Chapter 3

Linear algebra I: vector spaces and operators

We define real and complex vector spaces. Using subspaces we introduce the concept of the direct sum representation of a vector space. We define spanning sets, linearly independent sets, basis vectors, and the concept of dimensionality. Linear operators are linear functions from a vector space to itself. The set of linear operators on a vector space form themselves a vector space, with a product structure that arises by the composition. While the product is associative, it is not in general commutative. We discuss when operators are injective, surjective, and invertible. We explain how operators can be represented by matrices once we have made a choice of basis vectors on the vector space. We derive the relation between matrix representations in different basis and show that traces and determinants are basis independent. Finally we discuss eigenvectors and eigenvalues of operators, connecting them to the idea of invariant subspaces.

3.1 Vector spaces and examples

In quantum mechanics the state of a physical system is a *vector* in a *complex* vector space. Observables are linear operators, in fact, Hermitian operators acting on this complex vector space. The purpose of this chapter is to learn the basics of vector spaces, the structures that can be built on those spaces, and the operators that act on them.

Complex vector spaces are somewhat different from the more familiar real vector spaces. They have more powerful properties. In order to understand complex vector spaces it is useful to compare them often to their real dimensional friends. A good fraction of the discussion in this and the following chapter was inspired by the book *Linear algebra done right*, by Sheldon Axler.

In a vector space one has vectors and numbers. We can add vectors to get vectors and we can multiply vectors by numbers to get vectors. If the numbers we use are real, we have a real vector space. If the numbers we use are complex, we have a complex vector space.

More generally, the numbers we use belong to what is called a 'field' and denoted by the letter $\mathbb{F}$. We will discuss just two cases, $\mathbb{F} = \mathbb{R}$, meaning that the numbers are real, and $\mathbb{F} = \mathbb{C}$, meaning that the numbers are complex.

The definition of a vector space is the same for $\mathbb{F}$ being $\mathbb{R}$ or $\mathbb{C}$. A vector space V is a set of vectors with an operation of **addition** (+) that assigns an element $u + v \in V$ to each $u, v \in V$. This means that V is *closed* under addition. There is also a **scalar multiplication** by elements of $\mathbb{F}$, with $av \in V$ for any $a \in \mathbb{F}$ and $v \in V$. This means the space V is *closed* under multiplication by numbers. These operations must satisfy the following additional properties:

1. $u + v = v + u \in V$ for all $u, v \in V$ (addition is commutative).
2. $u + (v + w) = (u + v) + w$ and $(ab)u = a(bu)$ for any $u, v, w \in V$ and $a, b \in \mathbb{F}$ (associativity of addition and scalar multiplication).
3. There is a vector $0 \in V$ such that $0 + u = u$ for all $u \in V$ (additive identity).
4. For each $v \in V$ there is a $u \in V$ such that $v + u = 0$ (additive inverse).
5. The element $1 \in \mathbb{F}$ satisfies $1v = v$ for all $v \in V$ (multiplicative identity).
6. $a(u+v) = au + av$ and $(a+b)v = av + bv$ for every $u, v \in V$ and $a, b \in \mathbb{F}$ (distributive property).

This definition is very efficient. Several familiar properties follow from it by short proofs (which we will not give, but are not complicated and you may try to produce):

- The additive identity is unique: any vector $0'$ that acts like 0 is actually equal to 0.
- $0v = 0$, for any $v \in V$, where the first zero is a number and the second one is a vector. This means that the number zero acts as expected when multiplying a vector.
- $a0 = 0$, for any $a \in \mathbb{F}$. Here both zeroes are vectors. This means that the zero vector multiplied by any number is still the zero vector.
- The additive inverse of any vector $v \in V$ is unique. It is denoted by $-v$ and in fact $-v = (-1)v$.

We must emphasize that while the numbers in $\mathbb{F}$ are sometimes real or complex, we *do not* speak of the vectors themselves as real or complex. A vector multiplied by a complex number, for example, is not said to be a complex vector. The vectors in a real vector space are not themselves real, nor are the vectors in a complex vector space complex.

The definition above of a vector space does introduce a multiplication of vectors. Only in very special cases there is a natural way to multiply vectors to give vectors. One such example is the cross product in three spatial dimensions.

The following are examples of vector spaces:

1. The set of N-component vectors
$$\begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix}, \quad a_i \in \mathbb{R}, \quad i = 1, 2, \ldots N\,. \tag{3.1.1}$$
form a real vector space. We add two vectors by adding the corresponding components
$$\begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_N \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_N + b_N \end{pmatrix}. \tag{3.1.2}$$
Multiplication by a number $\alpha \in \mathbb{R}$ is defined by multiplying each component by α
$$\alpha \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} = \begin{pmatrix} \alpha\, a_1 \\ \vdots \\ \alpha\, a_N \end{pmatrix} \tag{3.1.3}$$
The zero vector is the vector with the number zero for each entry. You should verify that all the axioms are then satisfied. In order to save space, many people write the vectors as rows: $(a_1, \ldots, a_N)$ and we will do so whenever possible. This is the classic example of a vector space! If all entries and numbers are complex, this would be a complex vector space.

