2

Algebraic Structures

The main algebraic structure involved with the subject of this book is that of a "linear space" (or "vector space"). A linear space is a set endowed with an extra structure in addition to its set-theoretic structure (i.e., an extra structure that goes beyond the notions of inclusion, union, complement, function, and ordering, for instance). Roughly speaking, linear spaces are sets where two operations, called "addition" and "scalar multiplication", are properly defined so that we can refer to the "sum" of two points in a linear space, as well as to the "product" of a point in it by a "scalar". Although the reader is supposed to have already had a contact with linear algebra and, in particular, with "finite-dimensional vector spaces", we shall proceed from the very beginning. Our approach avoids the parochially "finite-dimensional" constructions (whenever this is possible), and focuses either on general results that do not depend on the "dimensionality" of the linear space, or on abstract "infinite-dimensional" linear spaces.

2.1 Linear Spaces

A *binary operation* on a set X is a mapping of $X\times X$ into X. If F is a function from $X\times X$ to X, then we generally write $z = F(x,y)$ to indicate that z in X is the value of F at the point (x,y) in $X\times X$. However, to emphasize the rule of the binary operation (the outcome of a binary operation on two points of X is again a point of X), it is convenient (and customary) to adopt a different notation. Moreover, in order to emphasize the abstract character of a binary operation, it is also common to use a noncommittal symbol to denote it. Thus, if $\star$ is a binary operation on X (so that $\star\colon X\times X \to X$), then we shall write $z = x\star y$ instead of $z = \star(x,y)$ to indicate that z in X is the value of $\star$ at the point (x,y) in $X\times X$. If a binary operation $\star$ on X has the property that

$$x\star(y\star z) = (x\star y)\star z$$

for every x, y, and z in X, then it is said to be *associative*. In this case we shall drop the parentheses and write $x\star y\star z$. If there exists an element e in X such that

C.S. Kubrusly, *The Elements of Operator Theory*, DOI 10.1007/978-0-8176-4998-2_2,

$$x \star e = e \star x = x$$

for every $x \in X$, then e is said to be the *neutral element* (or the *identity element*) with respect to the binary operation $\star$ on X. It is easy to show that, if a binary operation $\star$ has a neutral element e, then e is *unique*. If an associative binary operation $\star$ on X has a neutral element e in X, and if for some $x \in X$ there exists $x^{-1} \in X$ such that

$$x \star x^{-1} = x^{-1} \star x = e,$$

then x^{-1} is called the *inverse* of x with respect to $\star$. It is also easy to show that, if the inverse of x exists with respect to an associative binary operation $\star$, then it is *unique*. A *group* is a nonempty set X on which is defined a binary operation $\star$ such that

(a) $\star$ is associative,

(b) $\star$ has a neutral element in X, and

(c) every x in X has an inverse in X with respect to $\star$.

If a binary operation $\star$ on X has the property that

$$x \star y = y \star x$$

for every x and y in X, then it is said to be *commutative*. If X is a group with respect to a binary operation $\star$, and if

(d) $\star$ is commutative,

then X is said to be an *Abelian* (or *commutative*) *group*.

Example 2.A. Let X be a set with more than three elements. The collection of all injective mappings of X onto itself (i.e., the collection of all invertible mappings on X) is a non-Abelian group with respect to the composition operation $\circ$. The neutral element (or the identity element) of such a group is, of course, the identity map on X.

An *additive Abelian group* is an Abelian group X for which the underlying binary operation is interpreted as an *addition* and denoted by $+$ (instead of $\star$). In this case the element $x + y$ (which lies in X for every x and y in X) is called the *sum* of x and y. The (unique) neutral element with respect to addition is denoted by 0 (instead of e) and called *zero*. The (unique) inverse of x under addition is denoted by $-x$ (instead of x^{-1}) and is called the *negative* of x. Thus $x + 0 = 0 + x = x$ and $x + (-x) = (-x) + x = 0$ for every $x \in X$. Moreover, the operation of *subtraction* is defined by $x - y = x + (-y)$, and $x - y$ is called the *difference* between x and y.

If $\diamond \colon X \times X \to X$ is another binary operation on X, and if

$$x \diamond (y \star z) = (x \diamond y) \star (x \diamond z) \quad \text{and} \quad (y \star z) \diamond x = (y \diamond x) \star (z \diamond x)$$

for every x, y, and z in X, then $\diamond$ is said to be *distributive* with respect to $\star$. The above properties are called the *distributive laws*. A *ring* is an additive Abelian group X with a second binary operation on X, called *multiplication* and denoted by $\cdot$, such that

(e) the multiplication operation is associative and

(f) distributive with respect to the addition operation.

In this case the element $x \cdot y$ (which lies in X for every x and y in X) is called the *product* of x and y (alternative notation: xy instead of $x \cdot y$). A *commutative ring* is a ring for which

(g) the multiplication operation is commutative.

A *ring with identity* is a ring X such that

(h) the multiplication operation has a neutral element in X.

In this case such a (unique) neutral element in X with respect to the multiplication operation is denoted by 1 (so that $x \cdot 1 = 1 \cdot x = x$ for every $x \in X$) and is called the *identity*.

Example 2.B. The power set $\wp(X)$ of a nonempty set X is a commutative ring with identity if addition is interpreted as symmetric difference (or Boolean sum) and multiplication as intersection (i.e., $A + B = A \triangledown B$ and $A \cdot B = A \cap B$ for all subsets A and B of X). Here the neutral element under addition (i.e., the zero) is the empty set $\varnothing$, and the neutral element under multiplication (i.e., the identity) is X itself.

A ring with identity is *nontrivial* if it has another element besides the identity. (The set $\{0\}$ with the operations $0 + 0 = 0 \cdot 0 = 0$ is the trivial ring whose only element is the identity.) If a ring with identity is nontrivial, then the neutral element under addition and the neutral element under multiplication never coincide (i.e., $0 \neq 1$). In fact, $x \cdot 0 = 0 \cdot x = 0$ for every x in X whenever X is a ring (with or without identity). Incidentally (or not) this also shows that, in a nontrivial ring with identity, zero has no inverse with respect to the multiplication operation (i.e., there is no x in X such that $0 \cdot x = x \cdot 0 = 1$). A ring X with identity is called a *division ring* if

(i) each nonzero x in X has an inverse in X with respect to the multiplication operation.

That is, if $x \neq 0$ in X, then there exists a (unique) $x^{-1} \in X$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Example 2.C. Let the addition and multiplication operations have their ordinary ("numerical") meanings. The set of all natural numbers $\mathbb{N}$ is not a group under addition; neither is the set of all nonnegative integers $\mathbb{N}_0$. However, the set of all integers $\mathbb{Z}$ is a commutative ring with identity, but not a division ring. The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (of all rational, real, and complex numbers, respectively), when equipped with their respective operations of addition and multiplication, are all commutative division rings. These are infinite commutative division rings, but there are finite commutative division rings (e.g., if we declare that $1+1=0+0=0$, $0+1=1+0=1$, $0\cdot 0=0\cdot 1=1\cdot 0=0$, and $1\cdot 1=1$, then $\{0,1\}$ is a commutative division ring).

Roughly speaking, commutative division rings are the *number systems* of mathematics, and so they deserve a name of their own. A *field* is a nontrivial commutative division ring. The elements of a field are usually called *scalars*. We shall be particularly concerned with the fields $\mathbb{R}$ and $\mathbb{C}$ (the *real field* and the *complex field*). An arbitrary field will be denoted by $\mathbb{F}$. Summing up: A field $\mathbb{F}$ is a set with more than one element (at least 0 and 1 are distinct elements of it) equipped with two binary operations, called addition and multiplication, that satisfy all the properties (a) through (i) — clearly, with $\star$ replaced by $+$ in properties (a) through (d).

Definition 2.1. A *linear space* (or *vector space*) over a field $\mathbb{F}$ is a nonempty set $\mathcal{X}$ (whose elements are called *vectors*) satisfying the following axioms.

Vector Addition. $\mathcal{X}$ is an additive Abelian group under a binary operation $\dot{+}$ called *vector addition*.

Scalar Multiplication. There is given a mapping of $\mathbb{F}\times\mathcal{X}$ into $\mathcal{X}$ that assigns to each scalar α in $\mathbb{F}$ and each vector x in $\mathcal{X}$ a vector αx in $\mathcal{X}$. Such a mapping defines an operation, called *scalar multiplication*, with the following properties. For all scalars α and β in $\mathbb{F}$, and all vectors x and y in $\mathcal{X}$,

$$\begin{aligned} 1x &= x, \\ \alpha(\beta x) &= (\alpha\cdot\beta)x, \\ \alpha(x\dot{+}y) &= \alpha x\dot{+}\alpha y, \\ (\alpha+\beta)x &= \alpha x\dot{+}\beta x. \end{aligned}$$

Some remarks on notation and terminology. The *underlying set* of a linear space is the nonempty set upon which the linear space is built. We shall use the same notation $\mathcal{X}$ for both the linear space and its underlying set, even though the underlying set alone has no algebraic structure of its own. A set $\mathcal{X}$ needs a binary operation on it, a field, and another operation involving such a field with $\mathcal{X}$ to acquire the necessary algebraic structure that will grant it the status of a linear space. The scalar 1 in the above definition stands, of course, for the identity in the field $\mathbb{F}$ with respect to the multiplication $\cdot$ in $\mathbb{F}$, and $+$ denotes the addition in $\mathbb{F}$. Observe that $+$ (addition in the field $\mathbb{F}$) and $\dot{+}$ (addition in the group $\mathcal{X}$) are different binary operations. However, once the difference has been pointed out, we shall use the same symbol $+$ to denote both addition in the field $\mathbb{F}$ and addition in the group $\mathcal{X}$. Moreover, we shall also drop the dot from the multiplication notation in $\mathbb{F}$, and write $\alpha\beta$ instead of $\alpha \cdot \beta$. The neutral element under the vector addition in $\mathcal{X}$ (i.e., the vector zero) is referred to as the *origin* of the linear space $\mathcal{X}$. Again, we shall use one and the same symbol 0 to denote both the origin in $\mathcal{X}$ and the scalar zero in $\mathbb{F}$. A linear space over $\mathbb{R}$ is called a *real linear space*, and a linear space over $\mathbb{C}$ is called a *complex linear space*.

Example 2.D. $\mathbb{R}$ itself is a linear space over $\mathbb{R}$. That is, the plain set $\mathbb{R}$ when equipped with the ordinary binary operations of addition and multiplication becomes a field, also denoted by $\mathbb{R}$. If vector addition is identified with scalar addition, then it becomes a real linear space, denoted again by $\mathbb{R}$. More generally, for each $n \in \mathbb{N}$, let $\mathbb{F}^n$ denote the Cartesian product of n copies of a field $\mathbb{F}$ (i.e., the set of all ordered n-tuples of scalars in $\mathbb{F}$). Now define vector addition and scalar multiplication coordinatewise, as usual:

$$x + y = (\xi_1 + \upsilon_1, \ldots, \xi_n + \upsilon_n) \quad \text{and} \quad \alpha x = (\alpha\xi_1, \ldots, \alpha\xi_n)$$

for every $x = (\xi_1, \ldots, \xi_n)$ and $y = (\upsilon_1, \ldots, \upsilon_n)$ in $\mathbb{F}^n$ and every α in $\mathbb{F}$. This makes $\mathbb{F}^n$ into a linear space over $\mathbb{F}$. In particular, $\mathbb{R}^n$ (the Cartesian product of n copies of $\mathbb{R}$) and $\mathbb{C}^n$ (the Cartesian product of n copies of $\mathbb{C}$) become real and complex linear spaces, respectively, whenever vector addition and scalar multiplication are defined coordinatewise. However, if we restrict scalar multiplication to real multiplication only, then $\mathbb{C}^n$ can also be made into a real linear space.

Example 2.E. Let S be a nonempty set, and let $\mathbb{F}$ be an arbitrary field. Consider the set

$$\mathcal{X} = \mathbb{F}^S$$

of all functions from S to $\mathbb{F}$ (i.e., the set of all *scalar-valued functions* on S, where "scalar-valued" stands for "$\mathbb{F}$-valued"). Let vector addition and scalar multiplication be defined pointwise. That is, if x and y are functions in $\mathcal{X}$ and α is a scalar in $\mathbb{F}$, then $x + y$ and αx are functions in $\mathcal{X}$ defined by

$$(x + y)(s) = x(s) + y(s) \quad \text{and} \quad (\alpha x)(s) = \alpha(x(s))$$

for every $s \in S$. Now it is easy to show that $\mathcal{X}$, when equipped with these two operations, in fact is a linear space over $\mathbb{F}$. Particular cases: $\mathbb{F}^{\mathbb{N}}$ (the set of all *scalar-valued sequences*) and $\mathbb{F}^{[0,1]}$ (the set of all scalar-valued functions on the interval $[0,1]$) are linear spaces over $\mathbb{F}$, whenever vector addition and scalar multiplication are defined pointwise. Note that the linear space $\mathbb{F}^n$ in the previous example also is a particular case of the present example, where the coordinatewise operations are identified with the pointwise operations (recall: $\mathbb{F}^n = \mathbb{F}^{\mathbb{I}_n}$ where $\mathbb{I}_n = \{i \in \mathbb{N} \colon i \leq n\}$).

Example 2.F. What was the role played by the field $\mathbb{F}$ in the previous example? Answer: Vector addition and scalar multiplication in $\mathbb{F}^S$ were defined pointwise by using addition and multiplication in $\mathbb{F}$. This suggests the following generalization of Example 2.E. Let S be a nonempty set, and let $\mathcal{Y}$ be an arbitrary linear space (over a field $\mathbb{F}$). Consider the set

$$\mathcal{X} = \mathcal{Y}^S$$

of all functions from S to $\mathcal{Y}$ (i.e., the set of all $\mathcal{Y}$-valued functions on S). Let vector addition and scalar multiplication in $\mathcal{X}$ be defined pointwise by using vector addition and scalar multiplication in $\mathcal{Y}$. That is, if f and g are functions in $\mathcal{X}$ (so that $f(s)$ and $g(s)$ are elements of $\mathcal{Y}$ for each $s \in S$) and α is a scalar in $\mathbb{F}$, then $f+g$ and αf are functions in $\mathcal{X}$ defined by

$$(f+g)(s) = f(s) + g(s) \quad \text{and} \quad (\alpha f)(s) = \alpha(f(s))$$

for every $s \in S$. As before, it is easily verified that $\mathcal{X}$, when equipped with these operations, becomes a linear space over the same field $\mathbb{F}$. The origin of $\mathcal{X}$ is the *null function* $0\colon S \to \mathcal{Y}$ (which is defined by $0(s) = 0$ for all $s \in S$). Examples 2.D and 2.E can be thought of as particular cases of this one.

Example 2.G. Let $\mathcal{X}$ be a linear space over $\mathbb{F}$, and let x, x', y, and y' be arbitrary vectors in $\mathcal{X}$. An equivalence relation $\sim$ on $\mathcal{X}$ is *compatible with vector addition* if

$$x' \sim x \text{ and } y' \sim y \quad \text{imply} \quad x' + y' \sim x + y.$$

Similarly, it is said to be *compatible with scalar multiplication* if, for x and x' in $\mathcal{X}$ and α in $\mathbb{F}$,

$$x' \sim x \quad \text{implies} \quad \alpha x' \sim \alpha x.$$

If an equivalence relation $\sim$ on a linear space $\mathcal{X}$ is compatible with both vector addition and scalar multiplication, then we shall say that $\sim$ is a *linear equivalence relation*. Now consider $\mathcal{X}/\!\sim$, the quotient space of $\mathcal{X}$ modulo $\sim$ (i.e., the collection of all equivalence classes $[x]$ with respect to $\sim$), and suppose the equivalence relation $\sim$ on $\mathcal{X}$ is linear. In this case a binary operation $+$ on $\mathcal{X}/\!\sim$ can be defined by setting

$$[x] + [y] = [x + y]$$

for every $[x]$ and $[y]$ in $\mathcal{X}/\!\sim$. Indeed, since $\sim$ is compatible with vector addition, it follows that $[x+y]$ does not depend on which particular members x and y of the equivalence classes $[x]$ and $[y]$ were taken. Thus the operation $+$ actually is a function from $(\mathcal{X}/\!\sim \times \mathcal{X}/\!\sim)$ to $\mathcal{X}/\!\sim$. This defines vector addition in $\mathcal{X}/\!\sim$. Scalar multiplication in $\mathcal{X}/\!\sim$ can be similarly defined by setting

$$\alpha[x] = [\alpha x]$$

for every $[x]$ in $\mathcal{X}/\!\sim$ and α in $\mathbb{F}$. Therefore, if $\sim$ is a linear equivalence relation on a linear space $\mathcal{X}$ over a field $\mathbb{F}$, then $\mathcal{X}/\!\sim$ becomes a linear space over $\mathbb{F}$ when vector addition and scalar multiplication in $\mathcal{X}/\!\sim$ are defined this way.

It is clear by the definition of a linear space $\mathcal{X}$ that $x+y+z$ is a well-defined vector in $\mathcal{X}$ whenever x, y, and z are vectors in $\mathcal{X}$. Similarly, if $\{x_i\}_{i=1}^n$ is a *finite* set of vectors in $\mathcal{X}$, then the sum $x_1+\cdots+x_n$, denoted by $\sum_{i=1}^n x_i$, is again a vector in $\mathcal{X}$. (The notion of *infinite sums* needs *topology* and we shall consider these topics in Chapters 4 and 5.)

2.2 Linear Manifolds

A *linear manifold* of a linear space $\mathcal{X}$ over $\mathbb{F}$ is a nonempty subset $\mathcal{M}$ of $\mathcal{X}$ with the following properties.

$$x+y\in\mathcal{M} \quad \text{and} \quad \alpha x\in\mathcal{M}$$

for every pair of vectors x,y in $\mathcal{M}$ and every scalar α in $\mathbb{F}$. It is readily verified that a linear manifold $\mathcal{M}$ of a linear space $\mathcal{X}$ over a field $\mathbb{F}$ is itself a linear space over the same field $\mathbb{F}$. The origin 0 of $\mathcal{X}$ is the origin of every linear manifold $\mathcal{M}$ of $\mathcal{X}$. The *zero linear manifold* is $\{0\}$, consisting of the single vector 0. If a linear manifold $\mathcal{M}$ is a proper subset of $\mathcal{X}$, then it is said to be a *proper linear manifold*. A *nontrivial linear manifold* $\mathcal{M}$ of a linear space $\mathcal{X}$ is a nonzero proper linear manifold of it ($\{0\}\neq\mathcal{M}\neq\mathcal{X}$).

Example 2.H. Let $\mathcal{M}$ be a linear manifold of a linear space $\mathcal{X}$ and consider a relation $\sim$ on $\mathcal{X}$ defined as follows. If x and x' are vectors in $\mathcal{X}$, then

$$x'\!\sim x \quad \text{if} \quad x'-x\in\mathcal{M}.$$

That is, $x'\!\sim x$ if x' is *congruent to x modulo $\mathcal{M}$* — notation: $x'\equiv x(\text{mod }\mathcal{M})$. Since $\mathcal{M}$ is a linear manifold of $\mathcal{X}$, the relation $\sim$ in fact is an equivalence relation on $\mathcal{X}$ (reason: $0\in\mathcal{M}$ — reflexivity, $x'-x''=(x'-x)+(x-x'')\in\mathcal{M}$ whenever $x'-x$ and $x-x''$ lie in $\mathcal{M}$ — transitivity, and $x-x'\in\mathcal{M}$ whenever $x'-x\in\mathcal{M}$ — symmetry). The equivalence class (with respect to $\sim$)

$$[x] \;=\; \big\{x'\in\mathcal{X}\colon\; x'\!\sim x\big\} \;=\; \big\{x'\in\mathcal{X}\colon\; x'=x+z \text{ for some } z\in\mathcal{M}\big\}$$

of a vector x in $\mathcal{X}$ is called the *coset of x modulo $\mathcal{M}$* — notation: $[x]=x+\mathcal{M}$. The set of all cosets $[x]$ modulo $\mathcal{M}$ for every $x\in\mathcal{X}$ (i.e., the collection of all equivalence classes $[x]$ with respect to the equivalence relation $\sim$ for every x in $\mathcal{X}$) is precisely the quotient space $\mathcal{X}/\!\sim$ of $\mathcal{X}$ modulo $\sim$. Following the terminology introduced in Example 2.G, $\sim$ is a *linear equivalence relation* on the linear space $\mathcal{X}$. Indeed, if $x'-x\in\mathcal{M}$ and $y'-y\in\mathcal{M}$, then $(x'+y')-(x+y)=(x'-x)+(y'-y)\in\mathcal{M}$ and $\alpha x'-\alpha x=\alpha(x'-x)\in\mathcal{M}$ for every scalar α, so that $x'\!\sim x$ and $y'\!\sim y$ imply $x'+y'\!\sim x+y$ and $\alpha x'\!\sim \alpha x$. Therefore, with vector addition and scalar multiplication defined by

$$[x]+[y]=[x+y] \quad \text{and} \quad \alpha[x]=[\alpha x],$$

$\mathcal{X}/\!\sim$ is made into a linear space over the same scalar field. This is usually denoted by $\mathcal{X}/\mathcal{M}$ (instead of $\mathcal{X}/\!\sim$), and called the *quotient space of* $\mathcal{X}$ *modulo* $\mathcal{M}$. The origin of $\mathcal{X}/\mathcal{M}$ is, of course, $[0]=\mathcal{M}$. Let $\pi\colon\mathcal{X}\to\mathcal{X}/\mathcal{M}$ be the natural mapping of $\mathcal{X}$ onto the quotient space $\mathcal{X}/\mathcal{M}$ as defined in Section 1.4:

$$\pi(x) \,=\, [x] \,=\, x+\mathcal{M} \quad \text{for every} \quad x\in\mathcal{X}.$$

The concept of "linear transformation" will be defined in Section 2.5. It can be easily shown that π is a linear transformation between the linear spaces $\mathcal{X}$ and $\mathcal{X}/\mathcal{M}$. The *null space* of π, viz., $\mathcal{N}(\pi)=\{x\in\mathcal{X}\colon\ \pi(x)=[0]\}$, is given by

$$\mathcal{N}(\pi) \,=\, \mathcal{M}.$$

Indeed, if $\pi(x)=[0]=\mathcal{M}$, then $x+\mathcal{M}=[x]=[0]=\mathcal{M}$, and so $x\in\mathcal{M}$. On the other hand, if $u\in\mathcal{M}$, then $\pi(u)=u+\mathcal{M}=0+\mathcal{M}=\mathcal{M}=[0]$.

If $\mathcal{M}$ and $\mathcal{N}$ are linear manifolds of a linear space $\mathcal{X}$, then the *sum* of $\mathcal{M}$ and $\mathcal{N}$, denoted by $\mathcal{M}+\mathcal{N}$, is the subset of $\mathcal{X}$ made up of all sums $x+y$ where x is a vector in $\mathcal{M}$ and y is a vector in $\mathcal{N}$:

$$\mathcal{M}+\mathcal{N} \,=\, \big\{z\in\mathcal{X}\colon\ z=x+y,\ x\in\mathcal{M} \text{ and } y\in\mathcal{N}\big\}.$$

It is trivially verified that $\mathcal{M}+\mathcal{N}$ is a linear manifold of $\mathcal{X}$. If $\{\mathcal{M}_i\}_{i=1}^n$ is a finite family of linear manifolds of a linear space $\mathcal{X}$, then the sum $\sum_{i=1}^n\mathcal{M}_i$ is the linear manifold $\mathcal{M}_1+\cdots+\mathcal{M}_n$ of $\mathcal{X}$ consisting of all sums $\sum_{i=1}^n x_i$ where each vector x_i lies in $\mathcal{M}_i$. More generally, if $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ is an arbitrary indexed family of linear manifolds of a linear space $\mathcal{X}$, then the *sum* $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ is defined as the set of all sums $\sum_{\gamma\in\Gamma}x_\gamma$ with $x_\gamma\in\mathcal{M}_\gamma$ for each index γ and $x_\gamma=0$ except for some finite set of indices (i.e., $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ is the set made up of *all finite sums* with each summand being a vector in one of the linear manifolds $\mathcal{M}_\gamma$). Clearly, $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ is itself a linear manifold of $\mathcal{X}$, and $\mathcal{M}_\alpha\subseteq\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ for every $\mathcal{M}_\alpha\in\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$.

