\mathbf{Q}_1 = \mathbf{P}$. Then

$$\mathbf{P}_1 = \mathbf{P} + \mathbf{Q}_2 + \cdots + \mathbf{Q}_r,$$

[10] This is equivalent to replacing $\mathcal{L}$ with $\mathbf{s}\mathcal{L}\mathbf{s}^{-1}$, which is allowed by Theorem 3.2.7 and the non-uniqueness clause of Theorem 3.5.27.

and $\mathbf{P}$ is orthogonal to all the $\mathbf{Q}_i$. Multiplying both sides on the left by $\mathbf{P}$, we get $\mathbf{PP}_1 = \mathbf{P}$ and

$$\mathcal{L} = \mathcal{A}\mathbf{P} = \mathcal{A}\mathbf{P}\mathbf{P}_1 \subseteq \mathcal{L}_1,$$

implying that $\mathcal{L} = \mathcal{L}_1$. The case of a right ideal follows similarly. □

3.6 Polynomial Algebra

Let $\mathcal{A}$ be an associative algebra with identity $\mathbf{1}$. For any fixed element $\mathbf{a} \in \mathcal{A}$, consider the set $\mathcal{P}[\mathbf{a}]$ of elements of the algebra of the form

$$p(\mathbf{a}) \equiv \sum_{k=0}^{\infty} \alpha_k \mathbf{a}^k, \quad \alpha_k \in \mathbb{C},$$

in which only a finite number of the terms in the sum are nonzero. These are clearly polynomials in $\mathbf{a}$ for which addition and multiplication is defined as usual.

leading coefficient, monic, degree, monomial

Definition 3.6.1 Let $\mathcal{A}$ be an associative algebra with identity $\mathbf{1}$. For any fixed element $\mathbf{a} \in \mathcal{A}$, the set $\mathcal{P}[\mathbf{a}]$ is a commutative algebra with identity called the **polynomial algebra** generated by $\mathbf{a}$. The coefficient of the highest power of $\mathbf{a}$ in $p(\mathbf{a}) = \sum_{k=0}^{\infty} \alpha_k \mathbf{a}^k$ is called the **leading coefficient** of p, and α_0 is called the **scalar term**. A polynomial with leading coefficient 1 is called **monic**. The highest power of $\mathbf{a}$ in p is called the **degree** of p and denoted by $\deg p$. A nonzero polynomial of the form $\alpha_n \mathbf{a}^n$ is called a **monomial** of degree n.

It is clear that $\{\mathbf{a}^k\}_{k=0}^{\infty}$ is a basis of the polynomial algebra $\mathcal{P}[\mathbf{a}]$. If $p(\mathbf{a}) \equiv \sum_{k=0}^{\infty} \alpha_k \mathbf{a}^k$ and $q(\mathbf{a}) \equiv \sum_{j=0}^{\infty} \beta_j \mathbf{a}^j$, then

$$(p+q)(\mathbf{a}) = \sum_{k=0}^{\infty} (\alpha_k + \beta_k)\mathbf{a}^k,$$

$$(pq)(\mathbf{a}) = \sum_{i=0}^{\infty} \gamma_i \mathbf{a}^i, \quad \text{where } \gamma_i = \sum_{j+k=i} \alpha_k \beta_j.$$

Consider two nonzero polynomials $p(\mathbf{a})$ and $q(\mathbf{a})$. Then obviously

$$\begin{aligned} \deg(p+q) &\leq \max(\deg p, \deg q), \\ \deg(pq) &= \deg p + \deg q. \end{aligned} \tag{3.16}$$

differentiation map

Definition 3.6.2 The linear map $\mathbf{d} : \mathcal{P}[\mathbf{a}] \to \mathcal{P}[\mathbf{a}]$ defined by

$$\mathbf{d}\mathbf{a}^k = k\mathbf{a}^{k-1}, \quad k \geq 1$$

$$\mathbf{d}\mathbf{a}^0 \equiv \mathbf{d}\mathbf{1} = 0$$

is called the **differentiation map** in $\mathcal{P}[\mathbf{a}]$.

Theorem 3.6.3 *The differentiation map* $\mathbf{d}$ *is a derivation of* $\mathcal{P}[\mathbf{a}]$. *We denote* $\mathbf{d}(p)$ *by* p'.