2. Here is a slightly more unusual example in which matrices are the vectors. Consider the set of $M \times N$ matrices with complex entries
$$\begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{M1} & \ldots & a_{MN} \end{pmatrix}, \qquad a_{ij} \in \mathbb{C}\,. \tag{3.1.4}$$
We define addition as follows
$$\begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{M1} & \ldots & a_{MN} \end{pmatrix} + \begin{pmatrix} b_{11} & \ldots & b_{1N} \\ \vdots & & \vdots \\ b_{M1} & \ldots & b_{MN} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \ldots & a_{1N} + b_{1N} \\ \vdots & & \vdots \\ a_{M1} + b_{M1} & \ldots & a_{MN} + b_{MN} \end{pmatrix}. \tag{3.1.5}$$
and multiplication by a constant $f \in \mathbb{C}$ as follows
$$f \begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{M1} & \ldots & a_{MN} \end{pmatrix} = \begin{pmatrix} f a_{11} & \ldots & f a_{1N} \\ \vdots & & \vdots \\ f a_{M1} & \ldots & f a_{MN} \end{pmatrix}. \tag{3.1.6}$$
The zero matrix is defined as the matrix all of whose entries is the number zero. With these definitions the set of $M \times N$ matrices forms a complex vector space.

3. Consider the set of $N \times N$ hermitian matrices. These are matrices with complex entries that are left invariant by the successive operations of transposition and complex conjugation. Curiously, they form a *real* vector space. This is because multiplication by a real numbers preserves the property of hermiticity while multiplication by complex numbers does not. The set of $N \times N$ hermitian matrices form a real vector space! This illustrates the earlier claim that we should not use the labels real or complex for the vectors themselves.

4. Here comes another slightly unusual example where polynomials are the vectors. Consider the set $\mathcal{P}(\mathbb{F})$ of polynomials. A polynomial $p \in \mathcal{P}(\mathbb{F})$ is a function from $\mathbb{F}$ to $\mathbb{F}$: acting on the variable $z \in \mathbb{F}$ it gives a value $p(z) \in \mathbb{F}$. Each polynomial p is defined by coefficients $a_0, a_1, \ldots a_n \in \mathbb{F}$, with n a finite, non-negative integer:

$$p(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n \,. \tag{3.1.7}$$

   Addition of polynomials works as expected. If $p_1, p_2 \in \mathcal{P}(\mathbb{F})$ then $p_1 + p_2 \in \mathcal{P}(\mathbb{F})$ is defined by

$$(p_1 + p_2)(z) \;=\; p_1(z) + p_2(z)\,. \tag{3.1.8}$$

   and multiplication works as $(ap)(z) = ap(z)$, for $a \in \mathbb{F}$ and $p \in \mathcal{P}(\mathbb{F})$. The zero vector is the polynomial with all coefficients zero. The space $\mathcal{P}(\mathbb{F})$ of all polynomials so defined form a vector space over $\mathbb{F}$.

   This is a curious vector space because it can't be described by assembling finite size vectors from the coefficients. This vector space actually represents quite nicely the state space of the quantum harmonic oscillator!

5. The set $\mathbb{F}^\infty$ of infinite sequences $(x_1, x_2, \ldots)$ of elements $x_i \in \mathbb{F}$. Here

$$\begin{aligned}(x_1, x_2, \ldots) + (y_1, y_2, \ldots) \;&=\; (x_1 + y_1, x_2 + y_2, \ldots) \\ a(x_1, x_2, \ldots) \;&=\; (ax_1, ax_2, \ldots) \quad a \in \mathbb{F}\,.\end{aligned} \tag{3.1.9}$$

   This is a vector space over $\mathbb{F}$.

6. The set of complex functions $f(x)$ on an interval $x \in [0, L]$, form a vector space over $\mathbb{C}$. Here the functions are the vectors. The required definitions are

$$(f_1 + f_2)(x) \;=\; f_1(x) + f_2(x)\,, \quad (af)(x) \;=\; af(x) \tag{3.1.10}$$

   with $f_1(x)$ and $f_2(x)$ complex functions on the interval and a a complex number. This vector space contains, for example, the wavefunctions of a particle in a one-dimensional potential that confines it to the interval $x \in [0, L]$.

3.2 Subspaces, direct sums, and dimensionality

To better understand a vector space one can try to figure out its possible subspaces. A **subspace** of a vector space V is a subset of V that is also a vector space. To verify that a subset U of V is a subspace you must check that U contains the vector 0, and that U is closed under addition and scalar multiplication. All other properties required by the axioms for U to be a vector space are automatically satisfied because U is contained in V (think about this!).