A linear manifold of a linear space $\mathcal{X}$ is never empty: the origin of $\mathcal{X}$ is always there. Note that the intersection $\mathcal{M}\cap\mathcal{N}$ of two linear manifolds $\mathcal{M}$ and $\mathcal{N}$ of a linear space $\mathcal{X}$ is itself a linear manifold of $\mathcal{X}$. In fact, if $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ is an arbitrary collection of linear manifolds of a linear space $\mathcal{X}$, then the intersection $\bigcap_{\gamma\in\Gamma}\mathcal{M}_\gamma$ is again a linear manifold of $\mathcal{X}$. Moreover, $\bigcap_{\gamma\in\Gamma}\mathcal{M}_\gamma\subseteq\mathcal{M}_\alpha$ for every $\mathcal{M}_\alpha\in\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$.

Consider the collection $\mathcal{L}at(\mathcal{X})$ of all linear manifolds of a linear space $\mathcal{X}$. Since $\mathcal{L}at(\mathcal{X})$ is a subcollection of the power set $\wp(\mathcal{X})$, it follows that $\mathcal{L}at(\mathcal{X})$ is partially ordered in the inclusion ordering. If $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ is a subcollection of $\mathcal{L}at(\mathcal{X})$, then $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ in $\mathcal{L}at(\mathcal{X})$ is an upper bound for $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ and $\bigcap_{\gamma\in\Gamma}\mathcal{M}_\gamma$ in $\mathcal{L}at(\mathcal{X})$ is a lower bound for $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$. If $\mathcal{U}\in\mathcal{L}at(\mathcal{X})$ is an upper bound for $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ (i.e., $\mathcal{M}_\gamma\subseteq\mathcal{U}$ for all $\gamma\in\Gamma$), then $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma\subseteq\mathcal{U}$. Thus

$$\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma \,=\, \sup\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}.$$

Similarly, if $\mathcal{V} \in \mathcal{L}at(\mathcal{X})$ is a lower bound for $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ (i.e., if $\mathcal{V} \subseteq \mathcal{M}_\gamma$ for all $\gamma \in \Gamma$), then $\mathcal{V} \subseteq \bigcap_{\gamma\in\Gamma}\mathcal{M}_\gamma$. Thus

$$\bigcap_{\gamma\in\Gamma} \mathcal{M}_\gamma \,=\, \inf\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}.$$

Conclusion: $\mathcal{L}at(\mathcal{X})$ is a complete lattice. *The collection of all linear manifolds of a linear space is a complete lattice in the inclusion ordering*. If $\{\mathcal{M},\mathcal{N}\}$ is a pair of elements of $\mathcal{L}at(\mathcal{X})$, then $\mathcal{M} \vee \mathcal{N} = \mathcal{M} + \mathcal{N}$ and $\mathcal{M} \wedge \mathcal{N} = \mathcal{M} \cap \mathcal{N}$.

Let A be an arbitrary subset of a linear space $\mathcal{X}$, and consider the subcollection (a sublattice, actually) $\mathcal{L}_A$ of the complete lattice $\mathcal{L}at(\mathcal{X})$,

$$\mathcal{L}_A \,=\, \big\{\mathcal{M} \in \mathcal{L}at(\mathcal{X}) \colon\; A \subseteq \mathcal{M}\big\},$$

consisting of all linear manifolds of $\mathcal{X}$ that include A. Set

$$\operatorname{span} A \,=\, \inf \mathcal{L}_A \,=\, \bigcap \mathcal{L}_A,$$

which is called the (linear) *span* of A. Since $A \subseteq \bigcap \mathcal{L}_A$ (for $A \subseteq \mathcal{M}$ for every $\mathcal{M} \in \mathcal{L}_A$), it follows that $\inf \mathcal{L}_A = \min \mathcal{L}_A$ so that $\operatorname{span} A \in \mathcal{L}_A$. Thus $\operatorname{span} A$ *is the smallest linear manifold of* $\mathcal{X}$ *that includes* A, which coincides with *the intersection of all linear manifolds of* $\mathcal{X}$ *that include* A. It is readily verified that $\operatorname{span}\varnothing = \{0\}$, $\operatorname{span}\mathcal{M} = \mathcal{M}$ for every $\mathcal{M} \in \mathcal{L}at(\mathcal{X})$, and $A \subseteq \operatorname{span} A = \operatorname{span}(\operatorname{span} A)$ for every $A \in \wp(\mathcal{X})$. Moreover, if A and B are subsets of $\mathcal{X}$, then

$$A \subseteq B \quad \text{implies} \quad \operatorname{span} A \subseteq \operatorname{span} B.$$

If $\mathcal{M}$ and $\mathcal{N}$ are linear manifolds of a linear space $\mathcal{X}$, then $\mathcal{M} \cup \mathcal{N} \subseteq \mathcal{M} + \mathcal{N}$. Moreover, if $\mathcal{K}$ is a linear manifold of $\mathcal{X}$ such that $\mathcal{M} \cup \mathcal{N} \subseteq \mathcal{K}$, then $x + y \in \mathcal{K}$ for every $x \in \mathcal{M}$ and every $y \in \mathcal{N}$, and hence $\mathcal{M} + \mathcal{N} \subseteq \mathcal{K}$. Thus $\mathcal{M} + \mathcal{N}$ is the smallest linear manifold of $\mathcal{X}$ that includes $\mathcal{M} \cup \mathcal{N}$, which means that

$$\mathcal{M} + \mathcal{N} \,=\, \operatorname{span}(\mathcal{M} \cup \mathcal{N}).$$

More generally, let $\{\mathcal{M}_\gamma\}_{\gamma\in\Gamma}$ be an arbitrary subcollection of $\mathcal{L}at(\mathcal{X})$, and suppose $\mathcal{K} \in \mathcal{L}at(\mathcal{X})$ is such that $\bigcup_{\gamma\in\Gamma}\mathcal{M}_\gamma \subseteq \mathcal{K}$. Then every (finite) sum $\sum_{\gamma\in\Gamma} x_\gamma$ with each x_γ in $\mathcal{M}_\gamma$ is a vector in $\mathcal{K}$. Thus $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma \subseteq \mathcal{K}$. Since $\bigcup_{\gamma\in\Gamma}\mathcal{M}_\gamma \subseteq \sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$, it follows that $\sum_{\gamma\in\Gamma}\mathcal{M}_\gamma$ is the smallest element of $\mathcal{L}at(\mathcal{X})$ that includes $\bigcup_{\gamma\in\Gamma}\mathcal{M}_\gamma$. Equivalently,

$$\sum_{\gamma\in\Gamma} \mathcal{M}_\gamma \,=\, \operatorname{span}\Big(\bigcup_{\gamma\in\Gamma} \mathcal{M}_\gamma\Big).$$

2.3 Linear Independence

Let A be a nonempty subset of a linear space $\mathcal{X}$. A vector $x \in \mathcal{X}$ is a *linear combination* of vectors in A if there exist a *finite* set $\{x_i\}_{i=1}^n$ of vectors in A and a *finite* family of scalars $\{\alpha_i\}_{i=1}^n$ such that

$$x = \sum_{i=1}^{n} \alpha_i x_i.$$

Warning: A linear combination is, by definition, *finite*. That is, a linear combination of vectors in a set A is a weighted sum of a finite subset of vectors in A, weighted by a finite family of scalars, no matter whether A is a finite or an infinite set. Since $\mathcal{X}$ is a linear space, any linear combination of vectors in A is a vector in $\mathcal{X}$.

Proposition 2.2. *The set of all linear combinations of vectors in a nonempty subset A of a linear space $\mathcal{X}$ coincides with the linear manifold* $\operatorname{span} A$.

Proof. Let A be an arbitrary subset of a linear space $\mathcal{X}$, consider the collection $\mathcal{L}_A$ of all linear manifolds of $\mathcal{X}$ that include A, and recall that

$$\operatorname{span} A = \min \mathcal{L}_A.$$

Suppose A is nonempty and let $\langle A \rangle$ denote the set of all linear combinations of vectors in A. It is plain that $A \subseteq \langle A \rangle$ (every vector in A is a trivial linear combination of vectors in A), and that $\langle A \rangle$ is a linear manifold of $\mathcal{X}$ (if $x, y \in \langle A \rangle$, then $x + y$ and αx lie in $\langle A \rangle$). Therefore,

$$\langle A \rangle \in \mathcal{L}_A.$$

Moreover, if $\mathcal{M}$ is an arbitrary linear manifold of $\mathcal{X}$, and if $x \in \mathcal{X}$ is a linear combination of vectors in $\mathcal{M}$, then $x \in \mathcal{M}$ (because $\mathcal{M}$ is itself a linear space). Thus $\langle \mathcal{M} \rangle \subseteq \mathcal{M}$. Since $\mathcal{M} \subseteq \langle \mathcal{M} \rangle$, it follows that $\langle \mathcal{M} \rangle = \mathcal{M}$ for every linear manifold $\mathcal{M}$ of $\mathcal{X}$. Furthermore, if $\mathcal{M} \in \mathcal{L}_A$, then $A \subseteq \mathcal{M}$ and so $\langle A \rangle \subseteq \langle \mathcal{M} \rangle$ (reason: $\langle A \rangle \subseteq \langle B \rangle$ whenever A and B are nonempty subsets of $\mathcal{X}$ such that $A \subseteq B$). Thus

$$\mathcal{M} \in \mathcal{L}_A \quad \text{implies} \quad \langle A \rangle \subseteq \mathcal{M}.$$

Conclusion: $\langle A \rangle$ is the smallest element of $\mathcal{L}_A$. That is,

$$\langle A \rangle = \operatorname{span} A. \qquad \square$$

Following the notation introduced in the proof of Proposition 2.2, $\langle A \rangle = \operatorname{span} A$ whenever $A \neq \varnothing$. Set $\langle \varnothing \rangle = \operatorname{span} \varnothing$ so that $\langle \varnothing \rangle = \{0\}$, and hence $\langle A \rangle$ is well defined for every subset A of $\mathcal{X}$. We shall use one and the same notation, viz., $\operatorname{span} A$, for both of them: the set of all linear combinations of vectors in A and the (linear) span of A. For this reason $\operatorname{span} A$ is also referred to as the *linear manifold generated* (or *spanned*) by A. If a linear manifold $\mathcal{M}$ of $\mathcal{X}$ (which may be $\mathcal{X}$ itself) is such that $\operatorname{span} A = \mathcal{M}$ for some subset A of $\mathcal{X}$, then we say that A *spans* $\mathcal{M}$.

A subset A of a linear space $\mathcal{X}$ is said to be *linearly independent* if each vector x in A is not a linear combination of vectors in $A \backslash \{x\}$. Equivalently, A

is linearly independent if $x \notin \operatorname{span}(A \backslash \{x\})$ for every $x \in A$. If a set A is not linearly independent, then it is said to be *linearly dependent*. Note that the empty set $\varnothing$ of a linear space $\mathcal{X}$ is linearly independent (there is no vector in $\varnothing$ that is a linear combination of vectors in $\varnothing$). Any singleton $\{x\}$ of $\mathcal{X}$ such that $x \neq 0$ is linearly independent. Indeed, $\operatorname{span}(\{x\} \backslash \{x\}) = \operatorname{span} \varnothing = \{0\}$ so that $x \notin \operatorname{span}(\{x\} \backslash \{x\})$ if $x \neq 0$. However, $0 \in \operatorname{span}(\{0\} \backslash \{0\}) = \{0\}$, and hence the singleton $\{0\}$ is not linearly independent. In fact, every subset of $\mathcal{X}$ that contains the origin of $\mathcal{X}$ is not linearly independent (indeed, if $0 \in A \subseteq \mathcal{X}$ and A has another vector, say $x \neq 0$, then $0 = 0x$). Thus, if a vector x is an element of a linearly independent subset of a linear space $\mathcal{X}$, then $x \neq 0$.

Proposition 2.3. *Let A be a nonempty subset of a linear space $\mathcal{X}$. The following assertions are pairwise equivalent.*

(a) *A is linearly independent.*

(b) *Each nonzero vector in* $\operatorname{span} A$ *has a unique representation as a linear combination of vectors in A.*

(c) *Every finite subset of A is linearly independent.*

(d) *There is no proper subset of A whose span coincides with* $\operatorname{span} A$.

Proof. The statement (b) can be rewritten as follows.

(b$'$) For every nonzero $x \in \operatorname{span} A$ there exist a unique finite family of scalars $\{\alpha_i\}_{i=1}^n$ and a unique finite subset $\{a_i\}_{i=1}^n$ of A such that $x = \sum_{i=1}^n \alpha_i a_i$.

Proof of (a)$\Rightarrow$(b). Suppose $A \neq \varnothing$ is linearly independent. Take an arbitrary nonzero $x \in \operatorname{span} A$, and consider two representations of it as a linear combination of vectors in A:

$$x = \sum_{i=1}^{n} \beta_i b_i = \sum_{i=1}^{m} \gamma_i c_i,$$

where each b_i and each c_i are vectors in A (and hence nonzero because A is linearly independent). Since $x \neq 0$ we may assume that the scalars β_i and γ_i are all nonzero. Set $B = \{b_i\}_{i=1}^n$ and $C = \{c_i\}_{i=1}^m$, both finite nonempty subsets of A. Take an arbitrary $b \in B$ and note that b is a linear combination of vectors in $(B \backslash \{b\}) \cup C$. However, since $b \in A$ and A is linearly independent, it follows that b is not a linear combination of any subset of $A \backslash \{b\}$. Thus $b \in C$. Similarly, take an arbitrary $c \in C$ and conclude that $c \in B$ by using the same argument. Hence $B \subseteq C \subseteq B$. That is, $B = C$. Therefore $x = \sum_{i=1}^n \beta_i b_i = \sum_{i=1}^n \gamma_i b_i$, which implies that $\sum_{i=1}^n (\beta_i - \gamma_i) b_i = 0$. Since each b_i is not a linear combination of vectors in $B \backslash \{b_i\}$, it follows that $\beta_i = \gamma_i$ for every i. Summing up: The two representations of x coincide.

Proof of (b)$\Rightarrow$(a). If A is nonempty and every nonzero vector x in $\operatorname{span} A$ has a unique representation as a linear combination of vectors in A, then the unique representation of an arbitrary a in A as a linear combination of vectors in A is a itself (recall: $A \subseteq \operatorname{span} A$). Therefore, every $a \in A$ is not a linear combination of vectors in $A \backslash \{a\}$, which means that A is linearly independent.

Proof of (a)$\Leftrightarrow$(c). If A is linearly independent, then every subset of it clearly is linearly independent. If A is not linearly independent, then either $A = \{0\}$ or there exists $x \in A$ which is a linear combination of vectors, say $\{x_i\}_{i=1}^n$ for some $n \in \mathbb{N}$, in $A\backslash\{x\} \neq \varnothing$. In the former case A is itself a finite subset of A which is not linearly independent. In the latter case $\{x_i\}_{i=1}^n \cup \{x\}$ is a finite subset of A that is not linearly independent. Conclusion: If every finite subset of A is linearly independent, then A is itself linearly independent.

Proof of (a)$\Rightarrow$(d). Recalling that $B \subseteq A$ implies $\operatorname{span} B \subseteq \operatorname{span} A$, the statement (d) can be rewritten as follows.

(d$'$) $B \subset A$ implies $\operatorname{span} B \subset \operatorname{span} A$.

Suppose A is nonempty and linearly independent. Let B be an arbitrary proper subset of A. If $B = \varnothing$, then (d$'$) holds trivially ($\varnothing \neq A \neq \{0\}$ so that $\operatorname{span} \varnothing \subset \operatorname{span} A$). Thus suppose $B \neq \varnothing$ and take any $x \in A\backslash B$. If $x \in \operatorname{span} B$, then x is a linear combination of vectors in B. This implies that $B \cup \{x\}$ is a subset of A that is not linearly independent, and so A itself is not linearly independent, which is a contradiction. Therefore, $x \notin \operatorname{span} B$ for every $x \in A\backslash B$ whenever $\varnothing \neq B \subset A$. Since $x \in \operatorname{span} A$ (for $x \in A$) and $\operatorname{span} B \subseteq \operatorname{span} A$ (for $B \subset A$), it follows that $\operatorname{span} B \subset \operatorname{span} A$ so that (d$'$) holds true.

Proof of (d)$\Rightarrow$(a). If A is not linearly independent, then either $A = \{0\}$ or there is an $x \in A$ which is a linear combination of vectors in $A\backslash\{x\}$. In the former case $B = \varnothing$ is the unique proper subset of A and $\operatorname{span} B = \{0\} = \operatorname{span} A$. In the latter case $B = A\backslash\{x\}$ is a proper subset of A such that $\operatorname{span} B = \operatorname{span} A$. (Indeed, $\operatorname{span} B \subseteq \operatorname{span} A$ as $B \subseteq A$, and $\operatorname{span} A \subseteq \operatorname{span} B$ as vectors in A are linear combinations of vectors in $A\backslash\{x\}$.) Thus (d$'$) implies (a). □

2.4 Hamel Basis

A linearly independent subset of a linear space $\mathcal{X}$ that spans $\mathcal{X}$ is called a *Hamel basis* (or a *linear basis*) for $\mathcal{X}$. In other words, a subset B of a linear space $\mathcal{X}$ is a Hamel basis for $\mathcal{X}$ if

(i) B is linearly independent, and

(ii) $\operatorname{span} B = \mathcal{X}$.

Let $B = \{x_\gamma\}_{\gamma\in\Gamma}$ be an indexed Hamel basis for a linear space $\mathcal{X}$. If x is a nonzero vector in $\mathcal{X}$, then Proposition 2.3 ensures the existence of a unique (similarly indexed) family of scalars $\{\alpha_\gamma\}_{\gamma\in\Gamma}$ (which may depend on x) such that $\alpha_\gamma = 0$ for all but a finite set of indices γ and $x = \sum_{\gamma\in\Gamma}\alpha_\gamma x_\gamma$. The weighted sum $\sum_{\gamma\in\Gamma}\alpha_\gamma x_\gamma$ (i.e., the unique representation of x as a linear combination of vectors in B, or the unique (linear) representation of x in terms of B) is called the *expansion* of x on B, and the coefficients of it (i.e., the unique indexed family of scalars $\{\alpha_\gamma\}_{\gamma\in\Gamma}$) are called the *coordinates* of x with respect to the indexed basis B. If $x = 0$, then its unique expansion on B is the trivial one whose coefficients are all null.

Since $\varnothing$ is linearly independent, and since $\operatorname{span}\varnothing = \{0\}$, it follows that the empty set $\varnothing$ is a Hamel basis for the zero linear space $\{0\}$. Now suppose $\mathcal{X}$ is a nonzero linear space. Every singleton $\{x\}$ in $\mathcal{X}$ such that $x \neq 0$ is linearly independent. Thus every nonzero linear space has many linearly independent subsets. If a linearly independent subset A of $\mathcal{X}$ is not already a Hamel basis for $\mathcal{X}$, then we can construct a larger linearly independent subset of $\mathcal{X}$.

Proposition 2.4. *If A is a linearly independent subset of a linear space $\mathcal{X}$, and if there exists a vector x in $\mathcal{X}\backslash\operatorname{span} A$, then $A \cup \{x\}$ is another linearly independent subset of $\mathcal{X}$.*

Proof. Suppose there exists $x \in \mathcal{X}\backslash\operatorname{span} A$. Note that $x \neq 0$, and so $\mathcal{X} \neq \{0\}$. If $A = \varnothing$, then the result is trivially verified ($\{x\} = \varnothing \cup \{x\}$ is linearly independent). Thus suppose A is nonempty and set $C = A \cup \{x\} \subset \mathcal{X}$. Since $x \notin \operatorname{span} A$, it follows that $x \notin \operatorname{span}(C\backslash\{x\})$. Take an arbitrary $a \in A$. Suppose it is a linear combination of vectors in $C\backslash\{a\}$. Since $a \neq \alpha x$ for every scalar α (for $x \notin \operatorname{span} A$ and $a \neq 0$ because A is linearly independent), we get

$$a = \alpha_0 x + \sum_{i=1}^{n} \alpha_i a_i,$$

where each a_i is a vector in $A\backslash\{a\}$ and each α_i is a nonzero scalar (recall: $0 \neq a \neq \sum_{i=1}^{n} \alpha_i a_i$ because A is linearly independent). Thus x is a linear combination of vectors in A, which contradicts the assumption that $x \notin \operatorname{span} A$. Therefore, every $a \in A$ is not a linear combination of vectors in $C\backslash\{a\}$. Conclusion: Every $c \in C$ is not a linear combination of vectors in $C\backslash\{c\}$, which means that C is linearly independent. $\square$

Can we proceed this way, enlarging linearly independent subsets of $\mathcal{X}$ in order to form a chain of linearly independent subsets, so that an "ultimate" linearly independent subset becomes a Hamel basis for $\mathcal{X}$? Yes, we can; and it seems reasonable that the Axiom of Choice (or any statement equivalent to it as, for instance, Zorn's Lemma) might be called into play. In fact, every linearly independent subset of any linear space $\mathcal{X}$ is included in some Hamel basis for $\mathcal{X}$, so that every linear space has a large supply of Hamel bases.

Theorem 2.5. *If A is a linearly independent subset of a linear space $\mathcal{X}$, then there exists a Hamel basis B for $\mathcal{X}$ such that $A \subseteq B$.*

Proof. Suppose A is a linearly independent subset of a linear space $\mathcal{X}$. Set

$$\mathcal{I}_A = \big\{B \in \wp(\mathcal{X})\colon\; B \text{ is linearly independent and } A \subseteq B\big\},$$

the collection of all linearly independent subsets of $\mathcal{X}$ that include A. Recall that, as a nonempty subcollection (since $A \in \mathcal{I}_A$) of the power set $\wp(\mathcal{X})$, $\mathcal{I}_A$ is partially ordered in the inclusion ordering.

Claim 1. $\mathcal{I}_A$ has a maximal element.

Proof. If $\mathcal{X} = \{0\}$, then $A = \varnothing$ and $\mathcal{I}_A = \{A\} = \{\varnothing\} \neq \varnothing$, so that the claimed result is trivially verified. Thus suppose $\mathcal{X} \neq \{0\}$. In this case, the nonempty collection $\mathcal{I}_A$ contains a nonempty set (e.g., if $A = \varnothing$, then every nonzero singleton in $\mathcal{X}$ belongs to $\mathcal{I}_A$; if $A \neq \varnothing$, then $A \in \mathcal{I}_A$). Now consider an arbitrary chain $\mathcal{C}$ in $\mathcal{I}_A$ containing a nonempty set. Recall that $\bigcup\mathcal{C}$ denotes the union of all sets in $\mathcal{C}$. Take an arbitrary finite nonempty subset of $\bigcup\mathcal{C}$, say, a set $D \subseteq \bigcup\mathcal{C}$ such that $\#D = n$ for some $n \in \mathbb{N}$. Each element of D belongs to a set in $\mathcal{C}$ (for $D \subseteq \bigcup\mathcal{C}$). Since $\mathcal{C}$ is a chain, we can arrange the elements of D as follows. $D = \{x_i\}_{i=1}^n$ such that $x_i \in C_i \in \mathcal{C}$ for each index i, where $C_1 \subseteq \cdots \subseteq C_n$. Thus $D \subseteq C_n$. Since C_n is linearly independent (because $C_n \in \mathcal{C} \subseteq \mathcal{I}_A$), it follows that D is linearly independent. Conclusion: Every finite subset of $\bigcup\mathcal{C}$ is linearly independent. Therefore $\bigcup\mathcal{C}$ is linearly independent by Proposition 2.3. Moreover, since $A \subseteq C$ for all $C \in \mathcal{C}$ (for $\mathcal{C} \subseteq \mathcal{I}_A$), it also follows that $A \subseteq \bigcup\mathcal{C}$. Hence $\bigcup\mathcal{C} \in \mathcal{I}_A$. Since $\bigcup\mathcal{C}$ clearly is an upper bound for $\mathcal{C}$, we may conclude: Every chain in $\mathcal{I}_A$ has an upper bound in $\mathcal{I}_A$. Thus $\mathcal{I}_A$ has a maximal element by Zorn's Lemma. □

Claim 2. $B \in \mathcal{I}_A$ is maximal in $\mathcal{I}_A$ if and only if B is a Hamel basis for X.