Proof The simple proof is left as Problem 3.35. □

Let p and q be two polynomials. Then $\mathbf{d}(pq) = \mathbf{d}(p)q + p\mathbf{d}(q)$, and in particular

$$\mathbf{d}\big(q^2\big) = 2q\mathbf{d}(q),$$

and in general

$$\mathbf{d}\big(q^k\big) = kq^{k-1}\mathbf{d}(q), \quad k \geq 1 \quad \text{and} \quad \mathbf{d}\big(q^0\big) = 0.$$

Because q is an element of $\mathcal{A}$, it can generate a polynomial in itself. We can construct, for example $p(q)$, by replacing $\mathbf{a}$ with q:

$$p(q) = \sum_{k=0}^{\infty} \alpha_k q^k.$$

Then, it is straightforward to show that (see Problem 3.36)

$$\mathbf{d}\big(p(q)\big) = p'(q) \cdot q' \tag{3.17}$$

chain rule This is the **chain rule** for the differentiation of polynomials.

Definition 3.6.4 The polynomial $\mathbf{d}^r(p)$ is called the r**th derivative** of p and denoted by $p^{(r)}$. We extend the notation by defining $p^{(0)} = p$.

It is clear that $p^{(r)} = 0$ if $r > \deg(p)$.
Consider the monomial $\mathbf{a}^n$, and note that

$$\mathbf{d}^r\big(\mathbf{a}^n\big) = \frac{n!}{(n-r)!}\mathbf{a}^{n-r} \quad \text{or} \quad \mathbf{a}^{n-r} = \frac{(n-r)!}{n!}\mathbf{d}^r\big(\mathbf{a}^n\big).$$

Now use the binomial theorem to write

$$(\mathbf{a}+\mathbf{b})^n = \sum_{r=0}^{n} \binom{n}{r} \mathbf{a}^{n-r} \cdot \mathbf{b}^r = \sum_{r=0}^{n} \frac{1}{r!}\mathbf{d}^r\big(\mathbf{a}^n\big) \cdot \mathbf{b}^r.$$

The left-hand side is an arbitrary term of the polynomial $p(\mathbf{a}+\mathbf{b})$. There-
Taylor formula fore, taking linear combination of such terms, we have

$$p(\mathbf{a}+\mathbf{b}) = \sum_{r=0}^{n} \frac{p^{(r)}(\mathbf{a})}{r!} \cdot \mathbf{b}^r. \tag{3.18}$$

This is called the **Taylor formula** for p.

A root of the polynomial $p(\mathbf{a}) = \sum_{k=0}^{n} \eta_k \mathbf{a}^k$ of degree n is a scalar $\lambda \in \mathbb{C}$ such that $p(\lambda) = \sum_{k=0}^{n} \eta_k \lambda^k = 0$. The fundamental theorem of algebra[11] states that $\mathbb{C}$ is algebraically closed, meaning that any polynomial with coefficients in $\mathbb{C}$ can be factored out into a product of polynomials of degree

[11] A proof of the theorem can be found in Sect. 10.5.

one with coefficients in $\mathbb{C}$:

$\mathbb{C}$ is algebraically closed

$$p(\mathbf{a}) = \eta_n(\mathbf{a} - \lambda_1\mathbf{1})^{k_1} \dots (\mathbf{a} - \lambda_s\mathbf{1})^{k_s}, \tag{3.19}$$

where $\eta_n \neq 0$, $\{\lambda_i\}_{i=1}^s$ are the distinct complex roots of the polynomial, k_i, called the **multiplicity** of λ_i, is a nonnegative integer, and $\sum_{i=1}^s k_i = n$.

multiplicity of a root

As the simple example $p(\mathbf{a}) = \mathbf{a}^2 + \mathbf{1}$ suggests, $\mathbb{R}$ is not algebraically closed. Nevertheless, a real polynomial can still be factored out into products of polynomials of degree 1 and 2 with real coefficients. To show this, first note that if λ is a complex root of a real polynomial, then its complex conjugate $\bar{\lambda}$ is also a root. This follows from taking the complex conjugate of $\sum_{k=0}^n \eta_k \lambda^k = 0$ and noting that $\bar{\eta}_k = \eta_k$ for real η_k. Furthermore, λ and $\bar{\lambda}$ must have the same multiplicity, otherwise the unmatched factors produce a polynomial with complex coefficients, which, when multiplied out with the rest of the factors, produce some complex coefficients for $p(\mathbf{a})$.