Example. Let $V = \mathbb{R}^2$ so that elements of V are pairs (v_1, v_2) with $v_1, v_2 \in \mathbb{R}$. Introduce now the subsets W_r defined by a real number r:

$$W_r \equiv \{(v_1, v_2)\big|\ 3v_1 + 4v_2 = r,\ \text{with } r \in \mathbb{R}\} \tag{3.2.11}$$

When is W_r a subspace of $\mathbb{R}$? Since we need the zero vector $(0, 0)$ to be contained this requires $3 \cdot 0 + 4 \cdot 0 = r$ or $r = 0$. Indeed, one readily verifies that W_0 is closed under addition and scalar multiplication and is therefore a subspace of V.

It is possible to visualize all nontrivial subspaces of $\mathbb{R}^2$. These are the lines that go through the origin. Each line is a vector space: it contains the zero vector (the origin) and all vectors defined by points on the line can be added or multiplied to find vectors on the same line.

Exercise. Let U_1 and U_2 be two subspaces of V. Is $U_1 \cap U_2$ a subspace of V?

To understand a complicated vector space it is useful to consider subspaces that together build up the space. Let $U_1, \ldots U_m$ be a collection of subspaces of V. We say that the space V is the **direct sum** of the subspaces $U_1, \ldots, U_m$ and we write

$$V \ = \ U_1 \oplus \cdots \oplus U_m\,, \tag{3.2.12}$$

if any vector in V can be written *uniquely* as the sum

$$u_1 + \ldots + u_m, \quad \text{where} \ \ u_i \in U_i\,. \tag{3.2.13}$$

This can be viewed as a decomposition of any vector into a sum of vectors, one in each of the subspaces. Part of the intuition here is that while the set of all subspaces fill the whole space, the various subspaces cannot overlap. More precisely, their only common element is zero: $U_i \cap U_j = \{0\}$ for $i \neq j$. If this is violated the decomposition of vectors in V would not be unique. Indeed for some vector $v \in U_i \cap U_j$ $(i \neq j)$ then also $-v \in U_i \cap U_j$ (why?) and therefore letting $u_i \to u_i + v$ and $u_j \to u_j - v$ would leave the total sum unchanged, making the decomposition non-unique. This condition of zero mutual overlaps is necessary for the uniqueness of the decomposition but it is not in general sufficient. Except in the case when we have two summands: to show that $V = U \oplus W$, it suffices to prove that any vector can be written as $u + w$ with $u \in U$ and $w \in W$ and that $U \cap W = 0$. In general, uniqueness of the sum in (3.2.13) follows if the only way to write 0 as a sum $u_1 + \ldots + u_m$ with $u_i \in U_i$ is by taking all u_i's equal to zero. Direct sum decompositions appear rather naturally when we consider the addition of angular momentum.

Given a vector space we can produce lists of vectors. A **list** $(v_1, v_2, \ldots, v_n)$ of vectors in V contains, by definition, a finite number of vectors. The number of vectors in a list is the length of the list. The **span** of a list of vectors $(v_1, v_2, \cdots v_n)$ in V, denoted as $\text{span}(v_1, v_2, \cdots, v_n)$, is the set of all linear combinations of these vectors

$$a_1 v_1 + a_2 v_2 + \ldots a_n v_n \,, \qquad a_i \in \mathbb{F} \tag{3.2.14}$$

A vector space V is spanned by a list $(v_1, v_2, \cdots v_n)$ if $V = \text{span}(v_1, v_2, \cdots v_n)$.

Now comes a very natural definition: A vector space V is said to be **finite dimensional** if it is spanned by some list of vectors in V. If V is not finite dimensional, it is **infinite dimensional**. In such case, no list of vectors from V can span V. Note that by definition, any finite dimensional vector space has a spanning list.

Let us explain why the vector space of all polynomials $p(z)$ in Example 4 is an infinite dimensional vector space. Indeed, consider any list of polynomials. Since a list is always of finite length, there is a polynomial of maximum degree in the list. Thus polynomials of higher degree are not in the span of the list. Since no list can span the space, it is infinite dimensional.

For example 1, consider the list of vectors $(e_1, \ldots, e_N)$ with

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \,, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \,, \quad \ldots \quad e_N = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \,. \tag{3.2.15}$$

This list spans the space: the general vector displayed in (3.1.1) is $a_1 e_1 + \ldots + a_N e_N$. This vector space is therefore finite dimensional.

To make further progress we need the concept of linear independence. A list of vectors $(v_1, v_2, \ldots, v_n)$, with $v_i \in V$ is said to be **linearly independent** if the equation

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \;=\; 0 \,, \tag{3.2.16}$$

only has the solution $a_1 = a_2 = \cdots = a_n = 0$. One can prove a key result: *the length of any linearly independent list is less than or equal to the length of any spanning list.* This is reasonable, as we discuss now. Spanning lists can be enlarged as much as desired (adding vectors to a spanning list gives still a spanning list), but they cannot be reduced arbitrarily because at some point the remaining vectors will fail to span. For linearly independent lists the situation is exactly reversed: they can be easily shortened (dropping vectors will not disturb the linear independence) but cannot be enlarged arbitrarily because at some point the new vectors can be expressed in terms of those already in the list. As it happens, in a finite vector space, the length of the longest list of linearly independent vectors is the same as the length of the shortest list of spanning vectors. This leads to the concept of dimensionality, as we will see below.