Proof. Again, if $\mathcal{X} = \{0\}$, then $B = A = \varnothing$ is the only (and so a maximal) element in $\mathcal{I}_A$ and $\operatorname{span} B = \mathcal{X}$, so that the claimed result holds trivially. Thus suppose $\mathcal{X} \neq \{0\}$, which implies that $\mathcal{I}_A$ contains nonempty sets, and take an arbitrary B in $\mathcal{I}_A$. If $\operatorname{span} B \neq \mathcal{X}$ (i.e., if $\operatorname{span} B \subset \mathcal{X}$), then take $x \in \mathcal{X}\backslash\operatorname{span} B$ so that $B \cup \{x\} \in \mathcal{I}_A$ (i.e., $B \cup \{x\}$ is linearly independent by Proposition 2.4, and $A \subset B \cup \{x\}$ because $A \subseteq B$). Hence B is not maximal in $\mathcal{I}_A$. Therefore, if B is maximal in $\mathcal{I}_A$, then $\operatorname{span} B = \mathcal{X}$. On the other hand, if $\operatorname{span} B = \mathcal{X}$, then $B \neq \varnothing$ (for $\mathcal{X} \neq \{0\}$) and every vector in $\mathcal{X}$ is a linear combination of vectors in B. Thus $B \cup \{x\}$ is not linearly independent for every $x \in \mathcal{X}\backslash B$. This implies that there is no $B' \in \mathcal{I}_A$ such that $B \subset B'$, which means that B is maximal in $\mathcal{I}_A$. Conclusion: If $B \in \mathcal{I}_A$, then B is maximal in $\mathcal{I}_A$ if and only if $\operatorname{span} B = \mathcal{X}$. According to the definition of Hamel basis, B in $\mathcal{I}_A$ is such that $\operatorname{span} B = \mathcal{X}$ if and only if B is a Hamel basis for $\mathcal{X}$. □

Claims 1 and 2 ensure that, for each linearly independent subset A of $\mathcal{X}$, there exists a Hamel basis B for $\mathcal{X}$ such that $A \subseteq B$. □

Since the empty set is a linearly independent subset of any $\mathcal{X}$, Theorem 2.5 ensures (by setting $A = \varnothing$) that *every linear space has a Hamel basis*. In this case $\mathcal{I}_\varnothing$ is the collection of all linearly independent subsets of $\mathcal{X}$, and so Claim 2 says that *a Hamel basis for a linear space is precisely a maximal linearly independent subset of it* (i.e., a Hamel basis is a maximal element of $\mathcal{I}_\varnothing$).

The idea behind the previous theorem was that of enlarging a linearly independent subset of $\mathcal{X}$ to get a Hamel basis for $\mathcal{X}$. Another way of facing the same problem (i.e., another way to obtain a Hamel basis for linear space $\mathcal{X}$) is to begin with a set that spans $\mathcal{X}$ and then to weed out from it a linearly independent subset that also spans $\mathcal{X}$.

Theorem 2.6. *If a subset A of a linear space $\mathcal{X}$ spans $\mathcal{X}$, then there exists a Hamel basis B for $\mathcal{X}$ such that $B \subseteq A$.*

Proof. Let A be a subset of a linear space $\mathcal{X}$ such that $\operatorname{span} A = \mathcal{X}$, and consider the collection $\mathcal{I}'_A$ of all linearly independent subsets of A:

$$\mathcal{I}'_A = \big\{B \in \wp(\mathcal{X}):\ B \text{ is linearly independent and } B \subseteq A\big\}.$$

If $\mathcal{X} = \{0\}$, then either $A = \varnothing$ or $A = \{0\}$. In any case $\mathcal{I}'_A = \{\varnothing\}$ trivially has a maximal element. If $\mathcal{X} \neq \{0\}$, then A has a nonzero vector (for $\operatorname{span} A = \mathcal{X}$) and every nonzero singleton $\{x\} \subseteq A$ is a element of $\mathcal{I}'_A$. Thus, proceeding exactly as in the proof of Theorem 2.5 (Claim 1), we can show that $\mathcal{I}'_A$ has a maximal element. Let A_0 be a maximal element of $\mathcal{I}'_A$. If A is linearly independent, then we are done (i.e., A is itself a Hamel basis for $\mathcal{X}$ since $\operatorname{span} A = \mathcal{X}$). Thus suppose A is not linearly independent so that A_0 is a proper subset of A. Take an arbitrary $a \in A \backslash A_0$ and consider the set $A_0 \cup \{a\} \subseteq A$, which is not linearly independent because A_0 is maximal in $\mathcal{I}'_A$. Since A_0 is linearly independent, it follows that a is a linear combination of vectors in A_0. Thus $A \backslash A_0 \subseteq \operatorname{span} A_0$, and hence $A = A_0 \cup (A \backslash A_0) \subseteq \operatorname{span} A_0$. Therefore $\operatorname{span} A \subseteq \operatorname{span}(\operatorname{span} A_0) = \operatorname{span} A_0 \subseteq \operatorname{span} A$, which implies that $\operatorname{span} A_0 = \operatorname{span} A = \mathcal{X}$. Conclusion: A_0 is a Hamel basis for $\mathcal{X}$. $\square$

Since $\mathcal{X}$ trivially spans $\mathcal{X}$, Theorem 2.6 holds for $A = \mathcal{X}$. In this case $\mathcal{I}'_{\mathcal{X}}$ is the collection of all linearly independent subsets of $\mathcal{X}$ (i.e., $\mathcal{I}'_{\mathcal{X}} = \mathcal{I}_{\varnothing}$), and the theorem statement again says that every linear space has a Hamel basis.

An ever-present purpose in mathematics is a quest for hidden invariants. The concept of Hamel basis supplies a fundamental invariant for a given linear space $\mathcal{X}$, namely, the cardinality of all Hamel bases for $\mathcal{X}$.

Theorem 2.7. *Every Hamel basis for a linear space has the same cardinality.*

Proof. If $\mathcal{X} = \{0\}$, then the result holds trivially. Suppose $\mathcal{X} \neq \{0\}$ and let B and C be arbitrary Hamel bases for $\mathcal{X}$ (so that they are nonempty and do not contain the origin). Proposition 2.3 ensures that for every nonzero vector x in $\mathcal{X}$ there is a unique finite subset of the Hamel basis C, say C_x, such that x is a linear combination of all vectors in $C_x \subseteq C$. Now take an arbitrary $c \in C$ and consider the unique representation of it as a linear combination of vectors in the Hamel basis B. Thus c is a linear combination of all vectors in $\{b\} \cup B'$ for some (nonzero) $b \in B$ and some finite subset B' of B. Hence $c = \beta b + d$, where β is a nonzero scalar and d is a vector in $\mathcal{X}$ different from c (for $\beta b \neq 0$). If $d = 0$, then $c = \beta b$ so that $C_b = \{c\}$, and hence $c \in C_b$ trivially. Suppose

$d \neq 0$. Recalling again that C also is a Hamel basis for $\mathcal{X}$, consider the unique representation of the nonzero vector d as a linear combination of vectors in C so that $\beta b = c - d \neq 0$ is a linear combination of vectors in C. Thus b is itself a linear combination of all vectors in $\{c\} \cup C'$ for some subset C' of C. Since such a representation is unique, $\{c\} \cup C' = C_b$. Therefore $c \in C_b$. Summing up: For every $c \in C$ there exists $b \in B$ such that $c \in C_b$. Hence

$$C \subseteq \bigcup_{b \in B} C_b.$$

Now we shall split the proof into two parts, one dealing with the case of finite Hamel bases, and the other with infinite Hamel bases.

Claim 0. If a subset E of a linear space $\mathcal{X}$ has exactly n elements and spans $\mathcal{X}$, then every subset of $\mathcal{X}$ with more than n elements is not linearly independent.

Proof. Assume the linear space $\mathcal{X}$ is nonzero (i.e., $\mathcal{X} \neq \{0\}$) to avoid trivialities. Take an integer $n \in \mathbb{N}$ and let $E = \{e_i\}_{i=1}^n$ be a subset of $\mathcal{X}$ with n elements such that $\operatorname{span} E = \mathcal{X}$. Take any subset of $\mathcal{X}$ with $n+1$ elements, say $D = \{d_i\}_{i=1}^{n+1}$. Suppose D is linearly independent. Now consider the set

$$S_1 = \{d_1\} \cup E$$

which clearly spans $\mathcal{X}$ (because E already does). Since $\operatorname{span} E = \mathcal{X}$, it follows that d_1 is a linear combination of vectors in E. Moreover, $d_1 \neq 0$ because D is linearly independent. Thus $d_1 = \sum_{i=1}^n \alpha_i e_i$ where at least one, say α_k, of the scalars $\{\alpha_i\}_{i=1}^n$ is nonzero. Therefore, if we delete e_k from S_1, then the set

$$S_1' = S_1 \backslash \{e_k\} = \{d_1\} \cup E \backslash \{e_k\}$$

still spans $\mathcal{X}$. That is, in forming this new set S_1' that spans $\mathcal{X}$ we have traded off one vector in D for one vector in E. Next rename the elements of S_1' by setting $s_i = e_i$ for each $i \neq k$ and $s_k = d_1$, so that $S_1' = \{s_i\}_{i=1}^n$. Since D has at least two elements, set

$$S_2 = \{d_2\} \cup S_1' = \{d_1, d_2\} \cup E \backslash \{e_k\}$$

which again spans $\mathcal{X}$ (for S_1' spans $\mathcal{X}$). Since $\operatorname{span} S_1' = \mathcal{X}$, it follows that d_2 is a linear combination of vectors in S_1', say $d_2 = \sum_{i=1}^n \beta_i s_i$ for some family of scalars $\{\beta_i\}_{i=1}^n$. Moreover, $0 \neq d_2 \neq \beta_k s_k = \beta_k d_1$ because D is linearly independent. Thus there is at least one nonzero scalar in $\{\beta_i\}_{i=1}^n$ different from β_k, say β_j. Hence, if we delete s_j from S_2 (recall: $s_j = e_j \neq e_k$), then the set

$$S_2' = S_2 \backslash \{e_j\} = \{d_1, d_2\} \cup E \backslash \{e_k, e_j\}$$

still spans $\mathcal{X}$. Continuing this way, we eventually get down to the set

$$S_n' = \{d_i\}_{i=1}^n \cup E \backslash \{e_i\}_{i=1}^n = D \backslash \{d_{n+1}\}$$

which once again spans $\mathcal{X}$. Thus d_{n+1} is a linear combination of vectors in $D\backslash\{d_{n+1}\}$, which contradicts the assumption that D is linearly independent. Conclusion: Every subset of $\mathcal{X}$ with $n+1$ elements is not linearly independent. Recalling that every subset of a linearly independent set is again linearly independent, it follows that every subset of $\mathcal{X}$ with more than n elements is not linearly independent. □

Claim 1. If B is finite, then $\#C = \#B$.

Proof. Recall that C_b is finite for every b in B. If B is finite, then $\bigcup_{b\in B} C_b$ is a finite union of finite sets. Hence any subset of it is finite. In particular, C is finite. Since C is linearly independent, it follows by Claim 0 that $\#C \leq \#B$. Dually (swap the Hamel bases B and C), $\#B \leq \#C$. Hence $\#C = \#B$. □

Claim 2. If B is infinite, then $\#C = \#B$.

Proof. If B is infinite, and since C_b is finite for every b in B, it follows that $\#C_b \leq \#B$ for all b in B. Thus, according to Theorems 1.9 and 1.10,

$$\#\Big(\bigcup_{b\in B} C_b\Big) \;\leq\; \#\big(B\times B\big) \;=\; \#B$$

because B is infinite. Hence $\#C \leq \#B$ (recall: $C \subseteq \bigcup_{b\in B} C_b$ and use Problems 1.21(a) and 1.22). Moreover, Claim 1 ensures that B and C are finite together. Thus C must be infinite as B is infinite. Since C is infinite we may reverse the argument (swapping again the Hamel bases B and C) and get $\#B \leq \#C$. Hence $\#C = \#B$ by the Cantor–Bernstein Theorem (Theorem 1.6). □

Claims 1 and 2 ensure that, if B and C are Hamel bases for a linear space $\mathcal{X}$, then B and C have the same cardinal number. □

Such an invariant (i.e., the cardinality of any Hamel basis) is called the *dimension* (or the *linear dimension*) of the linear space $\mathcal{X}$, denoted by $\dim \mathcal{X}$. Thus $\dim \mathcal{X} = \#B$ for any Hamel basis B for $\mathcal{X}$. If the dimension of $\mathcal{X}$ is finite (equivalently, if any Hamel basis for $\mathcal{X}$ is a finite set), then we say that $\mathcal{X}$ is a *finite-dimensional linear space*. Otherwise (i.e., if any Hamel basis for $\mathcal{X}$ is an infinite set) we say that $\mathcal{X}$ is an *infinite-dimensional linear space*.

Example 2.I. The *Kronecker delta* (or *Kronecker function*) is the mapping in $2^{\mathbb{Z}\times\mathbb{Z}}$ (i.e., the function from $\mathbb{Z}\times\mathbb{Z}$ to $\{0,1\}$) defined by

$$\delta_{ij} \;=\; \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$$

for all integers i, j. Now consider the linear space $\mathbb{F}^n$ (for an arbitrary positive integer n, over an arbitrary field $\mathbb{F}$ — see Example 2.D). The subset $B = \{e_i\}_{i=1}^n$ of $\mathbb{F}^n$ consisting of the n-tuples $e_i = (\delta_{i1}, \ldots, \delta_{in})$, with 1 at the ith position and zeros elsewhere, constitute a Hamel basis for $\mathbb{F}^n$. This is called the *canonical basis* (or the *natural basis*) for $\mathbb{F}^n$. Thus $\dim \mathbb{F}^n = n$. As we shall see later, $\mathbb{F}^n$ in fact is a prototype for every finite-dimensional linear space (of dimension n) over a field $\mathbb{F}$.

Example 2.J. Let $\mathbb{F}^{\mathbb{N}}$ be the linear space (over a field $\mathbb{F}$) of all scalar-valued sequences (see Example 2.E), and let $\mathcal{X}$ be the subset of $\mathbb{F}^{\mathbb{N}}$ defined as follows. $x = \{\xi_k\}_{k\in\mathbb{N}}$ belongs to $\mathcal{X}$ if and only if $\xi_k = 0$ except for some finite set of indices k in $\mathbb{N}$. That is, $\mathcal{X}$ is the set consisting of *all* $\mathbb{F}$*-valued sequences with a finite number of nonzero entries*, which clearly is a linear manifold of $\mathbb{F}^{\mathbb{N}}$, and hence a linear space itself over $\mathbb{F}$. For each integer $j \in \mathbb{N}$ let e_j be an $\mathbb{F}$-valued sequence with just one nonzero entry (equal to 1) at the jth position; that is, $e_j = \{\delta_{jk}\}_{k\in\mathbb{N}} \in \mathcal{X}$ for every $j \in \mathbb{N}$. Now set $B = \{e_j\}_{j\in\mathbb{N}} \subset \mathcal{X}$. It is readily verified that B is linearly independent and that $\operatorname{span} B = \mathcal{X}$ (every vector in $\mathcal{X}$ is a linear combination of vectors in B). Thus B is a Hamel basis for $\mathcal{X}$. Since B is countably infinite, $\mathcal{X}$ is an infinite-dimensional linear space with $\dim \mathcal{X} = \aleph_0$. Therefore (see Problem 2.6(b)), $\mathbb{F}^{\mathbb{N}}$ is an infinite-dimensional linear space. Note that B is not a Hamel basis for $\mathbb{F}^{\mathbb{N}}$ (reason: $\operatorname{span} B = \mathcal{X}$ and $\mathcal{X}$ is properly included in $\mathbb{F}^{\mathbb{N}}$). The next example shows that $\aleph_0 < \dim \mathbb{F}^{\mathbb{N}}$ whenever $\mathbb{F} = \mathbb{Q},\ \mathbb{F} = \mathbb{R}$, or $\mathbb{F} = \mathbb{C}$.

Example 2.K. Let $\mathbb{C}^{\mathbb{N}}$ be the complex linear space of all complex-valued sequences. For each real number $t \in (0,1)$ consider the real sequence $x_t = \{t^{k-1}\}_{k\in\mathbb{N}} = \{t^k\}_{k\in\mathbb{N}_0} = (1, t, t^2, \dots) \in \mathbb{C}^{\mathbb{N}}$ whose entries are the nonnegative powers of t. Set $A = \{x_t\}_{t\in(0,1)} \subseteq \mathbb{C}^{\mathbb{N}}$. We claim that A is linearly independent. A bit of elementary real analysis (rather than pure algebra) supplies a very simple proof as follows. Suppose A is not linearly independent. Then there exists $s \in (0,1)$ such that x_s is a linear combination of vectors in $A\backslash\{x_s\}$. That is, $x_s = \sum_{i=1}^n \alpha_i x_{t_i}$ for some $n \in \mathbb{N}$, where $\{\alpha_i\}_{i=1}^n$ is a family of nonzero complex numbers and $\{x_{t_i}\}_{i=1}^n$ is a (finite) subset of A such that $x_{t_i} \neq x_s$ for every $i = 1, \dots, n$. Hence $n > 1$ (reason: if $n = 1$, then $x_s = \alpha_1 x_{t_1}$ so that $s^k = \alpha_1 t_1^k$ for every $k \in \mathbb{N}_0$, which implies that $x_s = x_{t_1}$). As the set $\{t_i\}_{i=1}^n$ consists of distinct points from $(0,1)$, suppose it is decreasingly ordered (reorder it if necessary) so that $t_i < t_1$ for each $i = 2, \dots, n$. Since $s^k = \sum_{i=1}^n \alpha_i t_i^k$, we get $(s/t_1)^k = \alpha_1 + \sum_{i=2}^n \alpha_i (t_i/t_1)^k$ for every $k \in \mathbb{N}_0$. But $\lim_k \sum_{i=2}^n \alpha_i (t_i/t_1)^k = 0$, because each t_i/t_1 lies in $(0,1)$, and hence $\lim_k (s/t_1)^k = \alpha_1$. Thus $\alpha_1 = 0$ (recall: $x_s \neq x_{t_1}$ so that $s \neq t_1$) which is a contradiction. Conclusion: A is linearly independent. Therefore, by Theorem 2.5 there is a Hamel basis B for $\mathbb{C}^{\mathbb{N}}$ including A. Since $A \subseteq B$ and $\#A = \#(0,1) = 2^{\aleph_0}$, it follows that $2^{\aleph_0} \leq \#B$. However, $\#\mathbb{C} = \#\mathbb{R} = 2^{\aleph_0} \leq \#B = \dim \mathbb{C}^{\mathbb{N}}$, and so $\#\mathbb{C}^{\mathbb{N}} = \dim \mathbb{C}^{\mathbb{N}}$ (Problem 2.8). Conclusion: $\mathbb{C}^{\mathbb{N}}$ is an infinite-dimensional linear space such that

$$2^{\aleph_0} \;\leq\; \dim \mathbb{C}^{\mathbb{N}} \;=\; \#\mathbb{C}^{\mathbb{N}}.$$

Note that the whole argument does apply for $\mathbb{C}$ replaced by $\mathbb{R}$, so that

$$2^{\aleph_0} \;\leq\; \dim \mathbb{R}^{\mathbb{N}} \;=\; \#\mathbb{R}^{\mathbb{N}};$$

but it does not apply to the rational field $\mathbb{Q}$ (the interval $(0,1)$ is not a subset of $\mathbb{Q}$, and hence the set A is not included in $\mathbb{Q}^{\mathbb{N}}$). However, the final conclusion does hold for the linear space $\mathbb{Q}^{\mathbb{N}}$. Indeed, if $\mathbb{F}$ is an arbitrary infinite field, then $2^{\aleph_0} = \#2^{\mathbb{N}} \leq \#\mathbb{F}^{\mathbb{N}} = \max\{\#\mathbb{F}, \dim \mathbb{F}^{\mathbb{N}}\}$ according to Problems 1.24 and 2.8. Therefore, since $\#\mathbb{Q} = \aleph_0 < 2^{\aleph_0}$ (Problem 1.25(c)), it follows that

$$2^{\aleph_0} \;\leq\; \dim \mathbb{Q}^{\mathbb{N}} \;=\; \#\mathbb{Q}^{\mathbb{N}}.$$

2.5 Linear Transformations

A mapping $L\colon \mathcal{X} \to \mathcal{Y}$ of a linear space $\mathcal{X}$ over a field $\mathbb{F}$ into a linear space $\mathcal{Y}$ over the same field $\mathbb{F}$ is *homogeneous* if

$$L(\alpha x) \;=\; \alpha L x$$

for every vector $x \in \mathcal{X}$ and every scalar $\alpha \in \mathbb{F}$. The scalar multiplication on the left-hand side is an operation on $\mathcal{X}$ and that on the right-hand side is an operation on $\mathcal{Y}$ (so that the linear spaces $\mathcal{X}$ and $\mathcal{Y}$ must indeed be defined over the same field $\mathbb{F}$). L is *additive* if

$$L(x_1 + x_2) \;=\; L(x_1) + L(x_2)$$

for all vectors x_1, x_2 in $\mathcal{X}$. Again, the vector addition on the left-hand side is an operation on $\mathcal{X}$ while the one on the right-hand side is an operation on $\mathcal{Y}$. If $\mathcal{X}$ and $\mathcal{Y}$ are linear spaces over the same scalar field, and if L is a homogeneous and additive mapping of $\mathcal{X}$ into $\mathcal{Y}$, then L is a *linear transformation*: a linear transformation is a homogeneous and additive mapping between linear spaces over the same scalar field. When we say that $L\colon \mathcal{X} \to \mathcal{Y}$ is a linear transformation, it is implicitly assumed that $\mathcal{X}$ and $\mathcal{Y}$ are linear spaces over the same field $\mathbb{F}$. If $\mathcal{X} = \mathcal{Y}$ and $L\colon \mathcal{X} \to \mathcal{X}$ is a linear transformation, then we refer to L as a *linear transformation on* $\mathcal{X}$. Trivial example: The identity $I\colon \mathcal{X} \to \mathcal{X}$ (such that $I(x) = x$ for every $x \in \mathcal{X}$) is a linear transformation on $\mathcal{X}$. Recall that a field $\mathbb{F}$ can be made into a linear space over $\mathbb{F}$ itself (see Example 2.D). If $\mathcal{X}$ is a linear space over $\mathbb{F}$, then a linear transformation $f\colon \mathcal{X} \to \mathbb{F}$ is called a *linear functional*: a linear functional is a scalar-valued linear transformation (i.e., a linear transformation of a linear space $\mathcal{X}$ into its scalar field).

If $y \in \mathcal{Y}$ is the value of a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ at $x \in \mathcal{X}$, then we shall often write $y = Lx$ (instead of $y = L(x)$). Since $\mathcal{Y}$ is a linear space, it has an origin. The *null space* (or *kernel*) of a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ is the subset

$$\mathcal{N}(L) \;=\; \big\{x \in \mathcal{X}\colon\; Lx = 0\big\} \;=\; L^{-1}(\{0\})$$

of $\mathcal{X}$ consisting of all vectors in $\mathcal{X}$ mapped into the origin of $\mathcal{Y}$ by L. Since $\mathcal{X}$ also is a linear space, it has an origin too. The origin of $\mathcal{X}$ is always in $\mathcal{N}(L)$

(i.e., $L0 = 0$ for every linear transformation L). The *null transformation* (denoted by O) is the mapping $O\colon \mathcal{X} \to \mathcal{Y}$ such that $Ox = 0$ for every $x \in \mathcal{X}$, which certainly is a linear transformation. In fact, if $L\colon \mathcal{X} \to \mathcal{Y}$ is a linear transformation, then $L = O$ if and only if $\mathcal{N}(L) = \mathcal{X}$. Equivalently, $L = O$ if and only if $\mathcal{R}(L) = \{0\}$. The null space $\mathcal{N}(L) = L^{-1}(\{0\})$ of any linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ is a linear manifold of $\mathcal{X}$, and the range $\mathcal{R}(L) = L(\mathcal{X})$ of L is a linear manifold of $\mathcal{Y}$ (Problem 2.10(a)). These are indeed particular cases of Problem 2.11: *The linear image of a linear manifold is a linear manifold*, and *the inverse image of a linear manifold under a linear transformation is again a linear manifold.*

The theorem below supplies an elegant and useful, although very simple, necessary and sufficient condition that a linear transformation be injective.