Next, multiply each factor in Eq. (3.19) containing a complex root by its complex conjugate. So, if $\lambda_m = \gamma_m + i\xi_m$, then

$$\begin{aligned}(\mathbf{a} - \lambda_m\mathbf{1})^{k_m}(\mathbf{a} - \bar{\lambda}_m\mathbf{1})^{k_m} &= (\mathbf{a} - \gamma_m\mathbf{1} - i\xi_m\mathbf{1})^{k_m}(\mathbf{a} - \gamma_m\mathbf{1} + i\xi_m\mathbf{1})^{k_m} \\ &= \left(\mathbf{a}^2 - 2\gamma_m\mathbf{a} + \gamma_m^2\mathbf{1} + \xi_m^2\mathbf{1}\right)^{k_m} \\ &\equiv \left(\mathbf{a}^2 + \alpha_m\mathbf{a} + \beta_m\mathbf{1}\right)^{k_m}, \quad \alpha_m^2 < 4\beta_m.\end{aligned}$$

The inequality ensures that $\xi_m \neq 0$, i.e., that the root is not real. We have just proved the following:

Theorem 3.6.5 *A real polynomial* $p(\mathbf{a}) = \sum_{k=0}^n \eta_k \mathbf{a}^k$ *of degree* n *has the following factorization*:

$$p(\mathbf{a}) = \eta_n \prod_{i=1}^r (\mathbf{a} - \lambda_i\mathbf{1})^{k_i} \prod_{j=1}^R \left(\mathbf{a}^2 + \alpha_j\mathbf{a} + \beta_j\mathbf{1}\right)^{K_j}, \quad \alpha_j^2 < 4\beta_j,$$

where $\lambda_i, \alpha_j, \beta_j \in \mathbb{R}$, $k_i, K_j \in \mathbb{N}$, λ_i *are all distinct, the pairs* (α_j, β_j) *are all distinct, and* $2\sum_{j=1}^R K_j + \sum_{i=1}^r k_i = n$.

Corollary 3.6.6 *A real polynomial of odd degree has at least one real root.*

3.7 Problems

3.1 Show that

(a) the product on $\mathbb{R}^2$ defined by

$$(x_1, x_2)(y_1, y_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1)$$

turns $\mathbb{R}^2$ into an associative and commutative algebra, and

(b) the cross product on $\mathbb{R}^3$ turns it into a nonassociative, noncommutative algebra.

3.2 Show that the center of an algebra is a subspace of that algebra. If the algebra is associative, then its center is a subalgebra.

3.3 Prove that $\mathcal{A}^2$, the derived algebra of $\mathcal{A}$, is indeed an algebra.

3.4 Prove that the set $\mathcal{A}$ of $n \times n$ matrices, with the product defined by Eq. (3.3), form a nonassociative noncommutative algebra.

3.5 Prove that the set $\mathcal{A}$ of $n \times n$ upper triangular matrices, with the product defined by ordinary multiplication of matrices is an associative noncommutative algebra. Show that the same set with multiplication defined by Eq. (3.3), is a nonassociative noncommutative algebra, and that the derived algebra $\mathcal{A}^2 \equiv \mathcal{B}$ is the set of strictly upper triangular matrices. What is the derived algebra $\mathcal{B}^2$ of $\mathcal{B}$?

3.6 Prove Proposition 3.1.23.

3.7 Let $\omega \in \mathcal{L}(\mathcal{V})$ be defined by $\omega(\mathbf{a}) = -\mathbf{a}$ for all $\mathbf{a} \in \mathcal{V}$. Is ω an involution of $\mathcal{V}$? Now suppose that $\mathcal{V}$ is an *algebra*. Is ω so defined an involution of the algebra $\mathcal{V}$? Recall that an involution of an algebra must be a *homomorphism* of that algebra.