We can now explain what is a basis for a vector space. A **basis** of V is a list of vectors in V that both spans V and is linearly independent. It is not hard to prove that any finite dimensional vector space has a basis. While bases are not unique, happily all bases of a finite dimensional vector space have the same length. The **dimension** of a finite-dimensional vector space is equal to the length of any list of basis vectors. If V is a space of dimension n we write $\dim V = n$. It is also true that for a finite dimensional vector space a list of vectors of length $\dim V$ is a basis if it is linearly independent list or if it is a spanning list.

In example 1 the list $(e_1, \ldots, e_N)$ in (3.2.15) is not only a spanning list but a linearly independent list (prove it!). Thus the dimensionality of this space is N.

Consider example 3 and focus on the case of the vector space of two-by-two hermitian matrices. Recall that the most general hermitian two-by-two matrix takes the form

$$\begin{pmatrix} a_0 + a_3 & a_1 - ia_2 \\ a_1 + ia_2 & a_0 - a_3 \end{pmatrix}, \qquad a_0, a_1, a_2, a_3 \in \mathbb{R}. \tag{3.2.17}$$

Now consider the following list of four 'vectors' $(\mathbf{1}, \sigma_1, \sigma_2, \sigma_3)$, with σ_i the Pauli matrices and $\mathbf{1}$ the two-by-two identity matrix. All entries in this list are hermitian matrices, so this is a list of vectors in the space. Moreover the list spans the space since the general hermitian matrix shown above is $a_0\mathbf{1} + a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3$. The list is linearly independent since

$$a_0\mathbf{1} + a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3 = 0 \quad \to \quad \begin{pmatrix} a_0 + a_3 & a_1 - ia_2 \\ a_1 + ia_2 & a_0 - a_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \tag{3.2.18}$$

and you can quickly see that this implies that a_0, a_1, a_2, and a_3 are all zero. So the list is a basis and the space in question is a four-dimensional real vector space.

Exercise. Explain why the vector space in example 2 has dimension $M \cdot N$.

The vector space $\mathbb{F}^\infty$ in example 5 is infinite dimensional, as we now justify. Assume $\mathbb{F}^\infty$ is finite dimensional, in which case it has a spanning list of some lenght n. Define s_k as the element in $\mathbb{F}^\infty$ with a 1 in the k-th position and zero elsewhere. The list $(s_1, \ldots, s_m)$ is a clearly a linearly independent list of length m, with m arbitrary. Choosing $m > n$ we have a linearly independent list longer than a spanning list. This is a contradiction, and therefore $\mathbb{F}^\infty$ cannot be finite dimensional. The space of complex functions on the interval $[0, L]$ (example 6) is also infinite dimensional.

Equipped with the concept of dimensionality there is a simple way to see if we have a direct sum decomposition of a vector space. In fact, we have $V = U_1 \oplus \cdots \oplus U_m$ if any vector in V can be written as $u_1 + \ldots + u_m$, with $u_i \in U_i$ and if $\dim U_1 + \ldots + \dim U_m = \dim V$. The proof of this result is not complicated.

3.3 Linear operators

A linear map is a particular kind of function from one vector space V to another vector space W. When the linear map takes the vector space V to itself, we call the linear map a linear operator. We will focus our attention on those operators. In quantum mechanics linear operators produce the time evolution of states. Moreover, physical observables are associated with linear operators.

A **linear operator** T on a vector space V is a function that takes V to V with the properties:

1. $T(u+v) = Tu + Tv$, for all $u, v \in V$.
2. $T(au) = aTu$, for all $a \in \mathbb{F}$ and $u \in V$.

In the above notation Tu, for example, means the result of the action of the operator T on the vector u. It could also be written as $T(u)$ but it is simpler to write it as Tu, in a way that the action of T on u looks "multiplicative".

A simple consequence of the axioms is that the action of a linear operator on the zero vector is the zero vector:

$$T\,0 \;=\; 0\,. \tag{3.3.19}$$

This follows from $Tu = T(u+0) = Tu + T\,0$, and canceling the common Tu term.

Let us consider a few examples of linear operators.

1. Let $V = \mathcal{P}[x]$ denote the space of real polynomials $p(x)$ of a real variable x with real coefficients. Here are two linear operators T and S on V:

   - Let T denote differentiation: $Tp = p'$ where $p' \equiv \frac{dp}{dx}$. This operator is linear because

   $$\begin{aligned} T(p_1+p_2) = &\;\; (p_1+p_2)' = p_1' + p_2' = Tp_1 + Tp_2\,, \\ T(ap) = &\;\; (ap)' = ap' = a\,Tp\,. \end{aligned} \tag{3.3.20}$$

   - Let S denote multiplication by x: $Sp = xp$. S is also a linear operator.