Theorem 2.8. *A linear transformation L is injective if and only if $\mathcal{N}(L) = \{0\}$.*

Proof. Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over the same scalar field and consider a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$. If L is injective, then $L^{-1}(L(\{0\})) = \{0\}$ (see Problem 1.3(d)). But $L(\{0\}) = \{0\}$ (since $L0 = 0$) so that $L^{-1}(\{0\}) = \{0\}$, which means $\mathcal{N}(L) = \{0\}$. On the other hand, suppose $\mathcal{N}(L) = \{0\}$. Take x_1 and x_2 arbitrary in $\mathcal{X}$, and note that $Lx_1 - Lx_2 = L(x_1 - x_2)$ since L is linear. Thus, if $Lx_1 = Lx_2$, then $L(x_1 - x_2) = 0$ and hence $x_1 = x_2$ (i.e., $x_1 - x_2 = 0$ because $\mathcal{N}(L) = \{0\}$). Therefore L is injective. $\square$

The collection $\mathcal{Y}^S$ of all mappings of a set S into a linear space $\mathcal{Y}$ over a field $\mathbb{F}$ is itself a linear space over $\mathbb{F}$ (see Example 2.F). Now suppose $\mathcal{X}$ is a linear space (over the same field $\mathbb{F}$) and let $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ denote the collection of all linear transformations of $\mathcal{X}$ into $\mathcal{Y}$. Since $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is a linear manifold of $\mathcal{Y}^{\mathcal{X}}$, it follows that $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is a linear space over the same field $\mathbb{F}$ (see Problem 2.13). Set $\mathcal{L}[\mathcal{X}] = \mathcal{L}[\mathcal{X}, \mathcal{X}]$ for short so that $\mathcal{L}[\mathcal{X}] \subset \mathcal{X}^{\mathcal{X}}$ is the linear space of all linear transformations on $\mathcal{X}$. The linear space $\mathcal{L}[\mathcal{X}, \mathbb{F}]$ of all linear functionals defined on a linear space $\mathcal{X}$, which is a linear manifold of the linear space $\mathbb{F}^{\mathcal{X}}$ (see Example 2.E), is called the *algebraic dual* (or *algebraic conjugate*) of $\mathcal{X}$ and is denoted by $\mathcal{X}'$. (Dual spaces will be considered in Chapter 4.)

Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over the same scalar field. Let $L|_{\mathcal{M}}\colon \mathcal{M} \to \mathcal{Y}$ be the restriction of a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ to a linear manifold $\mathcal{M}$ of $\mathcal{X}$. Since $\mathcal{M}$ is a linear space, it is easy to show that $L|_{\mathcal{M}}$ is a linear transformation: *The restriction of a linear transformation to a linear manifold is again a linear transformation* (Problem 2.14). The next result ensures the converse: If $\mathcal{M}$ is a linear manifold of $\mathcal{X}$ and $L \in \mathcal{L}[\mathcal{M}, \mathcal{Y}]$, then there exists $T \in \mathcal{L}[\mathcal{X}, \mathcal{Y}]$ such that $L = T|_{\mathcal{M}}$. T is called a *linear extension* of L over $\mathcal{X}$.

Theorem 2.9. *Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over the same field $\mathbb{F}$, and let $\mathcal{M}$ be a linear manifold of $\mathcal{X}$. If $L\colon \mathcal{M} \to \mathcal{Y}$ is a linear transformation, then there exists a linear extension $T\colon \mathcal{X} \to \mathcal{Y}$ of L defined on the whole space $\mathcal{X}$.*

Proof. Set

$$\mathcal{K} = \big\{K \in \mathcal{L}[\mathcal{N},\mathcal{Y}]:\ \mathcal{N} \in \mathcal{L}at(\mathcal{X}),\, \mathcal{M} \subseteq \mathcal{N} \text{ and } L = K|_{\mathcal{M}}\big\},$$

the collection of all linear transformations from linear manifolds of $\mathcal{X}$ to $\mathcal{Y}$ which are extensions of L. Note that $\mathcal{K}$ is nonempty (at least L is there). Moreover, as a subcollection of $\mathcal{F} = \bigcup_{A\in\wp(\mathcal{X})}\mathcal{Y}^A$, $\mathcal{K}$ is partially ordered in the extension ordering (see Problem 1.17). Problem 1.17 also tells us that every chain $\{K_\gamma\}$ in $\mathcal{K}$ has a supremum $\bigvee_\gamma K_\gamma$ in $\mathcal{F}$ with domain $\mathcal{D}\big(\bigvee_\gamma K_\gamma\big) = \bigcup_\gamma \mathcal{D}(K_\gamma)$ and range $\mathcal{R}\big(\bigvee_\gamma K_\gamma\big) = \bigcup_\gamma \mathcal{R}(K_\gamma)$. Since $\mathcal{D}(K_\gamma) \in \mathcal{L}at(\mathcal{X})$ (each K_γ is a linear transformation defined on a linear manifold of $\mathcal{X}$), and since $\mathcal{L}at(\mathcal{X})$ is a complete lattice, it follows that $\mathcal{D}\big(\bigvee_\gamma K_\gamma\big)$ is a linear manifold of $\mathcal{X}$ (i.e., $\bigcup_\gamma \mathcal{D}(K_\gamma) \in \mathcal{L}at(\mathcal{X})$). Similarly, $\mathcal{R}\big(\bigvee_\gamma K_\gamma\big)$ is a linear manifold of $\mathcal{Y}$.

Claim. The supremum $\bigvee_\gamma K_\gamma$ lies in $\mathcal{K}$.

Proof. Take u and v arbitrary in $\mathcal{D}\big(\bigvee_\gamma K_\gamma\big)$, so that $u \in \mathcal{D}(K_\lambda)$ for some $K_\lambda \in \{K_\gamma\}$ and $v \in \mathcal{D}(K_\mu)$ for some $K_\mu \in \{K_\gamma\}$. Since $\{K_\gamma\}$ is a chain, it follows that $K_\lambda \le K_\mu$ (or vice versa), so that $\mathcal{D}(K_\lambda) \subseteq \mathcal{D}(K_\mu)$. Thus $\alpha u + \beta v \in D(K_\mu)$ and hence $K_\mu(\alpha u + \beta v) = \alpha K_\mu u + \beta K_\mu v$ for every $\alpha, \beta \in \mathbb{F}$ (recall: each K_γ is linear). However $\big(\bigvee_\gamma K_\gamma\big)|_{\mathcal{D}(K_\mu)} = K_\mu$, which implies that $\big(\bigvee_\gamma K_\gamma\big)(\alpha u + \beta v) = \alpha\big(\bigvee_\gamma K_\gamma\big)u + \beta\big(\bigvee_\gamma K_\gamma\big)v$. That is, $\bigvee_\gamma K_\gamma\colon \mathcal{D}\big(\bigvee_\gamma K_\gamma\big) \to \mathcal{Y}$ is linear. Moreover, since each K_γ is such that $K_\gamma|_{\mathcal{M}} = L$, and since $\{K_\gamma\}$ is a chain, it follows that $\big(\bigvee_\gamma K_\gamma\big)|_{\mathcal{M}} = L$. Conclusion: $\bigvee_\gamma K_\gamma \in \mathcal{K}$. $\square$

Therefore, every chain in $\mathcal{K}$ has a supremum (and so an upper bound) in $\mathcal{K}$. Thus, according to Zorn's Lemma, $\mathcal{K}$ contains a maximal element, say $K_0\colon \mathcal{N}_0 \to \mathcal{Y}$. We shall show that $\mathcal{N}_0 = \mathcal{X}$, and hence K_0 is a linear extension of L over $\mathcal{X}$. The proof goes by contradiction. Suppose $\mathcal{N}_0 \ne \mathcal{X}$. Take $x_1 \in \mathcal{X}\backslash\mathcal{N}_0$ (so that $x_1 \ne 0$ because $\mathcal{N}_0$ is a linear manifold of $\mathcal{X}$) and consider the sum of $\mathcal{N}_0$ and the one-dimensional linear manifold of $\mathcal{X}$ spanned by $\{x_1\}$,

$$\mathcal{N}_1 = \mathcal{N}_0 + \operatorname{span}\{x_1\},$$

which is a linear manifold of $\mathcal{X}$ properly including $\mathcal{M}$ (because $\mathcal{M} \subseteq \mathcal{N}_0 \subset \mathcal{N}_1$). Since $\mathcal{N}_0 \cap \operatorname{span}\{x_1\} = \{0\}$, it follows that every x in $\mathcal{N}_1$ has a unique representation as a sum of a vector in $\mathcal{N}_0$ and a vector in $\operatorname{span}\{x_1\}$. That is, for each $x \in \mathcal{N}_1$ there is a unique pair (x_0, α) in $\mathcal{N}_0 \times \mathbb{F}$ such that $x = x_0 + \alpha x_1$. (Indeed, if $x = x_0 + \alpha x_1 = x_0' + \alpha' x_1$, then $x_0 - x_0' = (\alpha' - \alpha)x_1$ lies in $\mathcal{N}_0 \cap \operatorname{span}\{x_1\} = \{0\}$ so that $x_0' = x_0$ and $\alpha' = \alpha$ — recall: $x_1 \ne 0$.) Take any y in $\mathcal{Y}$ (e.g., $y = 0$) and consider the mapping $K_1\colon \mathcal{N}_1 \to \mathcal{Y}$ defined by

$$K_1 x = K_0 x_0 + \alpha y$$

for every $x \in \mathcal{N}_1$. Observe that K_1 is linear (it inherits the linearity of K_0) and $K_0 = K_1|_{\mathcal{N}_0}$ (so that $K_0 \le K_1$). Since $\mathcal{M} \subseteq \mathcal{N}_0 \subset \mathcal{N}_1$, it follows that

$L = K_0|_{\mathcal{M}} = K_1|_{\mathcal{M}}$. Thus $K_1 \in \mathcal{K}$, which contradicts the fact that K_0 is maximal in $\mathcal{K}$ (for $K_0 \neq K_1$). Therefore, $\mathcal{N}_0 = \mathcal{X}$. □

Let $\mathcal{X}$ and $\mathcal{Y}$ be nonzero linear spaces over the same field. Take $x \neq 0$ in $\mathcal{X}$ and $y \neq 0$ in $\mathcal{Y}$, set $\mathcal{M} = \operatorname{span}\{x\}$ in $\mathcal{L}at(\mathcal{X})$, and let $L\colon \mathcal{M} \to \mathcal{Y}$ be defined by $Lu = \alpha y$ for every $u = \alpha x \in \mathcal{M}$. Clearly, L is linear and $L \neq O$. Thus Theorem 2.9 ensures that, *if $\mathcal{X}$ and $\mathcal{Y}$ are nonzero linear spaces over the same field, then there exist many $T \neq O$ in $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$* (at least as many as one-dimensional linear manifolds in $\mathcal{L}at(\mathcal{X})$).

2.6 Isomorphisms

Two exemplars of a mathematical structure are indistinguishable, in the context of the theory in which that structure is embedded, if there exists a one-to-one correspondence between them that preserves such a structure. This is a central concept in mathematics. From the point of view of the linear space theory, two linear spaces are essentially the same if there exists a one-to-one correspondence between them that preserves all the linear relations — they may differ in the set-theoretic nature of their elements but, as far as the linear space (algebraic) structure is concerned, they are indistinguishable. In other words, two linear spaces $\mathcal{X}$ and $\mathcal{Y}$ over the same scalar field are regarded as essentially the same linear space if there exists a one-to-one correspondence between them that preserves vector addition and scalar multiplication; that is, if there exists at least one invertible linear transformation from $\mathcal{X}$ to $\mathcal{Y}$ whose inverse from $\mathcal{Y}$ to $\mathcal{X}$ also is linear. The theorem below shows that the inverse of an invertible linear transformation is always linear.

Theorem 2.10. *Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over the same field $\mathbb{F}$. If $L\colon \mathcal{X} \to \mathcal{Y}$ is an invertible linear transformation, then its inverse $L^{-1}\colon \mathcal{Y} \to \mathcal{X}$ is a linear transformation.*

Proof. Suppose $L\colon \mathcal{X} \to \mathcal{Y}$ is an invertible linear transformation. Recall that a function is invertible if it is injective and surjective. Take y_1 and y_2 arbitrary in $\mathcal{Y}$ so that there exist x_1 and x_2 in $\mathcal{X}$ such that $y_1 = Lx_1$ and $y_2 = Lx_2$ (because $\mathcal{Y} = \mathcal{R}(L)$ — i.e., L is surjective). Since L is injective (i.e., $L^{-1}L$ is the identity on $\mathcal{X}$ — see Problems 1.5 and 1.7) and additive, it follows that

$$\begin{aligned} L^{-1}(y_1 + y_2) &= L^{-1}(Lx_1 + Lx_2) = L^{-1}L(x_1 + x_2) = x_1 + x_2 \\ &= L^{-1}Lx_1 + L^{-1}Lx_2 = L^{-1}y_1 + L^{-1}y_2, \end{aligned}$$

and hence L^{-1} is additive. Similarly, since L is injective and homogeneous,

$$L^{-1}(\alpha y) = L^{-1}(\alpha Lx) = L^{-1}L(\alpha x) = \alpha x = \alpha L^{-1}Lx = \alpha L^{-1}y$$

for every $y \in \mathcal{Y} = \mathcal{R}(L)$ and every $\alpha \in \mathbb{F}$, which implies that L^{-1} is homogeneous. Thus L^{-1} is a linear transformation. □

An *isomorphism* between linear spaces (over the same scalar field) is an injective and surjective linear transformation. Equivalently, an *isomorphism* between linear spaces is an invertible linear transformation. Two linear spaces $\mathcal{X}$ and $\mathcal{Y}$ over the same field $\mathbb{F}$ are *isomorphic* if there exists an isomorphism (i.e., a linear one-to-one correspondence) of $\mathcal{X}$ onto $\mathcal{Y}$. Thus, according to Theorem 2.8, a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ of a linear space $\mathcal{X}$ into a linear space $\mathcal{Y}$ is an isomorphism if and only if $\mathcal{N}(L) = \{0\}$ and $\mathcal{R}(L) = \mathcal{Y}$. In particular, if $\mathcal{N}(L) = \{0\}$, then $\mathcal{X}$ and the range of L ($\mathcal{R}(L) = L(\mathcal{X})$) are isomorphic linear spaces.

We noticed in Example 2.I that $\mathbb{F}^n$ is a "prototype" for every n-dimensional linear space over $\mathbb{F}$. What this really means is that every n-dimensional linear space over a field $\mathbb{F}$ is *isomorphic* to $\mathbb{F}^n$, and hence two n-dimensional linear spaces over the same scalar field are isomorphic. In fact, such an isomorphism between linear spaces with the same dimension holds in general, either for finite-dimensional or for infinite-dimensional linear spaces. We shall prove this below (Theorem 2.12), but first we need the following auxiliary result.

Proposition 2.11. *Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over the same field, and let B be a Hamel basis for $\mathcal{X}$. For each mapping $F\colon B \to \mathcal{Y}$ there exists a unique linear transformation $T\colon \mathcal{X} \to \mathcal{Y}$ such that $T|_B = F$.*

Proof. If $B = \{x_\gamma\}_{\gamma\in\Gamma}$ is a Hamel basis for $\mathcal{X}$, indexed by an index set Γ (recall: any set can be thought of as an indexed set), then every vector x in $\mathcal{X}$ has a unique expansion on B, viz.,

$$x = \sum_{\gamma\in\Gamma} \alpha_\gamma x_\gamma,$$

where $\{\alpha_\gamma\}_{\gamma\in\Gamma}$ is a similarly indexed family of scalars with $\alpha_\gamma = 0$ for all but a finite set of indices γ (the coordinates of x with respect to the basis B). Set

$$Tx = \sum_{\gamma\in\Gamma} \alpha_\gamma F(x_\gamma)$$

for every $x \in \mathcal{X}$. This defines a mapping $T\colon \mathcal{X} \to \mathcal{Y}$ of $\mathcal{X}$ into $\mathcal{Y}$ which is homogeneous, additive, and equals F when restricted to B. That is, T is a linear transformation such that $T|_B = F$. Moreover, if $L\colon \mathcal{X} \to \mathcal{Y}$ is a linear transformation of $\mathcal{X}$ into $\mathcal{Y}$ such that $L|_B = F$, then $L = T$. Indeed, for every $x \in \mathcal{X}$,

$$Lx = L\Big(\sum_{\gamma\in\Gamma} \alpha_\gamma x_\gamma\Big) = \sum_{\gamma\in\Gamma} \alpha_\gamma F(x_\gamma) = T\Big(\sum_{\gamma\in\Gamma} \alpha_\gamma x_\gamma\Big) = Tx. \qquad \square$$

Theorem 2.12. *Two linear spaces $\mathcal{X}$ and $\mathcal{Y}$ over the same scalar field are isomorphic if and only if* $\dim \mathcal{X} = \dim \mathcal{Y}$.

Proof. (a) Let $L\colon \mathcal{X} \to \mathcal{Y}$ be an isomorphism of $\mathcal{X}$ onto $\mathcal{Y}$, and let B_X be a Hamel basis for $\mathcal{X}$. Set $B_Y = L(B_X)$, a subset of $\mathcal{Y}$.

Claim 1. B_Y is linearly independent.

Proof. Recall that L is an injective and surjective linear transformation. If B_Y is not linearly independent, then there exists $y \in B_Y$, which is a linear combination of vectors in $B_Y \backslash \{y\}$, say $y = \sum_{i=1}^n \alpha_i y_i$ where each y_i is a vector in $B_Y \backslash \{y\}$. Thus $x = L^{-1} y$ in $B_X = L^{-1}(B_Y)$ is a linear combination of vectors in $B_X \backslash \{x\}$. (Indeed, $x = \sum_{i=1}^n \alpha_i x_i$ where each $x_i = L^{-1} y_i$ is a vector in $B_X = L^{-1}(B_Y)$ different from $x = L^{-1} y$ — recall: each y_i is a vector in B_Y different from y, and L is injective.) But this contradicts the fact that B_X is linearly independent. Conclusion: B_Y is linearly independent. □

Claim 2. B_Y spans $\mathcal{Y}$.

Proof. Take $y \in \mathcal{Y}$ arbitrary so that $y = Lx$ for some $x \in \mathcal{X}$ (because L is surjective). Since $\operatorname{span} B_X = \mathcal{X}$, it follows that x is a linear combination of vectors in B_X. Hence $y = Lx$ is a linear combination of vectors in $B_Y = L(B_X)$ (since L is linear) so that $\operatorname{span} B_Y = \mathcal{Y}$. □

Therefore, B_Y is a Hamel basis for $\mathcal{Y}$. Moreover, $\# B_Y = \# B_X$ because L sets a one-to-one correspondence between B_X and B_Y. (In fact, the restriction $L|_{B_X} \colon B_X \to B_Y$ is injective and surjective, since L is injective and $B_Y = L(B_X)$ by definition.) Thus $\dim \mathcal{X} = \dim \mathcal{Y}$.

(b) Let B_X and B_Y be Hamel bases for $\mathcal{X}$ and $\mathcal{Y}$, respectively. If $\dim \mathcal{X} = \dim \mathcal{Y}$, then $\# B_Y = \# B_X$, which means that there exists a one-to-one mapping $F \colon B_X \to B_Y$ of B_X onto B_Y. Let $T \colon \mathcal{X} \to \mathcal{Y}$ be the unique linear transformation such that $T|_{B_X} = F$ (see Proposition 2.11), and hence $T(B_X) = F(B_X) = B_Y$.

Claim 3. T is injective.

Proof. If $\mathcal{X} = \{0\}$, then the result holds trivially. Thus suppose $\mathcal{X} \neq \{0\}$. Take any nonzero vector x in $\mathcal{X}$ and consider its (unique) representation as a linear combination of vectors in B_X. Therefore, Tx has a representation as a linear combination of vectors in $B_Y = T(B_X)$ because T is linear. Since B_Y is linearly independent, it follows that $Tx \neq 0$. That is, $\mathcal{N}(T) = \{0\}$ which means, by Theorem 2.8, that T is injective. □

Claim 4. T is surjective.

Proof. Take an arbitrary vector $y \in \mathcal{Y}$ and consider its expansion on B_Y, say $y = \sum_{i=1}^n \alpha_i y_i$ with each y_i in B_Y. Thus $y = \sum_{i=1}^n \alpha_i T(x_i)$ with each x_i in B_X because $B_Y = T(B_X)$. But T is linear so that $y = T\big(\sum_{i=1}^n \alpha_i x_i\big)$, where $\sum_{i=1}^n \alpha_i x_i$ is a vector in $\mathcal{X}$ (since $\mathcal{X}$ is a linear space). Hence $y \in \mathcal{R}(T)$. □

Therefore, $T \colon \mathcal{X} \to \mathcal{Y}$ is an isomorphism of $\mathcal{X}$ onto $\mathcal{Y}$. □

Example 2.L. Let $\mathcal{X}$ and $\mathcal{Y}$ be *finite-dimensional* linear spaces over the same field $\mathbb{F}$, with $\dim \mathcal{X} = n$ and $\dim \mathcal{Y} = m$. Let $B_X = \{x_j\}_{j=1}^n$ and $B_Y = \{y_i\}_{i=1}^m$ be Hamel bases for $\mathcal{X}$ and $\mathcal{Y}$, respectively. Take an arbitrary vector x in $\mathcal{X}$ and consider its unique expansion on B_X,

$$x = \sum_{j=1}^{n} \xi_j x_j,$$

where the family of scalars $\{\xi_j\}_{j=1}^n$ consists of the coordinates of x with respect to B_X. Now let $A\colon \mathcal{X} \to \mathcal{Y}$ be any linear transformation so that

$$Ax = \sum_{j=1}^{n} \xi_j Ax_j,$$

where Ax_j is a vector in $\mathcal{Y}$ for each j. Consider its unique expansion on B_Y,

$$Ax_j = \sum_{i=1}^{m} \alpha_{ij} y_i,$$

where $\{\alpha_{ij}\}_{i=1}^m$ is a family of scalars (the coordinates of each Ax_j with respect to B_Y). Set $y = Ax$ in $\mathcal{Y}$ and consider the unique expansion of y on B_Y,

$$y = \sum_{i=1}^{m} \upsilon_i y_i.$$

Again, $\{\upsilon_i\}_{i=1}^m$ is a family of scalars consisting of the coordinates of y with respect to B_Y. Thus the identity $y = Ax$ can be written as

$$\sum_{i=1}^{m} \upsilon_i y_i = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n} \xi_j \alpha_{ij} \Big) y_i.$$

Since the expansion of y on B_Y is unique, it follows that

$$\upsilon_i = \sum_{j=1}^{n} \alpha_{ij} \xi_j$$

for every $i = 1, \ldots, m$. This gives an expression for each coordinate of Ax as a function of the coordinates of x. In terms of standard matrix notation, and according to the ordinary matrix operations, the matrix equation

$$\begin{pmatrix} \upsilon_1 \\ \vdots \\ \upsilon_m \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

represents the identity $y = Ax$ (the vector y is the value of the linear transformation A at the point x), and the $m \times n$ array of scalars

$$[A] = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{pmatrix}$$

is the *matrix* that represents the linear transformation $A: \mathcal{X} \to \mathcal{Y}$ with respect to the bases B_X and B_Y. The matrix $[A]$ of a linear transformation A depends on the bases B_X and B_Y. If the bases are changed, then the matrix that represents the linear transformation may change as well. Different matrices representing the same linear transformation are simply different representations of it with respect to different bases. However, for fixed bases B_X and B_Y the representation $[A]$ of A is unique. Uniqueness is not all. It is easy to show that

(a) the set $\mathbb{F}_{m\times n}$ of all $m\times n$ matrices with entries in $\mathbb{F}$ is a linear space over $\mathbb{F}$ when equipped with the ordinary (entrywise) operations of matrix addition and scalar multiplication.

Moreover, for fixed bases B_X and B_Y,

(b) $\mathbb{F}_{m\times n}$ is isomorphic to $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$.

Indeed, if we fix the bases B_X and B_Y, then the relation between $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ and $\mathbb{F}_{m\times n}$ defined by "$[A]$ represents A with respect to B_X and B_Y" in fact is a function from $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ to $\mathbb{F}_{m\times n}$. It is readily verified that such a function, say $\Phi: \mathcal{L}[\mathcal{X}, \mathcal{Y}] \to \mathbb{F}_{m\times n}$, is homogeneous, additive, injective, and surjective. In other words, Φ is an isomorphism. For this reason we may and shall identify a linear transformation $A \in \mathcal{L}[\mathbb{F}^n, \mathbb{F}^m]$ with its matrix $[A] \in \mathbb{F}_{m\times n}$ relative to the *canonical* bases for $\mathbb{F}^n$ and $\mathbb{F}^m$ (which were introduced in Example 2.I).