3.8 Show that no *proper* left (right) ideal of an algebra with identity can contain an element that has a left (right) inverse.

3.9 Let $\mathcal{A}$ be an associative algebra, and $\mathbf{x} \in \mathcal{A}$. Show that $\mathcal{A}\mathbf{x}$ is a left ideal, $\mathbf{x}\mathcal{A}$ is a right ideal, and $\mathcal{A}\mathbf{x}\mathcal{A}$ is a two-sided ideal.

3.10 Let $\mathcal{L}$ be a left ideal and $\mathcal{R}$ a right ideal. Show that $\mathcal{L}\mathcal{R}$ is a two-sided ideal.

3.11 Show that Φ of Theorem 3.1.25 is an algebra isomorphism.

3.12 Show that the linear transformation of Example 3.1.18 is an isomorphism of the two algebras $\mathcal{A}$ and $\mathcal{B}$.

3.13 Let $\mathcal{A}$ be an algebra with identity $\mathbf{1}_A$ and ϕ an epimorphism of $\mathcal{A}$ onto another algebra $\mathcal{B}$. Show that $\phi(\mathbf{1}_A)$ is the identity of $\mathcal{B}$.

3.14 Show that the derived algebra of $\mathcal{A}$ is an ideal in $\mathcal{A}$.

3.15 Show that the algebra of quaternions is central.

3.16 Write down all the structure constants for the algebra of quaternions. Show that this algebra is associative.

3.17 Show that a quaternion is pure iff its square is a nonpositive real number.

3.18 Let p and q be two quaternions. Show that

(a) $(pq)^* = q^* p^*$,
(b) $q \in \mathbb{R}$ iff $q^* = q$, and $q \in \mathbb{R}^3$ iff $q^* = -q$, and
(c) $qq^* = q^* q$ is a nonnegative real number.

3.19 Prove Eq. (3.7).

3.20 Show that $\bar{\phi}$ of Example 3.2.16 is an algebra homomorphism.

3.21 Prove Theorem 3.3.2.

3.22 The algebra $\mathcal{A}$ has a basis $\{\mathbf{1}, \mathbf{e}\}$ with $\mathbf{e}^2 = \mathbf{1}$.

(a) Show that $\{\mathbf{f}_1, \mathbf{f}_2\}$ with $\mathbf{f}_1 = \frac{1}{2}(\mathbf{1} + \mathbf{e})$ and $\mathbf{f}_2 = \frac{1}{2}(\mathbf{1} - \mathbf{e})$ is also a basis.
(b) Show that $\mathcal{A} = \mathcal{L}_1 \oplus_V \mathcal{L}_2$, where $\mathcal{L}_i = \mathcal{A}\mathbf{f}_i$, $i = 1, 2$ and $\oplus_V$ indicates a vector space direct sum.
(c) Show that $\mathcal{L}_1$ an $\mathcal{L}_2$ are actually two-sided ideals and that $\mathcal{L}_1\mathcal{L}_2 = \{\mathbf{0}\}$. Therefore, $\mathcal{A} = \mathcal{L}_1 \oplus \mathcal{L}_2$.
(d) Multiply an arbitrary element of $\mathcal{L}_i$, $i = 1, 2$, by an arbitrary element of $\mathcal{A}$ to show that $\mathcal{L}_i = \text{Span}\{\mathbf{f}_i\}$, $i = 1, 2$. Thus, $\mathcal{L}_i \cong \mathbb{R}$, $i = 1, 2$, or $\mathcal{A} = \mathbb{R} \oplus \mathbb{R}$.

3.23 If $\mathcal{A}$ is an algebra and $\mathbf{D}$ is a derivation in $\mathcal{A}$, prove that both the center $\mathcal{Z}(\mathcal{A})$ and the derived algebra $\mathcal{A}^2$ are stable under $\mathbf{D}$, i.e., if $\mathbf{a} \in \mathcal{Z}(\mathcal{A})$ then $\mathbf{D}(\mathbf{a}) \in \mathcal{Z}(\mathcal{A})$, and if $\mathbf{a} \in \mathcal{A}^2$ then $\mathbf{D}(\mathbf{a}) \in \mathcal{A}^2$.