2. In the space $\mathbb{F}^\infty$ of infinite sequences define the **left-shift** operator L by

   $$L(x_1, x_2, x_3, \ldots) = (x_2, x_3, \ldots)\,. \tag{3.3.21}$$

   By shifting to the left we lose the information about the first entry, but that is perfectly consistent with linearity. We also have the **right-shift** operator R that acts as by shifting to the right and creating a new first entry as follows:

   $$R(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots)\,. \tag{3.3.22}$$

   The first entry after the action of R is zero. It could not be any other number because the zero element (a sequence of all zeroes) should be mapped to itself (by linearity).

3. For any vector space V we define the **zero operator** 0 that acting on any vector in V it maps it to the zero vector: $0v = 0$ for all $v \in V$. This map is very simple, almost trivial, but certainly linear. Note that now we have the zero number, the zero vector, and the zero operator, all denoted by 0.

4. For any vector space V we define the **identity operator** I that leaves all vectors in V invariant: $Iv = v$ for all $v \in V$.

On any vector space V there are many linear operators. We call $\mathcal{L}(V)$ the set of all linear operators on V. Since operators on V can be added and can also be multiplied by numbers, the set $\mathcal{L}(V)$ **is itself a vector space**, where the vectors are the operators. Indeed for any two operators $T, S \in \mathcal{L}(V)$ we have the natural definition

$$\begin{aligned} (S+T)v &= Sv + Tv\,, \\ (aS)v &= a(Sv)\,. \end{aligned} \tag{3.3.23}$$

A vector space must have an additive identity. Here it is an operator that can be added to other operators with no effect. The additive identity in the vector space $\mathcal{L}(V)$ is the zero operator on V, considered in example 3.

In the vector space $\mathcal{L}(V)$ there is a surprising new structure: the vectors (the operators!) can be naturally multiplied. There is a **multiplication of linear operators** that gives a linear operator: we just let one operator act first and the other next! So given $S, T \in \mathcal{L}(V)$ we define the operator ST as

$$(ST)v \equiv S(Tv)\,. \tag{3.3.24}$$

We easily verify linearity:

$$(ST)(u+v) = S(T(u+v)) = S(Tu+Tv) = S(Tu)+S(Tv) = (ST)(u)+(ST)(v) \tag{3.3.25}$$

and you can also verify that $(ST)(av) = a(ST)(v)$.

The product just introduced in the space of linear operators is **associative**. This is a fundamental property of operators and means that for S, T, U, linear operators

$$S(TU) = (ST)U\,. \tag{3.3.26}$$

This equality holds because acting on any vector v both the left-hand side and the right-hand side give $S(T(U(v)))$. The product has an identity element: the identity operator I of example 4. If we have a product we can ask if the elements (the operators) have inverses. As we will see later some operators have inverses, some do not.

Finally, and most crucially, this product is in general **noncommutative**. We can check this using the two operators T and S of example 1 acting on the polynomial $p = x^n$. Since T differentiates and S multiplies by x we get

$$\begin{aligned} (TS)x^n &= T(Sx^n) = T(x^{n+1}) = (n+1)x^n\,, \\ (ST)x^n &= S(Tx^n) = S(nx^{n-1}) = nx^n\,. \end{aligned} \tag{3.3.27}$$

We quantify the failure of commutativity by the difference $TS - ST$, which is itself a linear operator:

$$(TS - ST)x^n = (n+1)x^n - nx^n = x^n = I\, x^n\,, \tag{3.3.28}$$

where we inserted the identity operator at the last step. Since this relation is true acting on x^n, for any $n \geq 0$, it holds by linearity acting on any polynomial, namely on any element of the vector space. So we can simply write

$$[\,T\,, S\,] \;=\; I\,. \tag{3.3.29}$$

where we introduced the **commutator** $[\cdot,\cdot]$ of two linear operators X, Y, defined as

$$[X, Y] \equiv XY - YX\,. \tag{3.3.30}$$

Exercise: Calculate the commutator $[L\,, R]$ of the left-shift and right-shift operators. Express your answer using the identity operator and the operator P_1 defined by $P_1(x_1, x_2, \ldots) = (x_1, 0, 0, \ldots)$.

3.4 Null space, range, and inverses of operators

When we encounter a linear operator on a vector space there are two questions we can ask whose answers give us the most basic properties of the operator. We can ask: What vectors are mapped to zero by the operator? We can also ask: What are the vectors in V that are obtained from the action of T on V? The first question leads to the concept of null space, the second to the concept of range.

The **null space or kernel** of $T \in \mathcal{L}(V)$ is the subset of vectors in V that are mapped to zero by T:

$$\text{null}\; T \;=\; \{v \in V;\; Tv = 0\}\,. \tag{3.4.31}$$

Actually null$\,T$ is a *subspace* of V. Indeed, the null space contains the zero vector and is clearly a closed set under addition and scalar multiplication.