Example 2.M. Let $\mathbb{F}$ denote either the real field or the complex field. For every nonnegative integer n let $\mathcal{P}_n[0,1]$ be the collection of all polynomials in the variable $t \in [0,1]$ with coefficients in $\mathbb{F}$ of degree not greater than n:

$$\mathcal{P}_n[0,1] \,=\, \big\{p \in \mathbb{F}^{[0,1]}\colon\, p(t) = \textstyle\sum_{i=0}^{n} \alpha_i t^i,\ t \in [0,1], \text{ with each } \alpha_i \text{ in } \mathbb{F}\big\}.$$

Recall that the degree of a nonzero polynomial p is m if $p(t) = \sum_{i=0}^{m} \alpha_i t^i$ with $\alpha_m \neq 0$ (e.g., the degree of a constant polynomial is zero), and the degree of the zero polynomial is undefined (thus not greater than any $n \in \mathbb{N}_0$). It is readily verified that $\mathcal{P}_n[0,1]$ is a linear manifold of the linear space $\mathbb{F}^{[0,1]}$ (see Example 2.E), and hence a linear space over $\mathbb{F}$. Now consider the mapping $L: \mathbb{F}^{n+1} \to \mathcal{P}_n[0,1]$ defined as follows. For each $x = (\xi_0, \ldots, \xi_n) \in \mathbb{F}^{n+1}$ let $p = Lx$ in $\mathcal{P}_n[0,1]$ be given by

$$p(t) \,=\, \sum_{i=0}^{n} \xi_i t^i$$

for every $t \in [0,1]$. It is easy to show that L is a linear transformation. Moreover, $\mathcal{N}(L) = \{0\}$ (i.e., if $p(t) = \sum_{i=0}^{n} \xi_i t^i = 0$ for every $t \in [0,1]$, then $x = (\xi_0, \ldots, \xi_n) = 0$ — a nonzero polynomial has only a finite number of zeros) so that L is injective (see Theorem 2.8). Furthermore, every polynomial p in $\mathcal{P}_n[0,1]$ is of the form $p(t) = \sum_{i=0}^{n} \xi_i t^i$ for some $x = (\xi_0, \ldots, \xi_n)$ in $\mathbb{F}^{n+1}$, which means that $\mathcal{P}_n[0,1] \subseteq \mathcal{R}(L)$. Hence $\mathcal{P}_n[0,1] = \mathcal{R}(L)$; that is, L is also surjective. Therefore, the linear transformation L is an isomorphism between the linear spaces $\mathbb{F}^{n+1}$ and $\mathcal{P}_n[0,1]$. Thus, since $\dim \mathbb{F}^{n+1} = n+1$ (see Example 2.I), it follows by Theorem 2.12 that

$$\dim \mathcal{P}_n[0,1] \,=\, n+1.$$

Next consider the collection $\mathcal{P}[0,1]$ of all polynomials in the variable $t \in [0,1]$ with coefficients in $\mathbb{F}$ of any degree:

$$\mathcal{P}[0,1] \,=\, \bigcup_{n\in\mathbb{N}_0} \mathcal{P}_n[0,1].$$

Note that $\mathcal{P}[0,1]$ contains the zero polynomial together with every polynomial of finite degree. It is again readily verified that, as a linear manifold of $\mathbb{F}^{[0,1]}$, $\mathcal{P}[0,1]$ is itself a linear space over $\mathbb{F}$. The functions $p_j\colon [0,1] \to \mathbb{F}$, defined by $p_j(t) = t^j$ for every $t \in [0,1]$, clearly belong to $\mathcal{P}[0,1]$ for each $j \in \mathbb{N}_0$. Consider the set $B = \{p_j\}_{j\in\mathbb{N}_0} \subset \mathcal{P}[0,1]$. Since any polynomial in $\mathcal{P}[0,1]$ is, by definition, a (finite) linear combination of vectors in B, we get $\mathcal{P}[0,1] \subseteq \operatorname{span} B$. Hence B spans $\mathcal{P}[0,1]$ (i.e., $\operatorname{span} B = \mathcal{P}[0,1]$). We claim that B is also linearly independent. Indeed, suppose B is not linearly independent. Then there exists in B a linear combination p_k of vectors in $B\backslash\{p_k\}$. That is, $p_k = \sum_{i=1}^m \alpha_i p_{j_i}$ for some $m \in \mathbb{N}$, where $\{\alpha_i\}_{i=1}^m$ is a family of nonzero scalars and $\{p_{j_i}\}_{i=1}^m$ is a finite subset of B such that $p_{j_i} \neq p_k$ (i.e., $j_i \neq k$) for every $i = 1, \ldots, m$. Thus $p = p_k - \sum_{i=1}^m \alpha_i p_{j_i}$ is the origin of $\mathcal{P}[0,1]$, which means that

$$p(t) \,=\, t^k - \sum_{i=1}^m \alpha_i t^{j_i} \,=\, 0$$

for all $t \in [0,1]$. But this is a contradiction because p is a polynomial of degree equal to $\max\big\{\{k\} \cup \{j_i\}_{i=1}^m\big\} \geq 1$. Conclusion: B is linearly independent. Therefore the set $B = \{p_j\}_{j\in\mathbb{N}_0}$ is a Hamel basis for $\mathcal{P}[0,1]$, and hence

$$\dim \mathcal{P}[0,1] \,=\, \aleph_0$$

(since $\#B = \#\mathbb{N}_0 = \aleph_0$). Thus $\mathcal{P}[0,1]$ is isomorphic to the linear space $\mathcal{X}$ of all $\mathbb{F}$-valued sequences with a finite number of nonzero entries (which was introduced in Example 2.J).

2.7 Isomorphic Equivalence

Two linear spaces over the same scalar field are regarded as essentially the same linear space if they are isomorphic. Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be linear spaces over the same field $\mathbb{F}$. It is clear that $\mathcal{X}$ is isomorphic to itself (reflexivity), and $\mathcal{Y}$ is isomorphic to $\mathcal{X}$ whenever $\mathcal{X}$ is isomorphic to $\mathcal{Y}$ (symmetry). Moreover, since the composition of two isomorphisms is again an isomorphism (see Problems 1.9(c) and 2.15), it follows that, if $\mathcal{X}$ is isomorphic to $\mathcal{Y}$ and $\mathcal{Y}$ is isomorphic to

$\mathcal{Z}$, then $\mathcal{X}$ is isomorphic to $\mathcal{Z}$ (transitivity). Thus, if the notion of isomorphic linear spaces is restricted to a given set (for instance, to the collection of all linear manifolds $\mathcal{L}at(\mathcal{X})$ of a linear space $\mathcal{X}$), then it is an equivalence relation on that set. We shall now define an equivalence between linear transformations. As usual, let $GF\colon \mathcal{X} \to \mathcal{Z}$ denote the composition $G \circ F$ of a mapping $G\colon \mathcal{Y} \to \mathcal{Z}$ and a mapping $F\colon \mathcal{X} \to \mathcal{Y}$.

Definition 2.13. Let $\mathcal{X}$, $\widetilde{\mathcal{X}}$, $\mathcal{Y}$, and $\widetilde{\mathcal{Y}}$ be linear spaces over the same scalar field, where $\mathcal{X}$ is isomorphic to $\widetilde{\mathcal{X}}$ and $\mathcal{Y}$ is isomorphic to $\widetilde{\mathcal{Y}}$. Two linear transformations $T\colon \mathcal{X} \to \mathcal{Y}$ and $L\colon \widetilde{\mathcal{X}} \to \widetilde{\mathcal{Y}}$ are *isomorphically equivalent* if there exist isomorphisms $X\colon \mathcal{X} \to \widetilde{\mathcal{X}}$ and $Y\colon \mathcal{Y} \to \widetilde{\mathcal{Y}}$ such that

$$YT = LX.$$

That is, L and T are isomorphically equivalent if there are isomorphisms X and Y such that $T = Y^{-1}LX$ (or $L = YTX^{-1}$), which means that the diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\;T\;} & \mathcal{Y} \\ {\scriptstyle X}\big\downarrow & & \big\uparrow{\scriptstyle Y^{-1}} \\ \widetilde{\mathcal{X}} & \xrightarrow{\;L\;} & \widetilde{\mathcal{Y}} \end{array}$$

commutes. *Warning*: If $\mathcal{X}$ is isomorphic to $\widetilde{\mathcal{X}}$ and $\mathcal{Y}$ is isomorphic to $\widetilde{\mathcal{Y}}$, then there exists an uncountable supply of isomorphisms between $\mathcal{X}$ and $\widetilde{\mathcal{X}}$ and between $\mathcal{Y}$ and $\widetilde{\mathcal{Y}}$. If we take arbitrary linear transformations $T\colon \mathcal{X} \to \mathcal{Y}$ and $L\colon \widetilde{\mathcal{X}} \to \widetilde{\mathcal{Y}}$, it may happen that the above diagram does not commute (i.e., it may happen that $YT \neq LX$) for all isomorphisms of $\mathcal{X}$ onto $\widetilde{\mathcal{X}}$ and all isomorphisms of $\mathcal{Y}$ onto $\widetilde{\mathcal{Y}}$. In this case T and L are not isomorphically equivalent. However, if there exists at least one pair of isomorphisms X and Y for which $YT = LX$, then T and L are isomorphically equivalent.

Isomorphic equivalence deserves its name. In fact, every T in $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is isomorphically equivalent to itself (reflexivity), and L in $L[\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}]$ is isomorphically equivalent to T in $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ whenever T is isomorphically equivalent to L (symmetry). Moreover, if T in $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is isomorphically equivalent to L in $\mathcal{L}[\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}]$ and L is isomorphically equivalent to K in $\mathcal{L}[\widehat{\mathcal{X}}, \widehat{\mathcal{Y}}]$ (so that $\mathcal{X}$, $\widetilde{\mathcal{X}}$, and $\widehat{\mathcal{X}}$ are isomorphic linear spaces, as well as $\mathcal{Y}$, $\widetilde{\mathcal{Y}}$, and $\widehat{\mathcal{Y}}$), then it is easy to show that T is isomorphically equivalent to K (transitivity). Indeed, if $\mathcal{X} = \widetilde{\mathcal{X}}$ and $\mathcal{Y} = \widetilde{\mathcal{Y}}$, and if we restrict the concept of isomorphic equivalence to the set $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ of all linear transformations of $\mathcal{X}$ into $\mathcal{Y}$, then isomorphic equivalence actually is an equivalence relation on $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$.

An important particular case is obtained when $\mathcal{X} = \mathcal{Y}$ and $\widetilde{\mathcal{X}} = \widetilde{\mathcal{Y}}$ so that T lies in $\mathcal{L}[\mathcal{X}]$ and L lies in $\mathcal{L}[\widetilde{\mathcal{X}}]$. Let $\mathcal{X}$ and $\widetilde{\mathcal{X}}$ be isomorphic linear spaces. Two linear transformations $T\colon \mathcal{X} \to \mathcal{X}$ and $L\colon \widetilde{\mathcal{X}} \to \widetilde{\mathcal{X}}$ are *similar* if there exists an isomorphism $W\colon \mathcal{X} \to \widetilde{\mathcal{X}}$ such that

$$WT = LW.$$

To put it another way, if there is an isomorphism W such that the diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{T} & \mathcal{X} \\ {\scriptstyle W}\downarrow & & \downarrow{\scriptstyle W} \\ \widetilde{\mathcal{X}} & \xrightarrow{L} & \widetilde{\mathcal{X}} \end{array}$$

commutes. It should be noticed now that the concept of similarity will be redefined later in Chapter 4 where the linear spaces are endowed with an additional (topological) structure. Such a redefinition will assume that all linear transformations involved in the definition of similarity are "continuous" (including the inverse of W).

Example 2.N. Consider the setup of Example 2.L, where $\mathcal{X}$ and $\mathcal{Y}$ are *finite-dimensional* linear spaces over the same field $\mathbb{F}$. Let $X\colon\mathcal{X}\to\mathbb{F}^n$ and $Y\colon\mathcal{Y}\to\mathbb{F}^m$ be two mappings defined by

$$Xx = (\xi_1,\ldots,\xi_n) \quad \text{and} \quad Yy = (\upsilon_1,\ldots,\upsilon_m)$$

for every $x\in\mathcal{X}$ and every $y\in\mathcal{Y}$, where $\{\xi_j\}_{j=1}^n$ and $\{\upsilon_i\}_{i=1}^m$ consist of the coordinates of x and y with respect to the bases B_X and B_Y, respectively. It is readily verified that X and Y are both isomorphisms (for fixed bases B_X and B_Y). Let $\mathbb{F}_{n\times 1}$ denote the linear space (over the field $\mathbb{F}$) of all $n\times 1$ matrices (or, if you like, the linear space of all "column n-vectors" with entries in $\mathbb{F}$ — Example 2.L). Now consider the map $W_n\colon\mathbb{F}^n\to\mathbb{F}_{n\times 1}$ that assigns to each n-tuple $(\xi_1,\ldots,\xi_n)$ in $\mathbb{F}^n$ the $n\times 1$ matrix

$$\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} = W_n(\xi_1,\ldots,\xi_n)$$

in $\mathbb{F}_{n\times 1}$ whose entries are the (similarly ordered) coordinates of the ordered n-tuple with respect to the *canonical* basis for $\mathbb{F}^n$. It is easy to show that W_n is an isomorphism between $\mathbb{F}^n$ and $\mathbb{F}_{n\times 1}$. This is called the *natural isomorphism* of $\mathbb{F}^n$ onto $\mathbb{F}_{n\times 1}$. Note that any $m\times n$ matrix (with entries in $\mathbb{F}$) can be viewed as a linear transformation from $\mathbb{F}_{n\times 1}$ to $\mathbb{F}_{m\times 1}$: the action of an $m\times n$ matrix $[\alpha_{ij}]\in\mathbb{F}_{m\times n}$ on an $n\times 1$ matrix $[\xi_j]\in\mathbb{F}_{n\times 1}$ is simply the matrix product

$$[\alpha_{ij}][\xi_j] = \begin{pmatrix}\alpha_{11} & \ldots & \alpha_{1n}\\ \vdots & & \vdots\\ \alpha_{m1} & \ldots & \alpha_{mn}\end{pmatrix}\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix},$$

which is an $m\times 1$ matrix in $\mathbb{F}_{m\times 1}$. According to Example 2.L let $[A]\in\mathbb{F}_{m\times n}$ be the unique matrix representing the linear transformation $A\in\mathcal{L}[\mathcal{X},\mathcal{Y}]$ with respect to the bases B_X and B_Y. Now, if this matrix is viewed as a linear transformation of $\mathbb{F}_{n\times 1}$ into $\mathbb{F}_{m\times 1}$, then the diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{A} & \mathcal{Y} \\ {\scriptstyle X}\big\downarrow & & \big\uparrow{\scriptstyle Y^{-1}} \\ \mathbb{F}^n & & \mathbb{F}^m \\ {\scriptstyle W_n}\big\downarrow & & \big\uparrow{\scriptstyle W_m^{-1}} \\ \mathbb{F}_{n\times 1} & \xrightarrow{[A]} & \mathbb{F}_{m\times 1} \end{array}$$

commutes. This shows that the linear transformation $A\colon \mathcal{X} \to \mathcal{Y}$ is isomorphically equivalent to its matrix $[A]$ with respect to the bases B_X and B_Y when this matrix is viewed as a linear transformation $[A]\colon \mathbb{F}_{n\times 1} \to \mathbb{F}_{m\times 1}$. That is,

$$(W_m Y)A = [A](W_n X).$$

2.8 Direct Sum

Let $\{\mathcal{X}_i\}_{i=1}^n$ be a finite family of linear spaces over the same field $\mathbb{F}$ (not necessarily linear manifolds of the same linear space). The *direct sum* of $\{\mathcal{X}_i\}_{i=1}^n$, denoted by $\bigoplus_{i=1}^n \mathcal{X}_i$, is the set of all ordered n-tuples $(x_1, \ldots, x_n)$, with each x_i in $\mathcal{X}_i$, where vector addition and scalar multiplication are defined as follows.

$$(x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$
$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n)$$

for every $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ in $\bigoplus_{i=1}^n \mathcal{X}_i$ and every α in $\mathbb{F}$. It is easy to verify that the direct sum $\bigoplus_{i=1}^n \mathcal{X}_i$ of the linear spaces $\{\mathcal{X}_i\}_{i=1}^n$ is a linear space over $\mathbb{F}$ when vector addition (denoted by $\oplus$) and scalar multiplication are defined as above. The underlying set of the linear space $\bigoplus_{i=1}^n \mathcal{X}_i$ is the Cartesian product $\prod_{i=1}^n \mathcal{X}_i$ of the underlying sets of each linear space $\mathcal{X}_i$. The origin of $\bigoplus_{i=1}^n \mathcal{X}_i$ is the ordered n-tuple $(0_1, \ldots, 0_n)$ of the origins of each $\mathcal{X}_i$.

If $\mathcal{M}$ and $\mathcal{N}$ are linear manifolds of a linear space $\mathcal{X}$, then we may consider both their ordinary sum $\mathcal{M} + \mathcal{N}$ (defined as in Section 2.2) and their direct sum $\mathcal{M} \oplus \mathcal{N}$. These are different linear spaces over the same field. There is however a *natural mapping* $\Phi\colon \mathcal{M} \oplus \mathcal{N} \to \mathcal{M} + \mathcal{N}$, defined by

$$\Phi((x_1, x_2)) = x_1 + x_2,$$

which assigns to each pair (x_1, x_2) in $\mathcal{M} \oplus \mathcal{N}$ their sum in $\mathcal{M} + \mathcal{N} \subseteq \mathcal{X}$. It is readily verified that Φ is a surjective linear transformation of the linear space $\mathcal{M} \oplus \mathcal{N}$ onto the linear space $\mathcal{M} + \mathcal{N}$, but Φ is not always injective. We shall establish below a necessary and sufficient condition that $\varPhi$ be injective, viz., $\mathcal{M} \cap \mathcal{N} = \{0\}$. In such a case the mapping $\varPhi$ is an isomorphism (called the *natural isomorphism*) of $\mathcal{M} \oplus \mathcal{N}$ onto $\mathcal{M} + \mathcal{N}$, so that the direct sum $\mathcal{M} \oplus \mathcal{N}$ and the ordinary sum $\mathcal{M} + \mathcal{N}$ become isomorphic linear spaces.

Theorem 2.14. *Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$. The following assertions are pairwise equivalent.*

(a) $\mathcal{M} \cap \mathcal{N} = \{0\}$.

(b) *For each x in $\mathcal{M} + \mathcal{N}$ there exists a unique u in $\mathcal{M}$ and a unique v in $\mathcal{N}$ such that $x = u + v$.*

(c) *The natural mapping $\varPhi\colon \mathcal{M} \oplus \mathcal{N} \to \mathcal{M} + \mathcal{N}$ is an isomorphism.*

Proof. Take an arbitrary x in $\mathcal{M} + \mathcal{N}$. If $x = u_1 + v_1 = u_2 + v_2$, with u_1, u_2 in $\mathcal{M}$ and v_1, v_2 in $\mathcal{N}$, then $u_1 - u_2 = v_1 - v_2$ is in $\mathcal{M} \cap \mathcal{N}$ (for $u_1 - u_2 \in \mathcal{M}$ and $v_1 - v_2 \in \mathcal{N}$). Thus $\mathcal{M} \cap \mathcal{N} = \{0\}$ implies that $u_1 = u_2$ and $v_1 = v_2$, and hence (a)$\Rightarrow$(b). On the other hand, if $\mathcal{M} \cap \mathcal{N} \neq \{0\}$, then there exists a nonzero vector w in $\mathcal{M} \cap \mathcal{N}$. Take any nonzero vector x in $\mathcal{M} + \mathcal{N}$ so that $x = u + v$ with u in $\mathcal{M}$ and v in $\mathcal{N}$. Thus $x = (u + w) + (v - w)$, where $u + w$ is in $\mathcal{M}$ and $v - w$ is in $\mathcal{N}$. Since $w \neq 0$, it follows that $u + w \neq u$, and hence the representation of x as a sum $u + v$ with u in $\mathcal{M}$ and v in $\mathcal{N}$ is not unique. Thus, if (a) does not hold, then (b) does not hold. Equivalently, (b)$\Rightarrow$(a). Finally, recall that the natural mapping $\varPhi$ is linear and surjective. Since $\varPhi$ is injective if and only if (b) holds (by definition), it follows that (b)$\Leftrightarrow$(c). □

Two linear manifolds $\mathcal{M}$ and $\mathcal{N}$ of a linear space $\mathcal{X}$ are said to be *disjoint* (or *algebraically disjoint*) if $\mathcal{M} \cap \mathcal{N} = \{0\}$. (Note that, as linear manifolds of a linear space $\mathcal{X}$, $\mathcal{M}$ and $\mathcal{N}$ can never be "disjoint" in the set-theoretical sense — the origin of $\mathcal{X}$ always belongs to both of them.) Therefore, if $\mathcal{M}$ and $\mathcal{N}$ are disjoint linear manifolds of a linear space $\mathcal{X}$, then we may and shall identify their ordinary sum $\mathcal{M} + \mathcal{N}$ with their direct sum $\mathcal{M} \oplus \mathcal{N}$. Such an identification is carried out by the natural isomorphism $\varPhi\colon \mathcal{M} \oplus \mathcal{N} \to \mathcal{M} + \mathcal{N}$ (Theorem 2.14). When we identify $\mathcal{M} \oplus \mathcal{N}$ with $\mathcal{M} + \mathcal{N}$, which is a linear manifold of $\mathcal{X}$, we are automatically identifying the pairs $(u, 0)$ and $(0, v)$ in $\mathcal{M} \oplus \mathcal{N}$ with u in $\mathcal{M}$ and with v in $\mathcal{N}$, respectively. More generally, we shall be identifying the direct sums $\mathcal{M} \oplus \{0\}$ and $\{0\} \oplus \mathcal{N}$ with $\mathcal{M}$ and $\mathcal{N}$, respectively. For instance, if $x \in \mathcal{M} \oplus \mathcal{N}$ and $\mathcal{M} \cap \mathcal{N} = \{0\}$, then Theorem 2.14 ensures that there exists a unique u in $\mathcal{M}$ and a unique v in $\mathcal{N}$ such that $x = (u, v)$. Hence $x = (u, 0) \oplus (0, v)$ where $(u, 0) \in \mathcal{M} \oplus \{0\}$ and $(0, v) \in \{0\} \oplus \mathcal{N}$ (recall: $\mathcal{M} \oplus \{0\}$ and $\{0\} \oplus \mathcal{N}$ are both linear manifolds of $\mathcal{M} \oplus \mathcal{N}$). Now identify $(u, 0)$ with $\varPhi((u, 0)) = u$ and $(0, v)$ with $\varPhi((0, v)) = v$, and write $x = u \oplus v$ where $u \in \mathcal{M}$ and $v \in \mathcal{N}$ (instead of $x = (u, 0) \oplus (0, v) = \varPhi^{-1}(u) \oplus \varPhi^{-1}(v)$). Outcome: If $\mathcal{M}$ and $\mathcal{N}$ are disjoint linear manifolds of a linear space $\mathcal{X}$, then every x in $\mathcal{M} \oplus \mathcal{N}$ has a *unique decomposition with respect to $\mathcal{M}$ and $\mathcal{N}$*, denoted by $x = u \oplus v$, which is referred to as the *direct sum* of u in $\mathcal{M}$ and v in

$\mathcal{N}$. It should be noticed that $u \oplus v$ is just another notation for (u, v) that reminds us of the algebraic structure of the linear space $\mathcal{M} \oplus \mathcal{N}$. What really is being added in $\mathcal{M} \oplus \mathcal{N}$ is $(u, 0) \oplus (0, v)$.