3.24 Let $\mathbf{D} : \mathcal{A} \to \mathcal{A}$ be a derivation. Show that $\ker \mathbf{D}$ is a subalgebra of $\mathcal{A}$.

3.25 Show that a linear combination of two derivations is a derivation.

3.26 Fix a vector $\mathbf{a} \in \mathbb{R}^3$ and define the linear transformation $\mathbf{D}_\mathbf{a} : \mathbb{R}^3 \to \mathbb{R}^3$ by $\mathbf{D}_\mathbf{a}(\mathbf{b}) = \mathbf{a} \times \mathbf{b}$. Show that $\mathbf{D}_\mathbf{a}$ is a derivation of $\mathbb{R}^3$ with the cross product as multiplication.

3.27 Show that $\mathbf{D}$ defined on $\mathcal{C}^r(a, b)$ by $\mathbf{D}(f) = f'(c)$, where $a < c < b$, is a ϕ_c-derivation if ϕ_c is defined as the evaluation map $\phi_c(f) = f(c)$.

3.28 Let $\mathbf{\Omega} \in \text{End}(\mathcal{A})$ be an antiderivation of $\mathcal{A}$ with respect to ω. Show that $\ker \mathbf{\Omega}$ is a subalgebra of $\mathcal{A}$ and $\mathbf{\Omega}(\mathbf{e}) = \mathbf{0}$ if $\mathcal{A}$ has an identity.

3.29 Derive the Leibniz formula (3.11).

3.30 Prove Theorem 3.4.10.

3.31 Show that the algebra of the strictly upper triangular $n \times n$ matrices is nilpotent of index n.

3.32 Let $\mathbf{b}$ be a fixed element of an algebra $\mathcal{B}$. Consider the *linear* transformation $\mathbf{T}_b : \mathcal{B} \to \mathcal{B}$ given by $\mathbf{T}_b(\mathbf{x}) = \mathbf{xb}$. Using the dimension theorem, show that if $\mathcal{B}\mathbf{b} = \mathcal{B}$, then $\ker \mathbf{T}_b = \mathbf{0}$.

3.33 Let $\mathcal{A}$ be an algebra with an idempotent $\mathbf{P}$. Show that $\mathbf{P}\mathcal{A}\mathbf{P}$ consists of elements $\mathbf{a}$ such that $\mathbf{aP} = \mathbf{Pa} = \mathbf{a}$. For the subspaces of Theorem 3.5.11, let $\mathcal{A}_1 \equiv \mathbf{P}\mathcal{A}\mathbf{P}$, $\mathcal{A}_2 \equiv \mathbf{P}\mathcal{L}(\mathbf{P})$, $\mathcal{A}_3 \equiv \mathcal{R}(\mathbf{P})\mathbf{P}$, and $\mathcal{A}_4 \equiv \mathcal{I}(\mathbf{P})$. Show that $\{\mathcal{A}_i\}_{i=1}^3$ are subalgebras of $\mathcal{A}$ and that $\mathcal{A}_i \cap \mathcal{A}_j = \{\mathbf{0}\}$, but $\mathcal{A}_i\mathcal{A}_j \neq \{\mathbf{0}\}$ for all $i \neq j$, $i, j = 1, \ldots, 4$. Thus, Peirce decomposition is a vector space direct sum, but not an algebra direct sum.

3.34 Let $\mathbf{p}$ and $\mathbf{q}$ be orthogonal idempotents. Suppose that $\mathbf{q} = \mathbf{q}_1 + \mathbf{q}_2$, where $\mathbf{q}_1$ and $\mathbf{q}_2$ are orthogonal idempotents. Show that $\mathbf{qq}_i = \mathbf{q}_i\mathbf{q} = \mathbf{q}_i$ for $i = 1, 2$. Using this result, show that $\mathbf{pq}_i = \mathbf{q}_i\mathbf{p} = \mathbf{0}$ for $i = 1, 2$.

3.35 Use the basis $\{\mathbf{a}^k\}_{k=0}^{\infty}$ of $\mathcal{P}[\mathbf{a}]$ and apply Theorem 3.4.4 on it to show that the differentiation map of Definition 3.6.2 is a derivation.

3.36 Derive the chain rule (3.17).