A linear operator $T : V \to V$ is said to be **injective** if $Tu = Tv$, with $u, v \in V$, implies $u = v$. An injective map is called a *one-to-one* map, because two different elements cannot be mapped to the same one. In fact, physicist Sean Carroll has suggested that a better name would be *two-to-two* as injectivity really means that two different elements are mapped by T to two different elements! In fact, an operator is injective if and only if its null space vanishes:

$$T \text{ injective } \iff \text{null}\,(T) = 0\,. \tag{3.4.32}$$

First prove that injectivity implies zero null space. Indeed if $v \in \text{null}(T)$ then $Tv = T0$ (both sides are zero) and injectivity shows that $v = 0$, proving that $\text{null}(T) = 0$. In the other direction, zero null space means that $T(u - v) = 0$ implies $u - v = 0$ or, equivalently, that $Tu = Tv$ implies $u = v$. This is injectivity.

As mentioned above it is also of interest to consider the elements of V of the form Tv. We define the **range** of T as the image of V under the map T:

$$\text{range}\, T \;=\; \{Tv;\; v \in V\}\,. \tag{3.4.33}$$

Actually, range T is a *subspace* of V (try proving it!). A linear operator T is said to be **surjective** if range $T = V$. That is, for a surjective T the image of V under T is the complete V.

Since both the null space and the range of a linear operator $T : V \to V$ are themselves vector spaces one can calculate their dimensions. The larger the null space of an operator, more vectors are mapped to zero, and one would expect the range to be reduced accordingly. The smaller the null space the larger we expect the range to be. This intuition can be made precise. For **any** linear operator on V the sum of the dimensions of its null space and its range is equal to the dimension of the vector space V:

$$\boxed{\dim(\text{null}\, T) \;+\; \dim(\text{range}\, T) \;=\; \dim V\,.} \tag{3.4.34}$$

We do not give the proof but sketch the main steps. Let $(e_1, \ldots, e_m)$ with $m = \dim(\text{null}\, T)$ be a basis for null(T). This basis can be extended to a basis $(e_1, \ldots, e_m, f_1, \ldots f_n)$ of the full vector space V, where $m + n = \dim V$. The final step consists in showing that the Tf_i form a basis for the range of T (this takes a bit of effort!).

Example. Let us describe the null space and range of the operator T that acts on the two-dimensional vector space $\mathbb{R}^2$:

$$T = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\,. \tag{3.4.35}$$

Consider the null space first:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \rightarrow \quad b = 0\,, \tag{3.4.36}$$

so that the general vector in the null space is $\begin{pmatrix} a \\ 0 \end{pmatrix}$ with $a \in \mathbb{R}$. Therefore

$$\text{null}\, T \;=\; \text{span}\, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; \text{span}\, e_1\,. \tag{3.4.37}$$

To find the range we act with T on a general vector:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} \;=\; \begin{pmatrix} b \\ 0 \end{pmatrix}\,, \tag{3.4.38}$$

and we conclude that

$$\text{range}\, T \;=\; \text{span}\, e_1\,. \tag{3.4.39}$$

This may seem strange: the range and null spaces are the same. But there is nothing wrong: both are one-dimensional, adding to total dimension two, as appropriate for the example. Note, however, that since $e_1 = T\,e_2$ we actually have

$$\text{range}\, T \;=\; \text{span}\, T\,e_2 \tag{3.4.40}$$

in accordance to the sketch of the argument that leads to (3.4.34).

Example. Recall the action of the left and right shift operators on infinite sequences:

$$L(x_1, x_2, x_3, \ldots) \;=\; (x_2, x_3, \ldots)\,, \qquad R(x_1, x_2, \ldots) \;=\; (0, x_1, x_2, \ldots) \tag{3.4.41}$$

We can see immediately that $\text{null}\, L = (x_1, 0, 0, \ldots)$. Being different from zero, L is not injective. But L is surjective because any sequence can be obtained by the action of L: $(x_1, x_2, \ldots) = L(x_0, x_1, x_2, \ldots)$ for arbitrary x_0. The null space of R is zero, and thus R is injective. R is not surjective: we cannot get any element whose first entry is nonzero. In summary:

$$\begin{aligned} L :&\quad \text{not injective, surjective,} \\ R :&\quad \text{injective,} \quad \text{not surjective.} \end{aligned} \tag{3.4.42}$$

Since linear operators can be multiplied, given an operator we can ask if it has an inverse. It is interesting to consider the question in some detail, as there are some possible subtleties. To do so we have to discuss left inverses and right inverses.

Let $T \in \mathcal{L}(V)$ be a linear operator. The linear operator S is a **left inverse** for T if

$$S\,T \;=\; I\,, \tag{3.4.43}$$

namely, the product of S and T with S to the left of T is equal to the identity matrix. Analogously, the linear operator S' is a **right inverse** for T if

$$T\,S' \;=\; I\,, \tag{3.4.44}$$

namely, the product of T and S' with S' to the right of T is equal to the identity matrix. If both inverses exist then they are actually equal! This is easily proven using the above defining relations and associativity of the product:

$$S' = IS' = (ST)S' = S(TS') = SI = S\,. \tag{3.4.45}$$

If both left and right inverses of T exist then T is said to be **invertible.**

The left and right inverses are relevant for systems of linear equations. Say we have $T \in \mathcal{L}(V)$ a known vector $c \in V$ and an unknown vector $x \in V$ to be determined from the equation