If $\mathcal{M}$ and $\mathcal{N}$ are disjoint linear manifolds of a linear space $\mathcal{X}$, and if their (ordinary) sum is $\mathcal{X}$, then we say that $\mathcal{M}$ and $\mathcal{N}$ are *algebraic complements* of each other. In other words, two linear manifolds $\mathcal{M}$ and $\mathcal{N}$ of a linear space $\mathcal{X}$ form a pair of algebraic complements in $\mathcal{X}$ if

$$\mathcal{X} = \mathcal{M} + \mathcal{N} \quad \text{and} \quad \mathcal{M} \cap \mathcal{N} = \{0\}.$$

Accordingly, this can be written as

$$\mathcal{X} = \mathcal{M} \oplus \mathcal{N} \quad \text{and} \quad \mathcal{M} \cap \mathcal{N} = \{0\}$$

once we have identified the direct sum $\mathcal{M} \oplus \mathcal{N}$ with its isomorphic image $\Phi(\mathcal{M} \oplus \mathcal{N}) = \mathcal{M} + \mathcal{N} = \mathcal{X}$ through the natural isomorphism Φ.

Proposition 2.15. *Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$, and let B_M and B_N be Hamel bases for $\mathcal{M}$ and $\mathcal{N}$, respectively.*

(a) $\mathcal{M} \cap \mathcal{N} = \{0\}$ *if and only if* $B_M \cap B_N = \varnothing$ *and* $B_M \cup B_N$ *is linearly independent.*

(b) $\mathcal{M} + \mathcal{N} = \mathcal{X}$ *and* $B_M \cup B_N$ *is linearly independent if and only if* $B_M \cup B_N$ *is a Hamel basis for* $\mathcal{X}$.

In particular, if $B_M \cup B_N \subseteq B$, *where* B *is a Hamel basis for* $\mathcal{X}$, *then*

(a′) $\mathcal{M} \cap \mathcal{N} = \{0\}$ *if and only if* $B_M \cap B_N = \varnothing$,

(b′) $\mathcal{M} + \mathcal{N} = \mathcal{X}$ *if and only if* $B_M \cup B_N = B$.

Proof. (a) Recall that

$$\{0\} \subseteq \operatorname{span}(B_M \cap B_N) \subseteq \operatorname{span}(\mathcal{M} \cap \mathcal{N}) = \mathcal{M} \cap \mathcal{N}.$$

Thus $\mathcal{M} \cap \mathcal{N} = \{0\}$ implies $\operatorname{span}(B_M \cap B_N) = \{0\}$, which in turn implies $B_M \cap B_N = \varnothing$ (for $0 \notin B_M \cup B_N$). Moreover, if $\mathcal{M} \cap \mathcal{N} = \{0\}$, then the union of the linearly independent sets B_M and B_N is again linearly independent (see Problem 2.3). On the other hand, recall that

$$\{0\} \subseteq \mathcal{M} \cap \mathcal{N} = \operatorname{span} B_M \cap \operatorname{span} B_N = \operatorname{span}(B_M \cap B_N)$$

if $B_M \cup B_N$ is linearly independent (see Problem 2.4). Thus $B_M \cap B_N = \varnothing$ implies $\operatorname{span}(B_M \cap B_N) = \{0\}$, and hence $\mathcal{M} \cap \mathcal{N} = \{0\}$.

(b) Next recall that

$$\operatorname{span}(B_M \cup B_N) = \operatorname{span}(\mathcal{M} \cup \mathcal{N}) = \mathcal{M} + \mathcal{N} \subseteq \mathcal{X}$$

whenever B_M and B_N are Hamel bases for $\mathcal{M}$ and $\mathcal{N}$, respectively. Moreover, if $B_M \cup B_N$ is a Hamel basis for $\mathcal{X}$, then $B_M \cup B_N$ is linearly independent and $\mathcal{X} = \operatorname{span}(B_M \cup B_N)$ so that $\mathcal{M} + \mathcal{N} = \mathcal{X}$. On the other hand, if $\mathcal{M} + \mathcal{N} = \mathcal{X}$, then $\operatorname{span}(B_M \cup B_N) = \mathcal{X}$. Thus, according to Theorem 2.6, there exists a Hamel basis B' for $\mathcal{X}$ such that $B' \subseteq B_M \cup B_N$. If $B_M \cup B_N$ is linearly independent, then Theorem 2.5 ensures that there exists a Hamel basis B for $\mathcal{X}$ such that $B_M \cup B_N \subseteq B$. Therefore $B' \subseteq B$. But a Hamel basis is maximal (see Claim 2 in the proof of Theorem 2.5) so that $B' = B$. Hence $B_M \cup B_N = B$. □

Theorem 2.16. *Every linear manifold has an algebraic complement.*

Proof. Let $\mathcal{M}$ be a linear manifold of a linear space $\mathcal{X}$, let B_M be a Hamel basis for $\mathcal{M}$, and let B be a Hamel basis for $\mathcal{X}$ such that $B_M \subseteq B$ (see Theorem 2.5). Set $B_N = B \backslash B_M$ (which, as a subset of a linearly independent set B, is linearly independent itself), and set $\mathcal{N} = \operatorname{span} B_N$ (a linear manifold of $\mathcal{X}$). Thus B_M and B_N are Hamel basis for $\mathcal{M}$ and $\mathcal{N}$, respectively, both included in the Hamel basis B for $\mathcal{X}$. Since $B_M \cap B_N = \varnothing$ and $B_M \cup B_N = B$, it follows by Proposition 2.15 that $\mathcal{N}$ is an algebraic complement of $\mathcal{M}$. □

Lemma 2.17. *Let $\mathcal{M}$ be a linear manifold of a linear space $\mathcal{X}$. Every algebraic complement of $\mathcal{M}$ is isomorphic to the quotient space $\mathcal{X}/\mathcal{M}$.*

Proof. Let $\mathcal{M}$ be a linear manifold of a linear space $\mathcal{X}$ over a field $\mathbb{F}$, and let $\mathcal{X}/\mathcal{M}$ be the quotient space of $\mathcal{X}$ modulo $\mathcal{M}$, which is again a linear space over $\mathbb{F}$ (see Example 2.H). The natural mapping $\pi\colon \mathcal{X} \to \mathcal{X}/\mathcal{M}$, which assigns each vector x in $\mathcal{X}$ the equivalence class

$$\pi(x) \,=\, [x] \,=\, x + \mathcal{M}$$

in $\mathcal{X}/\mathcal{M}$, is a linear transformation (cf. Example 2.H). It is plain that π is surjective. Let $\mathcal{K}$ be a linear manifold of $\mathcal{X}$ and consider the restriction of π to $\mathcal{K}$, $\pi|_{\mathcal{K}}\colon \mathcal{K} \to \mathcal{X}/\mathcal{M}$, which is again a linear transformation (Problem 2.14).

Claim 1. If $\mathcal{M} \cap \mathcal{K} = \{0\}$, then $\pi|_{\mathcal{K}}$ is injective.

Proof. Problem 2.14 also says that $\mathcal{N}(\pi|_{\mathcal{K}}) = \mathcal{K} \cap \mathcal{N}(\pi)$. Since $\mathcal{N}(\pi) = \mathcal{M}$ (see Example 2.H), it follows that, if $\mathcal{M} \cap \mathcal{K} = \{0\}$, then $\mathcal{N}(\pi|_{\mathcal{K}}) = \{0\}$, and so the linear transformation $\pi|_{\mathcal{K}}$ is injective (Theorem 2.8). □

Claim 2. If $\mathcal{X} = \mathcal{M} + \mathcal{K}$, then $\pi|_{\mathcal{K}}$ is surjective.

Proof. Take an arbitrary $[x]$ in $\mathcal{X}/\mathcal{M}$ so that $[x] = x + \mathcal{M}$ for some x in $\mathcal{X}$. If $\mathcal{X} = \mathcal{M} + \mathcal{K}$, then $x = u + v$ with u in $\mathcal{M}$ and v in $\mathcal{K}$. Thus, as π is linear, $[x] = \pi(x) = \pi(u) + \pi(v)$. But $u \in \mathcal{M} = \mathcal{N}(\pi)$ so that $\pi(u) = [0]$, and hence $\pi(u) + \pi(v) = [0] + [v] = [0 + v] = [v] = \pi(v)$. Therefore, $[x] = \pi(v) = \pi|_{\mathcal{K}}(v)$, which lies in $\mathcal{R}(\pi|_{\mathcal{K}})$. Then $\mathcal{X}/\mathcal{M} \subseteq \mathcal{R}(\pi|_{\mathcal{K}})$, and so $\pi|_{\mathcal{K}}$ is surjective. □

Thus, if $\mathcal{K}$ is an algebraic complement of $\mathcal{M}$, then $\pi|_{\mathcal{K}}$ is invertible by Claims 1 and 2 and, since $\pi|_{\mathcal{K}}$ is linear, it is an isomorphism of $\mathcal{K}$ onto $\mathcal{X}/\mathcal{M}$. □

Theorem 2.18. *Let $\mathcal{M}$ be a linear manifold of a linear space $\mathcal{X}$. Every algebraic complement of $\mathcal{M}$ has the same dimension.*

Proof. According to Theorem 2.12 the above statement can be rewritten as follows. If $\mathcal{N}$ and $\mathcal{K}$ are algebraic complements of $\mathcal{M}$, then $\mathcal{K}$ and $\mathcal{N}$ are isomorphic. But this is a straightforward consequence of the previous lemma: $\mathcal{N}$ and $\mathcal{K}$ are both isomorphic to $\mathcal{X}/\mathcal{M}$, and hence isomorphic to each other. □

The dimension of an algebraic complement of $\mathcal{M}$ is therefore a property of $\mathcal{M}$ (i.e., it is an invariant for $\mathcal{M}$). We refer to this invariant as the *codimension* of $\mathcal{M}$: the codimension of a linear manifold $\mathcal{M}$, denoted by $\operatorname{codim}\mathcal{M}$, is the (constant) dimension of any algebraic complement of $\mathcal{M}$.

2.9 Projections

A *projection* is an idempotent linear transformation of a linear space into itself. Thus, if $\mathcal{X}$ is a linear space, then $P \in \mathcal{L}[\mathcal{X}]$ is a projection if and only if $P = P^2$. Briefly, projections are the idempotent elements of $\mathcal{L}[\mathcal{X}]$. It is plain that the null transformation O and the identity I in $\mathcal{L}[\mathcal{X}]$ are projections. A *nontrivial projection* in $\mathcal{L}[\mathcal{X}]$ is a projection P such that $O \neq P \neq I$. It is easy to verify that, if P is a projection, then so is $I - P$. Moreover, the null spaces and ranges of P and $I - P$ are related as follows (cf. Problem 1.4).

$$\mathcal{R}(P) = \mathcal{N}(I - P) \quad \text{and} \quad \mathcal{N}(P) = \mathcal{R}(I - P).$$

Projections are singularly useful linear transformations. One of their main properties is that the range and the null space of a projection form a pair of algebraic complements.

Theorem 2.19. *If $P \in \mathcal{L}[\mathcal{X}]$ is a projection, then $\mathcal{R}(P)$ and $\mathcal{N}(P)$ are algebraic complements of each other.*

Proof. Let $\mathcal{X}$ be a linear space and let $P\colon \mathcal{X} \to \mathcal{X}$ be a projection. Recall that both the range $\mathcal{R}(P)$ and the null space $\mathcal{N}(P)$ are linear manifolds of $\mathcal{X}$ (because P is linear). Since P is idempotent, it follows that

$$\mathcal{R}(P) \;=\; \big\{x \in \mathcal{X}\colon\; Px = x\big\}$$

(the range of an idempotent mapping is the set of all its fixed points — Problem 1.4). If $x \in \mathcal{R}(P) \cap \mathcal{N}(P)$, then $x = Px = 0$, and hence

$$\mathcal{R}(P) \cap \mathcal{N}(P) \;=\; \{0\}.$$

Moreover, write any vector x in $\mathcal{X}$ as $x = Px + (x - Px)$. Since P is linear and idempotent, $P(x - Px) = Px - P^2x = 0$, and so $(x - Px)$ lies in $\mathcal{N}(P)$. Hence $x = u + v$ with $u = Px$ in $\mathcal{R}(P)$ and $v = (x - Px)$ in $\mathcal{N}(P)$. Therefore,

$$\mathcal{X} \;=\; \mathcal{R}(P) + \mathcal{N}(P).$$ □

On the other hand, for any pair of algebraic complements there exists a unique projection whose range and null space coincide with them.

Theorem 2.20. *Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$. If $\mathcal{M}$ and $\mathcal{N}$ are algebraic complements of each other, then there exists a unique projection $P\colon \mathcal{X} \to \mathcal{X}$ such that $\mathcal{R}(P) = \mathcal{M}$ and $\mathcal{N}(P) = \mathcal{N}$.*

Proof. Let $\mathcal{M}$ and $\mathcal{N}$ be algebraic complements in a linear space $\mathcal{X}$ so that

$$\mathcal{M} + \mathcal{N} = \mathcal{X} \quad \text{and} \quad \mathcal{M} \cap \mathcal{N} = \{0\}.$$

According to Theorem 2.14, for each $x \in \mathcal{X}$ there exists a unique $u \in \mathcal{M}$ and a unique $v \in \mathcal{N}$ such that $x = u + v$. Let $P\colon \mathcal{X} \to \mathcal{X}$ be the function that assigns to each x in $\mathcal{X}$ its unique summand u in $\mathcal{M}$ (i.e., $Px = u$). It is easy to verify that P is linear. Moreover, for each vector x in $\mathcal{X}$, $P^2x = P(Px) = Pu = u = Px$ (reason: u is itself its unique summand in $\mathcal{M}$), so that P is idempotent. By the very definition of P we get $\mathcal{R}(P) = \mathcal{M}$ and $\mathcal{N}(P) = \mathcal{N}$. Conclusion: $P\colon \mathcal{X} \to \mathcal{X}$ is a projection with $\mathcal{R}(P) = \mathcal{M}$ and $\mathcal{N}(P) = \mathcal{N}$. Now let $P'\colon \mathcal{X} \to \mathcal{X}$ be any projection with $\mathcal{R}(P') = \mathcal{M}$ and $\mathcal{N}(P') = \mathcal{N}$. Take an arbitrary $x \in \mathcal{X}$ and consider again its unique representation as $x = u + v$ with $u \in \mathcal{M} = \mathcal{R}(P')$ and $v \in \mathcal{N} = \mathcal{N}(P')$. Since P' is linear and idempotent, it follows that $P'x = P'u + P'v = u = Px$. Therefore, $P' = P$. □

Remark: An immediate corollary of Theorems 2.16 and 2.20 says that any linear manifold of a linear space is the range of some projection. That is, *if $\mathcal{M}$ is a linear manifold of a linear space $\mathcal{X}$, then there exists a projection $P\colon \mathcal{X} \to \mathcal{X}$ such that $\mathcal{R}(P) = \mathcal{M}$.*

If $\mathcal{M}$ and $\mathcal{N}$ are algebraic complements in a linear space $\mathcal{X}$, then the unique projection P in $\mathcal{L}[\mathcal{X}]$ with range $\mathcal{R}(P) = \mathcal{M}$ and null space $\mathcal{N}(P) = \mathcal{N}$ is called *the projection on $\mathcal{M}$ along $\mathcal{N}$*. If P is the projection on $\mathcal{M}$ along $\mathcal{N}$, then the projection on $\mathcal{N}$ along $\mathcal{M}$ is precisely the projection $E = I - P$ in $\mathcal{L}[\mathcal{X}]$, referred to as the *complementary projection* of P. Note that $EP = PE = O$.

Proposition 2.21. *Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$. If $\mathcal{M}$ and $\mathcal{N}$ are algebraic complements of each other, then the unique decomposition of each x in $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$ as a direct sum*

$$x = u \oplus v$$

of u in $\mathcal{M}$ and v in $\mathcal{N}$ is such that

$$u = Px \quad \textit{and} \quad v = (I - P)x,$$

where $P\colon \mathcal{X} \to \mathcal{X}$ is the unique projection on $\mathcal{M}$ along $\mathcal{N}$.

Proof. Take an arbitrary x in $\mathcal{X}$ and consider its unique decomposition $x = u \oplus v$ in $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$. Note that the identification of $\mathcal{M} \oplus \mathcal{N}$ with

$\mathcal{M}+\mathcal{N}=\mathcal{X}$ is implicitly assumed in the proposition statement. Now write $x=(u,v)$ and set $Px=(u,0)$. The very same argument used in the proof of Theorem 2.20 can be applied here to verify that this actually defines a unique projection $P\colon\mathcal{M}\oplus\mathcal{N}\to\mathcal{M}\oplus\mathcal{N}$ such that $\mathcal{R}(P)=\mathcal{M}\oplus\{0\}$ and $\mathcal{N}(P)=\{0\}\oplus\mathcal{N}$. Finally, identify $\mathcal{M}\oplus\{0\}$ and $\{0\}\oplus\mathcal{N}$ with $\mathcal{M}$ and $\mathcal{N}$ (and hence $(u,0)$ and $(0,v)$ with u and v), respectively. □

According to Theorem 2.16 every linear space $\mathcal{X}$ can be represented as the sum $\mathcal{X}=\mathcal{M}+\mathcal{N}$ of a pair $\{\mathcal{M},\mathcal{N}\}$ of algebraic complements in $\mathcal{X}$. If $\mathcal{M}\oplus\mathcal{N}$ is identified with $\mathcal{M}+\mathcal{N}$, then this means that *every linear space $\mathcal{X}$ has a decomposition $\mathcal{X}=\mathcal{M}\oplus\mathcal{N}$ as a direct sum of disjoint linear manifolds of $\mathcal{X}$.*

Proposition 2.22. *Let $\mathcal{X}$ be a linear space and consider its decomposition*

$$\mathcal{X} = \mathcal{M}\oplus\mathcal{N}$$

as a direct sum of disjoint linear manifolds $\mathcal{M}$ and $\mathcal{N}$ of $\mathcal{X}$. Let $P\colon\mathcal{X}\to\mathcal{X}$ be the projection on $\mathcal{M}$ along $\mathcal{N}$, and let $E=I-P$ be the projection on $\mathcal{N}$ along $\mathcal{M}$. Every linear transformation $L\colon\mathcal{X}\to\mathcal{X}$ can be written as a $2{\times}2$ matrix with linear transformation entries

$$L = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where $A=PL|_{\mathcal{M}}\colon\mathcal{M}\to\mathcal{M}$, $B=PL|_{\mathcal{N}}\colon\mathcal{N}\to\mathcal{M}$, $C=EL|_{\mathcal{M}}\colon\mathcal{M}\to\mathcal{N}$, and $D=EL|_{\mathcal{N}}\colon\mathcal{N}\to\mathcal{N}$.

Proof. Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$. Suppose $\mathcal{M}$ and $\mathcal{N}$ are algebraic complements of each other, identify $\mathcal{M}\oplus\mathcal{N}$ with $\mathcal{M}+\mathcal{N}$, and consider the decomposition $\mathcal{X}=\mathcal{M}\oplus\mathcal{N}$. Let L be a linear transformation on $\mathcal{M}\oplus\mathcal{N}$ so that $L\in\mathcal{L}[\mathcal{X}]$. Take an arbitrary $x\in\mathcal{X}$ and consider its unique decomposition $x=u\oplus v$ in $\mathcal{X}=\mathcal{M}\oplus\mathcal{N}$ with u in $\mathcal{M}$ and v in $\mathcal{N}$. Now write $x=(u,v)$ so that $Lx = L(u,v) = L((u,0)\oplus(0,v)) = L(u,0)\oplus L(0,v) = L|_{\mathcal{M}\oplus\{0\}}(u,0)\oplus L|_{\{0\}\oplus\mathcal{N}}(0,v)$. Identifying $\mathcal{M}\oplus\{0\}$ and $\{0\}\oplus\mathcal{N}$ with $\mathcal{M}$ and $\mathcal{N}$ (and so $(u,0)$ and $(0,v)$ with u and v), respectively, it follows that

$$Lx = L|_{\mathcal{M}}u\oplus L|_{\mathcal{N}}v,$$

where $L|_{\mathcal{M}}u$ and $L|_{\mathcal{N}}v$ lie in $\mathcal{X}=\mathcal{M}\oplus\mathcal{N}$. By Proposition 2.21 we may write

$$L|_{\mathcal{M}}u = PL|_{\mathcal{M}}u\oplus EL|_{\mathcal{M}}u,$$

$$L|_{\mathcal{N}}v = PL|_{\mathcal{N}}v\oplus EL|_{\mathcal{N}}v,$$

where P is the unique projection on $\mathcal{M}$ along $\mathcal{N}$ and $E=I-P$. Therefore,

$$Lx = (PL|_{\mathcal{M}}u + PL|_{\mathcal{N}}v)\oplus(EL|_{\mathcal{M}}u + EL|_{\mathcal{N}}v),$$

where $PL|_{\mathcal{M}}u+PL|_{\mathcal{N}}v$ is in $\mathcal{M}$ and $EL|_{\mathcal{M}}u+EL|_{\mathcal{N}}v$ is in $\mathcal{N}$. Since the ranges of $PL|_{\mathcal{M}}$ and $PL|_{\mathcal{N}}$ are included in $\mathcal{R}(P)=\mathcal{M}$, we may think of them as linear transformations into $\mathcal{M}$. Similarly, $EL|_{\mathcal{M}}$ and $EL|_{\mathcal{N}}$ can be thought of as linear transformations into $\mathcal{N}$. Thus set $A = PL|_{\mathcal{M}}$ in $\mathcal{L}[\mathcal{M}]$, $B = PL|_{\mathcal{N}}$ in $\mathcal{L}[\mathcal{N},\mathcal{M}]$, $C = EL|_{\mathcal{M}}$ in $\mathcal{L}[\mathcal{M},\mathcal{N}]$, and $D = EL|_{\mathcal{N}}$ in $\mathcal{L}[\mathcal{N}]$ so that

$$Lx = (Au + Bv, Cu + Dv) \in \mathcal{M} \oplus \mathcal{N}$$

for every $x = (u, v) \in \mathcal{M} \oplus \mathcal{N}$. In terms of standard matrix notation, the vector Lx in $\mathcal{M} \oplus \mathcal{N}$ can be viewed as a 2×1 matrix with the first entry in $\mathcal{M}$ and the other in $\mathcal{N}$, namely, $\left(\begin{smallmatrix} Au+Bv \\ Cu+Dv \end{smallmatrix}\right)$. This is precisely the action of the 2×2 matrix with linear transformation entries, $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, on the 2×1 matrix with entries in $\mathcal{M}$ and $\mathcal{N}$ representing x, namely, $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$. Thus $Lx = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$, and hence we write $L = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. □

Example 2.O. Consider the setup of Proposition 2.22. Note that the projection on $\mathcal{M}$ along $\mathcal{N}$ can be written as

$$P = \begin{pmatrix} I & O \\ O & O \end{pmatrix}$$

with respect to the decomposition $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$, where I denotes the identity on $\mathcal{M}$. Thus $LP = \left(\begin{smallmatrix} A & O \\ C & O \end{smallmatrix}\right)$ and $PLP = \left(\begin{smallmatrix} A & O \\ O & O \end{smallmatrix}\right)$, so that $LP = PLP$ if and only if $C = O$. Note that $\mathcal{M}$ is L-invariant (i.e., $L(\mathcal{M}) \subseteq \mathcal{M}$) if and only if $PL|_{\mathcal{M}} = L|_{\mathcal{M}}$ (equivalently, if and only if $EL|_{\mathcal{M}} = O$ with $E = I - P$). Thus

$$L(\mathcal{M}) \subseteq \mathcal{M} \iff A = L|_{\mathcal{M}} \iff C = O \iff LP = PLP.$$

Conclusion 1: The following assertions are pairwise equivalent.

(a) $\mathcal{M}$ is L-invariant.

(b) $L = \left(\begin{smallmatrix} L|_{\mathcal{M}} & B \\ O & D \end{smallmatrix}\right)$.

(c) $LP = PLP$.

Similarly, if we apply the same argument to $\mathcal{N}$, then

$$L(\mathcal{N}) \subseteq \mathcal{N} \iff D = L|_{\mathcal{N}} \iff B = O \iff PL = PLP.$$

Conclusion 2: The following assertions are pairwise equivalent as well.

(a$'$) $\mathcal{M}$ and $\mathcal{N}$ are both L-invariant.

(b$'$) $L = \left(\begin{smallmatrix} L|_{\mathcal{M}} & O \\ O & L|_{\mathcal{N}} \end{smallmatrix}\right)$.

(c$'$) L and P commute (i.e., $PL = LP$).

Let $\mathcal{M}$ and $\mathcal{N}$ be algebraic complements in a linear space $\mathcal{X}$. If a linear transformation L in $\mathcal{L}[\mathcal{X}]$ is represented as $L = \left(\begin{smallmatrix} A & O \\ O & D \end{smallmatrix}\right)$ in terms of the decomposition $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$ (as in (a$'$) above), where $A \in \mathcal{L}[\mathcal{M}]$ and $D \in \mathcal{L}[\mathcal{N}]$, then it is usual to write $L = A \oplus D$. For instance, the projection on $\mathcal{M}$ along $\mathcal{N}$, which is represented as $P = \left(\begin{smallmatrix} I & O \\ O & O \end{smallmatrix}\right)$ with respect to the same decomposition $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$, is usually written as $P = I \oplus O$. These are examples of the following concept.

Let $\{\mathcal{X}_i\}_{i=1}^n$ be a finite family of linear spaces over the same scalar field and consider their direct sum $\bigoplus_{i=1}^n \mathcal{X}_i$. Let $\{L_i\}_{i=1}^n$ be a family of linear transformations such that each L_i lies in each $\mathcal{L}[\mathcal{X}_i]$. The *direct sum* of $\{L_i\}_{i=1}^n$, denoted by $\bigoplus_{i=1}^n L_i$, is the mapping of $\bigoplus_{i=1}^n \mathcal{X}_i$ into itself defined by

$$\bigoplus_{i=1}^n L_i(x_1, \ldots, x_n) \;=\; (L_1 x_1, \ldots, L_n x_n)$$

for every $(x_1, \ldots, x_n)$ in $\bigoplus_{i=1}^n \mathcal{X}_i$. It is readily verified that $\bigoplus_{i=1}^n L_i$ is linear (i.e., $\bigoplus_{i=1}^n L_i \in \mathcal{L}[\bigoplus_{i=1}^n \mathcal{X}_i]$) and also that, for every index i,

$$\Big(\bigoplus_{i=1}^n L_i\Big)\Big|_{\mathcal{X}_i} \;=\; L_i.$$

The above identity is a short notation for the following assertion. "If 0_i is the origin of each $\mathcal{X}_i$ and O_i is the unique (linear) transformation of $\{0_i\}$ onto itself, then each linear manifold $\{0_1\} \oplus \cdots \oplus \{0_{i-1}\} \oplus \mathcal{X}_i \oplus \{0_{i+1}\} \oplus \cdots \oplus \{0_n\}$ of $\bigoplus_{i=1}^n \mathcal{X}_i$ is invariant for $\bigoplus_{i=1}^n L_i$ and the restriction of $\bigoplus_{i=1}^n L_i$ to that invariant linear manifold is the direct sum $O_1 \oplus \cdots \oplus O_{i-1} \oplus L_i \oplus O_{i+1} \oplus \cdots \oplus O_n$". Of course, we shall always use the short notation. Conversely, if $L \in \mathcal{L}[\bigoplus_{i=1}^n \mathcal{X}_i]$ is such that each restriction $L|_{\mathcal{X}_i}$ lies in $\mathcal{L}[\mathcal{X}_i]$, then L is the direct sum of $\{L|_{\mathcal{X}_i}\}_{i=1}^n$. That is, if each $\mathcal{X}_i$ in $\bigoplus_{i=1}^n \mathcal{X}_i$ is invariant for $L \in \mathcal{L}[\bigoplus_{i=1}^n \mathcal{X}_i]$, then

$$L \;=\; \bigoplus_{i=1}^n L|_{\mathcal{X}_i}.$$

Summing up: Set $\mathcal{X} = \bigoplus_{i=1}^n \mathcal{X}_i$ and consider linear transformations L_i in $\mathcal{L}[\mathcal{X}_i]$ for each i and L in $\mathcal{L}[\mathcal{X}]$.

$$L = \bigoplus_{i=1}^n L_i \quad \text{if and only if} \quad L_i = L|_{\mathcal{X}_i}$$

for every index i (so that each $\mathcal{X}_i$, viewed as a linear manifold of the linear space $\bigoplus_{i=1}^n \mathcal{X}_i$, is invariant for L). The linear transformations $\{L_i\}$ are referred to as the *direct summands* of L.

In particular, consider the decomposition $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$ of a linear space $\mathcal{X}$ into the direct sum of a pair of algebraic complements $\mathcal{M}$ and $\mathcal{N}$ in $\mathcal{X}$, and take linear transformations $L \in \mathcal{L}[\mathcal{X}]$, $A \in \mathcal{L}[\mathcal{M}]$, and $D \in \mathcal{L}[\mathcal{N}]$. Then

$$L = \begin{pmatrix} A & O \\ O & D \end{pmatrix} = A \oplus D \quad \text{if and only if} \quad A = L|_{\mathcal{M}} \text{ and } D = L|_{\mathcal{N}}$$

(so that $\mathcal{M}$ and $\mathcal{N}$ are both L-invariant), where A and D are the direct summands of L with respect to the decomposition $\mathcal{X} = \mathcal{M} \oplus \mathcal{N}$.

Suggested Reading

Birkhoff and MacLane [1]
Brown and Pearcy [3]
Halmos [2], [5]
Herstein [1], [2]
Hoffman and Kunze [1]
Kaplansky [1]
Lax [2]
MacLane and Birkhoff [1]
Naylor and Sell [1]
Roman [1]
Simmons [1]
Taylor and Lay [1]

Problems

Problem 2.1. Let $\mathcal{X}$ be a linear space over a field $\mathbb{F}$. Take arbitrary α and β in $\mathbb{F}$ and arbitrary x, y, and z in $\mathcal{X}$. Verify the following propositions.

(a) $(-\alpha)x = -(\alpha x)$.

(b) $0x = 0 = \alpha 0$.

(c) $\alpha x = 0 \quad\Longrightarrow\quad \alpha = 0$ or $x = 0$.

(d) $x + y = x + z \quad\Longrightarrow\quad y = z$.

(e) $\alpha x = \alpha y \quad\Longrightarrow\quad x = y$ if $\alpha \neq 0$.

(f) $\alpha x = \beta x \quad\Longrightarrow\quad \alpha = \beta$ if $x \neq 0$.

Problem 2.2. Let $\mathcal{X}$ be a real or complex linear space. A subset C of $\mathcal{X}$ is *convex* if $\alpha x + (1-\alpha)y$ is in C for every x, y in C and every α in $[0,1]$. A vector $x \in \mathcal{X}$ is a *convex linear combination* of vectors in $\mathcal{X}$ if there exist a finite set $\{x_i\}_{i=1}^n$ of vectors in $\mathcal{X}$ and a finite family of nonnegative scalars $\{\alpha_i\}_{i=1}^n$ such that $x = \sum_{i=1}^n \alpha_i x_i$ and $\sum_{i=1}^n \alpha_i = 1$. If A is a subset of $\mathcal{X}$, then the intersection of all convex sets containing A is called the *convex hull* of A, denoted by $\mathrm{co}(A)$.

(a) Show that the intersection of an arbitrary nonempty collection of convex sets is convex.

(b) Show that $\mathrm{co}(A)$ is the smallest (in the inclusion ordering) convex set that includes A.

(c) Show that C is convex if and only if every convex linear combination of vectors in C belongs to C.

Hint: To verify that *every convex linear combination of vectors in a convex set C belongs to C*, proceed as follows. Note that the italicized result holds for any convex linear combination of two vectors in C (by definition of convex set). Suppose it holds for every convex linear combination of n vectors in C, for some $n \in \mathbb{N}$. This implies that $\alpha\sum_{i=1}^n \alpha^{-1}\alpha_i x_i + \alpha_{n+1}x_{n+1}$ lies in C whenever $\{x_i\}_{i=1}^{n+1} \subset C$ and $\sum_{i=1}^{n+1}\alpha_i = 1$ with $0 < \alpha_{n+1}$, where $\alpha = \sum_{i=1}^n \alpha_i$ (reason: $\sum_{i=1}^n \alpha^{-1}\alpha_i x_i \in C$). Conclude the proof by induction.

(d) Show that $\mathrm{co}(A)$ coincides with the set of all convex linear combinations of vectors in A.

Hint: Let $\mathrm{clc}(A)$ denote the set of all convex linear combinations of vectors in A. Verify that $\mathrm{clc}(A)$ is a convex set. Now use (b) and (c) to show that $\mathrm{co}(A) \subseteq \mathrm{clc}(A) \subseteq \mathrm{clc}(\mathrm{co}(A)) = \mathrm{co}(A)$.

Problem 2.3. Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space $\mathcal{X}$, and let A and B be linearly independent subsets of $\mathcal{M}$ and $\mathcal{N}$, respectively. If $\mathcal{M} \cap \mathcal{N} = \{0\}$, then $A \cup B$ is linearly independent.

Hint: If $a \in A$ is a linear combination of vectors in $A \cup B$, then $a = b + a'$ for some $a' \in \mathcal{M}$ and some $b \in \mathcal{N}$.

Problem 2.4. Let A be a linearly independent subset of a linear space $\mathcal{X}$. If B and C are subsets of A, then

$$\mathrm{span}\,(B \cap C) \;=\; \mathrm{span}\, B \cap \mathrm{span}\, C.$$

Hint: Show that $\mathrm{span}\, B \cap \mathrm{span}\, C \subseteq \mathrm{span}\,(B \cup C)$ by Proposition 2.3.

Problem 2.5. The cardinality of a linearly independent subset of a linear space $\mathcal{X}$ is less than or equal to the cardinality of a subset of $\mathcal{X}$ that spans $\mathcal{X}$.

Hint: That is, *if* $A \subseteq \mathcal{X}$ *is such that* $\mathrm{span}\, A = \mathcal{X}$, *then* $\#C \le \#A$ *for every linearly independent* $C \subseteq \mathcal{X}$. Indeed, if $B \subseteq \mathcal{X}$ is a Hamel basis for $\mathcal{X}$, then show that $\#C \le \#B \le \#A$. (Apply Theorems 2.5, 2.6, and 2.7 — see Problems 1.21(a) and 1.22.) Note that this generalizes Claim 0 in the proof of Theorem 2.7 for subsets of arbitrary cardinality.

Problem 2.6. Let $\mathcal{X}$ be a linear space, and let $\mathcal{M}$ be a linear manifold of $\mathcal{X}$. Verify the following propositions.

(a) $\dim \mathcal{M} = 0$ if and only if $\mathcal{M} = \{0\}$.

(b) $\dim \mathcal{M} \le \dim \mathcal{X}$. (*Hint*: Problem 2.5.)

Problem 2.7. If $\mathcal{M}$ is a proper linear manifold of a *finite-dimensional* linear space $\mathcal{X}$, then $\dim \mathcal{M} < \dim \mathcal{X}$. Prove the above statement and show that it does not hold for infinite-dimensional linear spaces.

Hint: Show that $\dim \mathcal{X}_0 = \dim \mathcal{X}$, where $\mathcal{X}$ is the linear space of Example 2.J and $\mathcal{X}_0 = \{x = (\xi_1, \xi_2, \xi_3, \ldots) \in \mathcal{X}\colon\ \xi_1 = 0\}$.

Problem 2.8. Let $\mathcal{X}$ be a nonzero linear space over an *infinite* field, and let B be a Hamel basis for $\mathcal{X}$. Recall that every nonzero vector x in $\mathcal{X}$ has a unique representation in terms of B. That is, for each $x \neq 0$ in $\mathcal{X}$ there exists a unique nonempty finite subset B_x of B and a unique finite family of nonzero scalars $\{\alpha_b\}_{b\in B_x} \subset \mathbb{F}$ such that

$$x = \sum_{b\in B_x} \alpha_b b.$$

For each positive integer $n \in \mathbb{N}$ let X_n be the set of all *nonzero* vectors in $\mathcal{X}$ whose representations as a (finite) linear combination of vectors in B have exactly n (nonzero) summands. That is, for each $n \in \mathbb{N}$, set

$$X_n = \big\{x \in \mathcal{X}\colon\ \#B_x = n\big\}.$$

(a) Prove that $\#X_n = \#(\mathbb{F}\times B)$ for all $n \in \mathbb{N}$.

Hint: Show that $\#X_n = \#(\mathbb{F}^n\times B)$ and recall: if $\mathbb{F}$ is an infinite set, then $\#\mathbb{F}^n = \#\mathbb{F}$ (Problems 1.23 and 1.28).

(b) Apply Theorem 1.10 to show that $\#\big(\bigcup_{n\in\mathbb{N}} X_n\big) \le \#(\mathbb{F}\times B)$.

(c) Verify that $\{X_n\}_{n\in\mathbb{N}}$ is a partition of $\mathcal{X}\backslash\{0\}$.

Thus conclude from (b) and (c) (see Problem 1.28(a)) that

$$\#\mathcal{X} = \#(\mathbb{F}\times B) = \max\{\#\mathbb{F}, \dim\mathcal{X}\}.$$

Problem 2.9. Prove the following proposition, which is known as the *Principle of Superposition*. A mapping $L\colon \mathcal{X} \to \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ are linear spaces over the same scalar field, is a linear transformation if and only if

$$L\Big(\sum_{i=1}^{n} \alpha_i x_i\Big) = \sum_{i=1}^{n} \alpha_i L x_i$$

for all *finite* sets $\{x_i\}_{i=1}^n$ of vectors in $\mathcal{X}$ and all *finite* sets of scalars $\{\alpha_i\}_{i=1}^n$.

Problem 2.10. Let $L\colon \mathcal{X} \to \mathcal{Y}$ be a linear transformation.

(a) Show that the null space $\mathcal{N}(L)$ and the range $\mathcal{R}(L)$ of L are linear manifolds of the linear spaces $\mathcal{X}$ and $\mathcal{Y}$, respectively. Moreover, show that they both are L-invariant. That is, $L(\mathcal{N}(L)) \subseteq \mathcal{N}(L)$ and $L(\mathcal{R}(L)) \subseteq \mathcal{R}(L)$.

Now set $\mathcal{X} = \mathcal{Y}$ and show that the positive integral powers of L are linear transformations. That is, $L^n \in \mathcal{L}[\mathcal{X}]$ for every $n \ge 1$ whenever $L \in \mathcal{L}[\mathcal{X}]$.

(b) Show that the linear manifolds $\mathcal{N}(L^n)$ and $\mathcal{R}(L^n)$ are L-invariant. That is, $L(\mathcal{N}(L^n)) \subseteq \mathcal{N}(L^n)$ and $L(\mathcal{R}(L^n)) \subseteq \mathcal{R}(L^n)$ for every $n \ge 1$.

(c) Show that L^n is injective or surjective if L is. That is, $\mathcal{N}(L) = \{0\}$ implies $\mathcal{N}(L^n) = \{0\}$, and $\mathcal{R}(L) = \mathcal{X}$ implies $\mathcal{R}(L^n) = \mathcal{X}$, for every $n \ge 1$.

Problem 2.11. Let $L\colon \mathcal{X} \to \mathcal{Y}$ be a linear transformation of a linear space $\mathcal{X}$ into a linear space $\mathcal{Y}$. Prove the following propositions.

(a) If $\mathcal{M}$ is a linear manifold of $\mathcal{X}$, then $L(\mathcal{M})$ is a linear manifold of $\mathcal{Y}$ (i.e., the linear image of a linear manifold is a linear manifold).

(b) If $\mathcal{N}$ is a linear manifold of $\mathcal{Y}$, then $L^{-1}(\mathcal{N})$ is a linear manifold of $\mathcal{X}$ (i.e., the inverse image of a linear manifold under a linear transformation is again a linear manifold).

Problem 2.12. Let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces, and let $L\colon \mathcal{X} \to \mathcal{Y}$ be a linear transformation. Show that the following assertions are equivalent.

(a) $A \subseteq \mathcal{X}$ is a linear manifold whenever $L(A) \subseteq \mathcal{Y}$ is a linear manifold.

(b) $\mathcal{N}(L) = \{0\}$.

Hint: Give a direct proof for (b)$\Rightarrow$(a) by using Problems 1.3(d) and 2.11(b). Give a contrapositive proof for (a)$\Rightarrow$(b) — recall: if x is a nonzero vector in $\mathcal{X}$, then $\{x\}$ is not a linear manifold of $\mathcal{X}$.

Problem 2.13. Prove that the set $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ of all linear transformations of a linear space $\mathcal{X}$ into a linear space $\mathcal{Y}$ is itself a linear space (over the same common field of $\mathcal{X}$ and $\mathcal{Y}$) when vector addition and scalar multiplication in $\mathcal{L}[\mathcal{X}, \mathcal{Y}]$ are defined pointwise as in Example 2.F.

Problem 2.14. Show that the restriction $L|_{\mathcal{M}}\colon \mathcal{M} \to \mathcal{Y}$ of a linear transformation $L\colon \mathcal{X} \to \mathcal{Y}$ to a linear manifold $\mathcal{M}$ of $\mathcal{X}$ is itself a linear transformation. Moreover, also show that $\mathcal{N}(L|_{\mathcal{M}}) = \mathcal{M} \cap \mathcal{N}(T)$.

Problem 2.15. Show that the composition of two linear transformations is again a linear transformation. That is, if $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are linear spaces over the same scalar field, and if $L \in \mathcal{L}[\mathcal{X}, \mathcal{Y}]$ and $T \in \mathcal{L}[\mathcal{Y}, \mathcal{Z}]$, then $TL \in \mathcal{L}[\mathcal{X}, \mathcal{Z}]$. Moreover, also show that $\mathcal{R}(TL) = T(\mathcal{R}(L))$.

Problem 2.16. Let $L\colon \mathcal{X} \to \mathcal{Y}$ be a linear transformation. It is trivially verified that, if L is surjective, then $\dim \mathcal{R}(L) = \dim \mathcal{Y}$. Now verify that, if L is injective, then $\dim \mathcal{R}(L) = \dim \mathcal{X}$.

Problem 2.17. Let $L\colon \mathcal{X} \to \mathcal{Y}$ be a linear transformation of a linear space $\mathcal{X}$ into a linear space $\mathcal{Y}$. The dimension of the range of L is the *rank* of L, and the dimension of the null space of L is the *nullity* of L. Show that rank and nullity are related as follows.

$$\dim \mathcal{N}(L) + \dim \mathcal{R}(L) \;=\; \dim \mathcal{X}.$$

Hint: Suppose $L \neq O$. Let B_N be a Hamel basis for $\mathcal{N}(L)$ and let B_X be a Hamel basis for $\mathcal{X}$ that properly includes B_N. (Theorem 2.5 — why is the inclusion proper?) Set $B_M = B_X \backslash B_N$ and $\mathcal{M} = \operatorname{span} B_M$. Show that B_M is a Hamel basis for $\mathcal{M}$, the restriction of L to $\mathcal{M}$ is injective (since $\mathcal{N}(L)$ and $\mathcal{M}$

are algebraic complements by Proposition 2.15), and $L|_{\mathcal{M}}: \mathcal{M} \to \mathcal{R}(L)$ is an isomorphism (Problem 2.14). Thus $\dim \mathcal{R}(L) = \dim \mathcal{M}$ (Theorem 2.12), and $\dim \mathcal{X} = \#B_X = \#B_N + \#B_M = \dim \mathcal{N}(L) + \dim \mathcal{M}$ (Problem 1.30).

Problem 2.18. If $\dim \mathcal{R}(L)$ is finite, then L is called a *finite-dimensional* (or a *finite-rank*) *linear transformation*. Clearly, if $\mathcal{Y}$ is a finite-dimensional linear space, then every $L \in \mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is finite dimensional. Verify that, if $\mathcal{X}$ is a finite-dimensional linear space, then every $L \in \mathcal{L}[\mathcal{X}, \mathcal{Y}]$ is finite dimensional. Moreover, if $L: \mathcal{X} \to \mathcal{Y}$ is a finite-dimensional linear transformation (so that $\mathcal{R}(L)$ is a finite-dimensional linear manifold of $\mathcal{Y}$), then show that

(a) L is injective if and only if $\dim \mathcal{R}(L) = \dim \mathcal{X}$,

(b) L is surjective if and only if $\dim \mathcal{R}(L) = \dim \mathcal{Y}$,

(c) L is injective if and only if it is surjective, whenever $\dim \mathcal{X} = \dim \mathcal{Y}$.

Problem 2.19. Let $\mathcal{X}$ be a linear space over a field $\mathbb{F}$ and let $\mathcal{X}^{\mathbb{N}_0}$ be the linear space (over the same field $\mathbb{F}$) of all $\mathcal{X}$-valued sequences $\{x_n\}_{n \in \mathbb{N}_0}$. Take a linear transformation of $\mathcal{X}$ into itself, $A \in \mathcal{L}[\mathcal{X}]$, and an arbitrary sequence $u = \{u_n\}_{n \in \mathbb{N}_0}$ in $\mathcal{X}^{\mathbb{N}_0}$. Consider the (unique) sequence $x = \{x_n\}_{n \in \mathbb{N}_0}$ in $\mathcal{X}^{\mathbb{N}_0}$ which is recursively defined as follows. Set $x_0 = u_0$ and, for each $n \in \mathbb{N}_0$, set

$$x_{n+1} \;=\; Ax_n + u_{n+1}.$$

As usual, let A^n denote the composition of A with itself n times for each integer $n \geq 0$, with $A^0 = I$, the identity in $\mathcal{L}[\mathcal{X}]$. Prove by induction that

$$x_n \;=\; \sum_{i=0}^{n} A^{n-i} u_i$$

for every $n \in \mathbb{N}_0$. Now let $L: \mathcal{X}^{\mathbb{N}_0} \to \mathcal{X}^{\mathbb{N}_0}$ be the map that assigns to each sequence u in $\mathcal{X}^{\mathbb{N}_0}$ this unique sequence x in $\mathcal{X}^{\mathbb{N}_0}$, so that

$$x \;=\; Lu.$$

Show that L is a linear transformation of $\mathcal{X}^{\mathbb{N}_0}$ into itself. The recursive equation (or the *difference equation*) $x_{n+1} = Ax_n + u_{n+1}$ is called a *discrete linear dynamical system* because L is *linear*. Its unique solution is given by $x = Lu$ (i.e., $x_n = \sum_{i=0}^{n} A^{n-i} u_i$ for every $n \in \mathbb{N}_0$).

Problem 2.20. Let $\mathbb{F}$ denote either the real or complex field, and let $\mathcal{X}$ and $\mathcal{Y}$ be linear spaces over $\mathbb{F}$. For any polynomial p (in one variable in $\mathbb{F}$ with coefficients α_i in $\mathbb{F}$ and of finite order n; i.e., $p(z) = \sum_{i=0}^{n} \alpha_i z^i$ for $z \in \mathbb{F}$), set

$$p(L) \;=\; \sum_{i=0}^{n} \alpha_i L^i,$$

where $L \in \mathcal{L}[\mathcal{X}]$ and $\{\alpha_i\}_{i=0}^n$ is a finite set of coefficients in $\mathbb{F}$ (note: $L^0 = I$). Show that $p(L) \in \mathcal{L}[\mathcal{X}]$ (in particular, $L^n \in \mathcal{L}[\mathcal{X}]$ for each $n \geq 0$) for every $L \in \mathcal{L}[\mathcal{X}]$. Take $L \in \mathcal{L}[\mathcal{X}]$, $K \in \mathcal{L}[\mathcal{Y}]$, and $M \in \mathcal{L}[\mathcal{X}, \mathcal{Y}]$. Prove the implication.

(a) If $ML = KM$, then $Mp(L) = p(K)M$ for any polynomial p.

Thus conclude: $p(L)$ *is similar to* $p(K)$ *whenever* L *is similar to* K. A linear transformation L in $\mathcal{L}[\mathcal{X}]$ is called *nilpotent* if $L^n = O$ for some integer $n \in \mathbb{N}$, and *algebraic* if $p(L) = O$ for some polynomial p. It is clear that every nilpotent linear transformation is algebraic. Prove the following propositions.

(b) A linear transformation is similar to an algebraic (nilpotent) linear transformation if and only if it is itself algebraic (nilpotent).

(c) Sum and composition of nilpotent linear transformations are not necessarily nilpotent.

Hint: The matrices $T = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $L = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ in $\mathcal{L}[\mathbb{C}^2]$ are both nilpotent. $L + T$ is an involution. LT and TL are idempotent.

Problem 2.21. Let $\mathbb{F}$ denote either the real or complex field, and let $\mathcal{X}$ be a linear space over $\mathbb{F}$. A subset K of $\mathcal{X}$ is a *cone* (with vertex at the origin) if $\alpha x \in K$ whenever $x \in K$ and $\alpha \geq 0$. Recall the definition of a convex set in Problem 2.2 and verify the following assertions.

(a) Every linear manifold is a convex cone.

(b) The union of nonzero disjoint linear manifolds is a nonconvex cone.