$$T\,x = c\,. \tag{3.4.46}$$

Suppose all you have is a left inverse S for T. Then acting with S on the equation gives you $ST\,x = Sc$ and therefore $x = Sc$. Have you solved the equation? Not quite. If you try to check that this is a solution you fail! Indeed, inserting the value $x = Sc$ on the left-hand side of the equation gives TSc, which may not equal c because S is not known to be a right inverse. All we can say is that $x = Sc$ is the *only possible solution,* given that it follows from the equation but cannot be verified to work without further analysis. If all you have is a right inverse S', you can now check that $x = S'c$ does solve the equation! This time, however, there is no guarantee that the solution is unique. Indeed, if T has a null space, the solution is clearly not unique, since any vector in the null space can be added to the solution to give another solution. Only if both left and right inverses exist we are guaranteed that a unique solution exists!

It is reasonable to ask when a linear operator $T \in \mathcal{L}(V)$ has a left inverse. Think of two pictures of V and T mapping elements from the first picture to elements on the second picture. A left inverse should map each element on the second picture back to the element it came from in the first picture. If T is not injective two different elements in the first picture are sometimes mapped to the same element in the second picture. The inverse operator can at best map back to one element so it fails to act as an inverse for the other element. This complication is genuine. A left inverse for T exists if and only if T is injective:

$$\boxed{T \text{ has a left inverse} \iff T \text{ is injective}\,.} \tag{3.4.47}$$

The proof from left to right is easy. Assume $Tv_1 = Tv_2$. Then multiply from the left by the left inverse S finding $v_1 = v_2$, which proves injectivity. To prove that injectivity implies a left inverse, we begin by considering a basis of V denoted by the collection of vectors $\{v_i\}$. We do not list the vectors because the space V could be infinite dimensional. Then define

$$Tv_i = w_i\,. \tag{3.4.48}$$

for all v_i's. One can use injectivity to show that the w_i's are linearly independent. Since the map T may not be surjective then the $\{w_i\}$ may not be a basis. They can be completed with a collection $\{y_k\}$ of vectors to form a basis for V. Then we define the action of S by saying how it acts on this basis

$$\begin{aligned} Sw_i &= \ v_i \\ S\,y_k &= \ 0\,. \end{aligned} \tag{3.4.49}$$

We then verify that

$$ST\,\Big(\sum_i a_i v_i\Big) \;=\; S\,\Big(\sum_i a_i w_i\Big) \;=\; \sum_i a_i v_i\,, \tag{3.4.50}$$

showing that $ST = I$ acting on any element of V. The action of S on the y_k had to be zero; we had no other natural option consistent with linearity. At any rate the final verification did not make use of that choice.

For the existence of a right inverse S' of T we need the operator T to be surjective:

$$\boxed{T \text{ has a right inverse} \iff T \text{ is surjective}\,.} \tag{3.4.51}$$

The necessity of subjectivity is quickly understood: if we have a right inverse we have $TS'(v) = v$, or equivalently, $T(S'v) = v$ for all $v \in V$. This says that any $v \in V$ is in the range of T. This is surjectivity of T. A more extended argument is needed to show that surjectivity implies the existence of a right inverse.

Since an operator is invertible if it has both a left and a right inverse, the two boxed results above imply that

$$T \in \mathcal{L}(V) : \quad \boxed{T \text{ is invertible}} \quad \longleftrightarrow \quad \boxed{T \text{ is injective and surjective}} \tag{3.4.52}$$

This is a completely general result, valid for infinite and finite dimensional vector spaces.

Example. Recall the properties (3.4.42) of the left and right shift operators L and R. Since L is surjective it must have a right inverse. Since R is injective it must have a left inverse. The right inverse of L is actually R and the left inverse of R is actually L. These two facts are encoded by the single equation

$$L\,R \;=\; I\,, \tag{3.4.53}$$

which is easily confirmed:

$$L\,R(x_1, x_2, \ldots,) \;=\; L(0, x_1, x_2, \ldots) = (x_1, x_2, \ldots)\,. \tag{3.4.54}$$

Neither L nor R is invertible.

When the vector space V is finite dimensional the results are simpler. Any injective operator is surjective and any surjective operator is injective. Therefore any injective operator or any surjective operator is also invertible. The following three properties are therefore completely equivalent for operators on finite-dimensional vector spaces:

$$\text{Finite dimension}\, V : \quad \boxed{T \text{ is invertible}} \quad \longleftrightarrow \quad \boxed{T \text{ is injective}} \quad \longleftrightarrow \quad \boxed{T \text{ is surjective}} \tag{3.4.55}$$

Proving these results are simple exercises.

3.5 Matrix representation of operators

To get an extra handle on linear operators we sometimes represent them as matrices. This is actually a completely general statement: after choosing a basis on the vector space V, *any* linear operator $T \in \mathcal{L}(V)$ can be represented by a particular matrix. This representation carries *all* the information about the linear operator. The matrix form of the operator can be very useful for some explicit computations. The only downside of matrix representations is that they depend on the chosen basis. On the upside, a clever choice of basis may result in a matrix representation of unusual simplicity, which can be quite valuable. Additionally, some quantities computed easily from the matrix representation of an operator do not depend on the choice of basis.