Let S be a nonempty set and consider the linear space $\mathbb{F}^S$. Show that

(c) $\{x \in \mathbb{F}^S\colon\, x(s) \geq 0 \text{ for all } s \in S\}$ is a convex cone in $\mathbb{F}^S$.

Problem 2.22. Show that the implication (a)$\Rightarrow$(b) in Theorem 2.14 does not generalize to three linear manifolds, say $\mathcal{M}$, $\mathcal{N}$, and $\mathcal{R}$, if we simply assume that they are pairwise disjoint. (*Hint*: $\mathbb{R}^3$.)

Problem 2.23. Let $\{\mathcal{M}_i\}_{i=1}^n$ be a finite collection of linear manifolds of a linear space $\mathcal{X}$. Show that the following assertions are equivalent.

(a) $\mathcal{M}_i \cap \sum_{j=1, j\neq i}^n \mathcal{M}_j = \{0\}$ for every $i = 1, \ldots, n$.

(b) For each x in $\sum_{i=1}^n \mathcal{M}_i$ there exists a unique n-tuple $(x_1, \ldots, x_n)$ in $\prod_{i=1}^n \mathcal{M}_i$ such that $x = \sum_{i=1}^n x_i$.

Hint: (a)$\Rightarrow$(b) for $n = 2$ by Theorem 2.14. Take any integer $n > 2$ and suppose (a)$\Rightarrow$(b) for every $2 \leq m < n$. Show that, if (a) holds true for $m + 1$, then (b) holds true for $m + 1$. Now conclude the proof of (a)$\Rightarrow$(b) by induction in n. Next show that (b)$\Rightarrow$(a) by Theorem 2.14.

Problem 2.24. Let $\{\mathcal{M}_i\}_{i=1}^n$ be a finite collection of linear manifolds of a linear space $\mathcal{X}$, and let B_i be a Hamel basis for each $\mathcal{M}_i$. If $\mathcal{M}_i \cap \sum_{j=1, j\neq i}^n \mathcal{M}_j = \{0\}$ for every $i = 1, \ldots, n$, then $\bigcup_{i=1}^n B_i$ is a Hamel basis for $\sum_{i=1}^n \mathcal{M}_i$. Prove.

Hint: Apply Proposition 2.15 for $n = 2$. Now use the hint to Problem 2.23.

Problem 2.25. Let $\mathcal{M}$ and $\mathcal{N}$ be linear manifolds of a linear space.

(a) If $\mathcal{M}$ and $\mathcal{N}$ are disjoint, then

$$\dim(\mathcal{M} \oplus \mathcal{N}) \,=\, \dim(\mathcal{M} + \mathcal{N}) \,=\, \dim \mathcal{M} + \dim \mathcal{N}.$$

Hint: Problem 1.30, Theorem 2.14, and Proposition 2.15.

(b) If $\mathcal{M}$ and $\mathcal{N}$ are finite-dimensional, then

$$\dim(\mathcal{M} + \mathcal{N}) \,=\, \dim \mathcal{M} + \dim \mathcal{N} - \dim(\mathcal{M} \cap \mathcal{N}).$$

Problem 2.26. Let $\mathcal{M}$ be a proper linear manifold of a linear space $\mathcal{X}$ so that $\mathcal{M} \in \mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$. Consider the inclusion ordering of $\mathcal{L}at(\mathcal{X})$. Show that

$$\mathcal{M} \text{ is maximal in } \mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\} \quad\iff\quad \operatorname{codim} \mathcal{M} = 1.$$

Problem 2.27. Let φ be a nonzero linear functional on a linear space $\mathcal{X}$ (i.e., a nonzero element of $\mathcal{X}'$, the algebraic dual of $\mathcal{X}$). Prove the following results.

(a) $\mathcal{N}(\varphi)$ is maximal in $\mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$.

That is, the null space of every nonzero linear functional in $\mathcal{X}'$ is a maximal proper linear manifold of $\mathcal{X}$. Conversely, if $\mathcal{M}$ is a maximal linear manifold in $\mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$, then there exists a nonzero φ in $\mathcal{X}'$ such that $\mathcal{M} = \mathcal{N}(\varphi)$.

(b) Every maximal element of $\mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$ is the null space of some nonzero φ in $\mathcal{X}'$.

Problem 2.28. Let $\mathcal{X}$ be a linear space over a field $\mathbb{F}$. The set

$$H_{\varphi,\alpha} \,=\, \big\{x \in \mathcal{X}\colon\; \varphi(x) = \alpha\big\},$$

determined by a *nonzero* φ in $\mathcal{X}'$ and a scalar α in $\mathbb{F}$, is called a *hyperplane* in $\mathcal{X}$. It is clear that $H_{\varphi,0}$ coincides with $\mathcal{N}(\varphi)$ but $H_{\varphi,\alpha}$ is not a linear manifold of $\mathcal{X}$ if α is a nonzero scalar. A *linear variety* is a translation of a proper linear manifold. That is, a linear variety V is a subset of $\mathcal{X}$ that coincides with the coset of x modulo $\mathcal{M}$,

$$V \,=\, \mathcal{M} + x \,=\, \big\{y \in \mathcal{X}\colon\; y = z + x \text{ for some } z \in \mathcal{M}\big\},$$

for some $x \in \mathcal{X}$ and some $\mathcal{M} \in \mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$. If $\mathcal{M}$ is maximal in $\mathcal{L}at(\mathcal{X})\backslash\{\mathcal{X}\}$, then $\mathcal{M} + x$ is called a *maximal linear variety*. Show that a hyperplane is precisely a maximal linear variety.

Problem 2.29. Let $\mathcal{X}$ be a linear space over a field $\mathbb{F}$, and let P and E be projections in $\mathcal{L}[\mathcal{X}]$. Suppose $E \neq O$, and let α be an arbitrary *nonzero* scalar in $\mathbb{F}$. Prove the following proposition.

(a) $P + \alpha E$ is a projection if and only if $PE + EP = (1 - \alpha)E$.

Moreover, if $P + \alpha E$ is a projection, then show that

(b) P and E commute (i.e., $PE = EP$), and so PE is a projection;

(c) $PE = O$ if and only if $\alpha = 1$ and $PE \neq O$ if and only if $\alpha = -1$.

Therefore,

(d) $P + \alpha E$ is a projection implies $\alpha = 1$ or $\alpha = -1$.

Thus conclude:

(e) $P + E$ is a projection if and only if $PE = EP = O$,

(f) $P - E$ is a projection if and only if $PE = EP = E$.

Next prove that, for arbitrary projections P and E in $\mathcal{L}[\mathcal{X}]$,

(g) $\mathcal{R}(P) \cap \mathcal{R}(E) \subseteq \mathcal{R}(PE) \cap \mathcal{R}(EP)$.

Furthermore, if P and E commute, then show that

(h) PE is a projection and $\mathcal{R}(P) \cap \mathcal{R}(E) = \mathcal{R}(PE)$,

and so (still under the assumption that E and P commute),

(i) $PE = O$ if and only if $\mathcal{R}(P) \cap \mathcal{R}(E) = \{0\}$.

Problem 2.30. An *algebra* (or a *linear algebra*) is a linear space $\mathcal{A}$ that is also a ring with respect to a second binary operation on $\mathcal{A}$ called *product* (notation: $xy \in \mathcal{A}$ is the product of $x \in \mathcal{A}$ and $y \in \mathcal{A}$). The product is related to scalar multiplication by the property

$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

for every $x, y \in \mathcal{A}$ and every scalar α. We shall refer to a *real* or *complex algebra* if $\mathcal{A}$ is a real or complex linear space. Recall that this new binary operation on $\mathcal{A}$ (i.e., the product in the ring $\mathcal{A}$) is associative,

$$x(yz) = (xy)z,$$

and distributive with respect to vector addition,

$$x(y + z) = xy + xz \quad \text{and} \quad (y + z)x = yx + zx,$$

for every x, y, and z in $\mathcal{A}$. If $\mathcal{A}$ possesses a neutral element 1 under the product operation (i.e., if there exists $1 \in \mathcal{A}$ such that $x1 = 1x = x$ for every $x \in \mathcal{A}$), then $\mathcal{A}$ is said to be an *algebra with identity* (or a *unital algebra*). Such a neutral element 1 is called the *identity* (or *unit*) of $\mathcal{A}$. If $\mathcal{A}$ is an algebra with identity, and if $x \in \mathcal{A}$ has an *inverse* (denoted by x^{-1}) with respect to the product operation (i.e., if there exists $x^{-1} \in \mathcal{A}$ such that $xx^{-1} = x^{-1}x = 1$), then x is an *invertible* element of $\mathcal{A}$. Recall that the identity is unique if it exists, and so is the inverse of an invertible element of $\mathcal{A}$. If the product operation is commutative, then $\mathcal{A}$ is said to be a *commutative algebra*.

(a) Let $\mathcal{X}$ be a linear space of dimension greater than 1. Show that $\mathcal{L}[\mathcal{X}]$ is a noncommutative algebra with identity when the product in $\mathcal{L}[\mathcal{X}]$ is interpreted as composition (i.e., $LT = L \circ T$ for every $L, T \in \mathcal{L}[\mathcal{X}]$). The identity I in $\mathcal{L}[\mathcal{X}]$ is precisely the neutral element under the product operation. L is an invertible of $\mathcal{L}[\mathcal{X}]$ if and only if L is injective and surjective.

A *subalgebra* of $\mathcal{A}$ is a linear manifold $\mathcal{M}$ of $\mathcal{A}$ (when $\mathcal{A}$ is viewed as a linear space) which is an algebra in its own right with respect to the product operation of $\mathcal{A}$ (i.e., $uv \in \mathcal{M}$ whenever $u \in \mathcal{M}$ and $v \in \mathcal{M}$). A subalgebra $\mathcal{M}$ of $\mathcal{A}$ is a *left ideal* of $\mathcal{A}$ if $ux \in \mathcal{M}$ whenever $u \in \mathcal{M}$ and $x \in \mathcal{A}$. A *right ideal* of $\mathcal{A}$ is a subalgebra $\mathcal{M}$ of $\mathcal{A}$ such that $xu \in \mathcal{M}$ whenever $x \in \mathcal{A}$ and $u \in \mathcal{M}$. An *ideal* (or a *two-sided ideal* or a *bilateral ideal*) of $\mathcal{A}$ is a subalgebra $\mathcal{I}$ of $\mathcal{A}$ that is both a left ideal and a right ideal.

(b) Let $\mathcal{X}$ be an infinite-dimensional linear space. Show that the set of all finite-dimensional linear transformations in $\mathcal{L}[\mathcal{X}]$ is a proper left ideal of $\mathcal{L}[\mathcal{X}]$ with no identity. (*Hint*: Problem 2.25(b).)

(c) Show that, if $\mathcal{A}$ is an algebra and $\mathcal{I}$ is a proper ideal of $\mathcal{A}$, then the quotient space $\mathcal{A}/\mathcal{I}$ of $\mathcal{A}$ modulo $\mathcal{I}$ is an algebra. This is called the *quotient algebra* of $\mathcal{A}$ with respect to $\mathcal{I}$. If $\mathcal{A}$ has an identity 1, then the coset $1 + \mathcal{I}$ is the identity of $\mathcal{A}/\mathcal{I}$.

Hint: Recall that vector addition and scalar multiplication in the linear space $\mathcal{A}/\mathcal{I}$ are defined by

$$(x + \mathcal{I}) + (y + \mathcal{I}) \;=\; (x + y) + \mathcal{I},$$
$$\alpha(x + \mathcal{I}) \;=\; \alpha x + \mathcal{I},$$

for every $x, y \in \mathcal{A}$ and every scalar α (see Example 2.H). Now show that the product of cosets in $\mathcal{A}/\mathcal{I}$ can be likewise defined by

$$(x + \mathcal{I})(y + \mathcal{I}) \;=\; xy + \mathcal{I}$$

for every $x, y \in \mathcal{A}$ (i.e., if $x' = x + u$ and $y' = y + v$, with $x, y \in \mathcal{A}$ and $u, v \in \mathcal{I}$, then there exists $z \in \mathcal{I}$ such that $x'y' + w = xy + z$ for any $w \in \mathcal{I}$, whenever $\mathcal{I}$ is a two-sided ideal of $\mathcal{A}$).

Problem 2.31. Let $\mathcal{A}$ and $\mathcal{B}$ be algebras over the same scalar field. A linear transformation $\Phi\colon \mathcal{A} \to \mathcal{B}$ (of the linear spaces $\mathcal{A}$ into the linear space $\mathcal{B}$) that preserves products — i.e., such that $\Phi(xy) = \Phi(x)\Phi(y)$ for every x, y in $\mathcal{A}$

— is called a *homomorphism* (or an *algebra homomorphism*) of $\mathcal{A}$ into $\mathcal{B}$. A *unital homomorphism* between unital algebras is one that takes the identity of $\mathcal{A}$ to the identity of $\mathcal{B}$. If $\varPhi$ is an isomorphism (of the linear spaces $\mathcal{A}$ onto the linear space $\mathcal{B}$) and also a homomorphism (of the algebra $\mathcal{A}$ onto the algebra $\mathcal{B}$), then it is an *algebra isomorphism* of $\mathcal{A}$ onto $\mathcal{B}$. In this case $\mathcal{A}$ and $\mathcal{B}$ are said to be *isomorphic algebras*.

(a) Let $\{e_\gamma\}$ be a Hamel basis for the linear space $\mathcal{A}$. Show that a linear transformation $\varPhi\colon \mathcal{A} \to \mathcal{B}$ is an algebra isomorphism if and only if $\varPhi(e_\alpha e_\beta) = \varPhi(e_\alpha)\varPhi(e_\alpha)$ for every pair $\{e_\alpha, e_\beta\}$ of elements of the basis $\{e_\gamma\}$.

(b) Let $\mathcal{I}$ be an ideal of $\mathcal{A}$ and let $\pi\colon \mathcal{A} \to \mathcal{A}/\mathcal{I}$ be the natural mapping of $\mathcal{A}$ onto the quotient algebra $\mathcal{A}/\mathcal{I}$. Show that π is a homomorphism such that $\mathcal{N}(\pi) = \mathcal{I}$. (*Hint*: Example 2.H.)

(c) Let $\mathcal{X}$ and $\mathcal{Y}$ be isomorphic linear spaces and let $W\colon \mathcal{X} \to \mathcal{Y}$ be an isomorphism between them. Consider the mapping $\varPhi\colon \mathcal{L}[\mathcal{X}] \to \mathcal{L}[\mathcal{Y}]$ defined by $\varPhi(L) = WLW^{-1}$ for every $L \in \mathcal{L}[\mathcal{X}]$. Show that $\varPhi$ is an algebra isomorphism of the algebra $\mathcal{L}[\mathcal{X}]$ onto the algebra $\mathcal{L}[\mathcal{Y}]$.

Problem 2.32. Here is a useful result, which holds in any ring with identity (sometimes referred to as the *Matrix Inversion Lemma*). Take $A, B \in \mathcal{L}[\mathcal{X}]$ on a linear space $\mathcal{X}$. If $I - AB$ is invertible, then so is $I - BA$, and

$$(I - BA)^{-1} \;=\; I + B(I - AB)^{-1}A.$$

Hint: For every $A, B, C \in \mathcal{L}[\mathcal{X}]$ verify that

(a) $(I + BCA)(I - BA) = I - BA + BCA - BCABA$,

(b) $(I - BA)(I + BCA) = I - BA + BCA - BABCA$,

(c) $I - BA + BCA - B(C - I)A = I$.

Now set $C = (I - AB)^{-1}$ so that $C(I - AB) = I = (I - AB)C$, and hence

(d) $CAB = C - I = ABC$.

Thus conclude that

(e) $(I + BCA)(I - BA) = I = (I - BA)(I + BCA)$.

Problem 2.33. Take a linear transformation $L \in \mathcal{L}[\mathcal{X}]$ on a linear space $\mathcal{X}$ and consider its nonnegative integral powers L^n. Verify that, for every $n \ge 0$,

$$\mathcal{N}(L^n) \subseteq \mathcal{N}(L^{n+1}) \quad \text{and} \quad \mathcal{R}(L^{n+1}) \subseteq \mathcal{R}(L^n).$$

Let n_0 be an arbitrary nonnegative integer. Prove the following propositions.

(a) If $\mathcal{N}(L^{n_0+1}) = \mathcal{N}(L^{n_0})$, then $\mathcal{N}(L^{n+1}) = \mathcal{N}(L^n)$ for every integer $n \ge n_0$.

(b) If $\mathcal{R}(L^{n_0+1}) = \mathcal{R}(L^{n_0})$, then $\mathcal{R}(L^{n+1}) = \mathcal{R}(L^n)$ for every integer $n \ge n_0$.

Hint: Rewrite the statements in (a) and (b) as follows.

(a) If $\mathcal{N}(L^{n_0+1}) = \mathcal{N}(L^{n_0})$, then $\mathcal{N}(L^{n_0+k+1}) = \mathcal{N}(L^{n_0+k})$ for every $k \geq 1$.

(b) If $L^{n_0+1}(\mathcal{X}) = L^{n_0}(\mathcal{X})$, then $L^{n_0+k+1}(\mathcal{X}) = L^{n_0+k}(\mathcal{X})$ for every $k \geq 1$.

Show that (a) holds for $k = 1$. Now show that the conclusion in (a) holds for $k+1$ whenever it holds for k. Similarly, show that (b) holds for $k = 1$, then show that the conclusion in (b) holds for $k+1$ whenever it holds for k. Thus conclude the proof of (a) and (b) by induction.

Problem 2.34. Set $\overline{\mathbb{N}}_0 = \mathbb{N}_0 \cup \infty$, the set of all *extended nonnegative integers* with its natural (extended) ordering. The previous problem suggests the following definitions. The *ascent* of $L \in \mathcal{L}[\mathcal{X}]$ (notation: $\operatorname{asc}(L)$) is the least nonnegative integer such that $\mathcal{N}(L^{n+1}) = \mathcal{N}(L^n)$, and the *descent* of L (notation: $\operatorname{dsc}(L)$) is the least nonnegative integer such that $\mathcal{R}(L^{n+1}) = \mathcal{R}(L^n)$:

$$\operatorname{asc}(L) = \min\big\{n \in \overline{\mathbb{N}}_0\colon\ \mathcal{N}(L^{n+1}) = \mathcal{N}(L^n)\big\},$$
$$\operatorname{dsc}(L) = \min\big\{n \in \overline{\mathbb{N}}_0\colon\ \mathcal{R}(L^{n+1}) = \mathcal{R}(L^n)\big\}.$$

It is plain that

$$\operatorname{asc}(L) = 0 \quad\Longleftrightarrow\quad \mathcal{N}(L) = \{0\},$$
$$\operatorname{dsc}(L) = 0 \quad\Longleftrightarrow\quad \mathcal{R}(L) = \mathcal{X}.$$

Now prove the following propositions.

(a) $\operatorname{asc}(L) < \infty$ and $\operatorname{dsc}(L) = 0$ implies $\operatorname{asc}(L) = 0$.

Hint: Suppose $\operatorname{dsc}(L) = 0$ (i.e., suppose $\mathcal{R}(L) = \mathcal{X}$). If $\operatorname{asc}(L) \neq 0$ (i.e., if $\mathcal{N}(L) \neq \{0\}$), then take $0 \neq x_1 \in \mathcal{N}(L) \cap \mathcal{R}(L)$ and x_2, x_3 in $\mathcal{R}(L) = \mathcal{X}$ such that $x_1 = Lx_2$ and $x_2 = Lx_3$, and so $x_1 = L^2x_3$. Proceed by induction to construct a sequence $\{x_n\}_{n\geq 1}$ of vectors in $\mathcal{X} = \mathcal{R}(L)$ such that $x_n = Lx_{n+1}$ and $0 \neq x_1 = L^n x_{n+1} \in \mathcal{N}(L)$, and so $L^{n+1}x_{n+1} = 0$. Then $x_{n+1} \in \mathcal{N}(L^{n+1})\backslash N(T^n)$ for each $n \geq 1$, and $\operatorname{asc}(L) = \infty$ by Problem 2.33.

(b) $\operatorname{asc}(L) < \infty$ and $\operatorname{dsc}(L) < \infty$ implies $\operatorname{asc}(L) = \operatorname{dsc}(L)$.

Hint: Set $m = \operatorname{dsc}(L)$, so that $\mathcal{R}(L^m) = \mathcal{R}(L^{m+1})$, and set $T = L|_{\mathcal{R}(L^m)}$. Since $\mathcal{R}(L^m)$ is L-invariant, $T \in \mathcal{L}[\mathcal{R}(L^m)]$ (Problem 2.10(b)). Verify that $\mathcal{R}(T) = T(\mathcal{R}(L^m)) = \mathcal{R}(TL^m) = \mathcal{R}(L^{m+1}) = \mathcal{R}(L^m)$ (see Problem 2.15). Thus conclude that $\operatorname{dsc}(T) = 0$. Since $\operatorname{asc}(T) < \infty$ (because $\operatorname{asc}(L) < \infty$), it follows by (a) that $\operatorname{asc}(T) = 0$. That is, $\mathcal{N}(T) = \{0\}$. Take $x \in \mathcal{N}(L^{m+1})$ and set $y = L^m x$ in $\mathcal{R}(L^m)$. Show that $Ty = L^{m+1}x = 0$, so $y = 0$, and hence $x \in \mathcal{N}(L^m)$. Therefore, $N(L^{m+1}) \subseteq \mathcal{N}(L^m)$. Use Problem 2.33 to conclude that $\operatorname{asc}(L) \leq m$. On the other hand, suppose $m \neq 0$ (otherwise apply (a)) and take z in $\mathcal{R}(L^{m-1})\backslash\mathcal{R}(L^m)$ so that $Lz = L(L^{m-1}u) = L^m u$ is in $\mathcal{R}(L^m)$ for $u \in \mathcal{X}$. Since $L^m(\mathcal{R}(L^m)) = \mathcal{R}(L^{2m}) = \mathcal{R}(L^m)$, infer that $Lz = L^m v$ for $v \in \mathcal{R}(L^m)$. Verify that $L^m(u - v) = 0$ and $L^{m-1}(u - v) = z - L^{m-1}v \neq 0$ (reason: since $v \in \mathcal{R}(L^m)$, $L^{m-1}v \in \mathcal{R}(L^{2m-1}) = \mathcal{R}(L^m)$ and $z \notin \mathcal{R}(L^m)$). Thus $(u - v) \in \mathcal{N}(L^m)\backslash\mathcal{N}(L^{m-1})$, and so $\operatorname{asc}(L) \geq m$.

Problem 2.35. Consider the setup of the previous problem. If $\operatorname{asc}(L)$ and $\operatorname{dsc}(L)$ are both finite, then they are equal by Problem 2.34(b). Set $m = \operatorname{asc}(L) = \operatorname{dsc}(L)$ in $\mathbb{N}$. Show that the linear manifolds $\mathcal{R}(L^m)$ and $\mathcal{N}(T^m)$ of the linear space $\mathcal{X}$ are algebraic complements of each other. That is,

$$\mathcal{R}(L^m) \cap \mathcal{N}(T^m) = \{0\} \quad \text{and} \quad \mathcal{X} = \mathcal{R}(L^m) \oplus \mathcal{N}(T^m).$$

Hint: If y is in $\mathcal{R}(T^m) \cap \mathcal{N}(L^m)$, then $y = L^m x$ for some $x \in \mathcal{X}$ and $L^m y = 0$. Verify that $x \in \mathcal{N}(L^{2m}) = \mathcal{N}(L^m)$, and infer that $y = 0$. Now consider the hint to Problem 2.34(b) with $T = L|_{\mathcal{R}(L^m)} \in \mathcal{L}[\mathcal{R}(L^m)]$. Since $\mathcal{R}(T) = \mathcal{R}(L^m)$, it follows that $\mathcal{R}(T^m) = \mathcal{R}(L^m)$ (Problem 2.10(c)). Take any $x \in \mathcal{X}$. Verify that there exists $u \in \mathcal{R}(L^m)$ such that $T^m u = L^m u = L^m x$, and so $v = x - u$ is in $\mathcal{N}(L^m)$. Thus $x = u + v \in \mathcal{R}(T^m) + \mathcal{N}(L^m)$. Finally, use Theorem 2.14.

http://www.springer.com/978-0-8176-4997-5

The Elements of Operator Theory
Kubrusly, C.
2011, XVI, 540 p., Hardcover
ISBN: 978-0-8176-4997-5
A product of Birkhäuser Basel