The **matrix representation** of a linear operator $T \in \mathcal{L}(V)$ is a matrix whose components $T_{ij}(\{v\})$ are read from the action of the operator T on each of the elements of a basis $(v_1, v_2, \ldots v_n)$ of V. The notation $T_{ij}(\{v\})$ reflects the fact that the matrix components depend on the choice of basis. If the choice of basis is clear by the context, we simply write the matrix components as T_{ij}. The rule that defines the matrix is simple: the j-th column of the matrix is the list of components of Tv_j when expanded along the basis.

$$\boxed{\begin{pmatrix} \ldots & \ldots & T_{1j} & \ldots \\ \ldots & \ldots & T_{2j} & \ldots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & T_{nj} & \vdots \end{pmatrix}, \qquad Tv_j \;=\; T_{1j}\,v_1 \,+\, T_{2j}\,v_2 \,+\, \ldots \,+ T_{nj}\,v_n\,.} \tag{3.5.56}$$

Example: The action of T on basis vectors (e_1, e_2, e_3) of $\mathbb{R}^3$ is given by

$$T(e_1, e_2, e_3) \;=\; (-e_1 + 7e_3\,,\, 2e_1 + e_2 + 3e_3\,,\, 6e_1 - 5e_2 + 8e_3)\,. \tag{3.5.57}$$

The matrix representation of T is then

$$\begin{pmatrix} -1 & 2 & 6 \\ 0 & 1 & -5 \\ 7 & 3 & 8 \end{pmatrix}. \tag{3.5.58}$$

This follows by direct application of the rule. From the action of T on e_1, for example, we have

$$Te_1 = -e_1 + 7e_3 = -e_1 + 0 \cdot e_2 + 7e_3 = T_{11}e_1 + T_{21}e_2 + T_{31}e_3 \tag{3.5.59}$$

allowing us to read the first column of the matrix.

The equation in (3.5.56) can be written more briefly as

$$Tv_j \;=\; \sum_{i=1}^{n} T_{ij}\,v_i\,. \tag{3.5.60}$$

Sometimes left implicit is the fact that while the operators are represented by matrices, **vectors** in V are **represented** by **column vectors**: the entries on the column vector are the components of the vector along the basis vectors. For a vector $a \in V$

$$a = a_1 v_1 + \ldots + a_n v_n \quad \longleftrightarrow \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \tag{3.5.61}$$

It is a simple consequence that the basis vector v_k is represented by a column vector of zeroes, with a one on the *k-th* entry:

$$v_k \quad \longleftrightarrow \quad \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow k\text{-}th\ entry\,. \tag{3.5.62}$$

With this you can now see why our key definition $Tv_j = \sum_{i=1}^{n} T_{ij} v_i$ is consistent with the familiar rule for multiplication of a matrix times a vector:

$$\begin{aligned} Tv_j \quad \longleftrightarrow \quad & \begin{pmatrix} T_{11} & \cdots & T_{1j} & \cdots & T_{1n} \\ T_{21} & \cdots & T_{2j} & \cdots & T_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{n1} & \cdots & T_{nj} & \cdots & T_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} j\text{-th} \;=\; \begin{pmatrix} T_{1j} \\ T_{2j} \\ \vdots \\ T_{nj} \end{pmatrix} \\ = T_{1j} & \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + T_{2j} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \ \ldots \ + T_{nj} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad \longleftrightarrow \quad T_{1j} v_1 + \ldots T_{nj} v_n \,. \end{aligned} \tag{3.5.63}$$

Exercise. Verify that in any basis the matrix representation of the identity operator is a diagonal matrix with an entry of one at each element of the diagonal.

Not only are the rules for representations consistent with the formula for multiplication of matrices times vectors, they actually *imply* this familiar formula. In fact they also imply the famous rule for matrix multiplication. We discuss both of these now.

Consider vectors a, b that expanded along the basis $(v_1, \ldots, v_n)$ read:

$$\begin{aligned} a &= a_1 v_1 + \ldots + a_n v_n \,, \\ b &= b_1 v_1 + \ldots + b_n v_n \,. \end{aligned} \tag{3.5.64}$$

Assume the vectors are related by the equation

$$b = Ta\,. \tag{3.5.65}$$

We want to see how this looks in terms of the representations of T, a, and b. We have

$$b = Ta = T \sum_j a_j v_j = \sum_j a_j \, Tv_j = \sum_{i,j} a_j \, T_{ij} v_i = \sum_i \Big(\sum_j T_{ij} a_j \Big) v_i \tag{3.5.66}$$

The object in parenthesis is the *i-th* component of b:

$$b_i \;=\; \sum_j T_{ij} a_j \,. \tag{3.5.67}$$

This is how $b = Ta$ is represented; we see on the right-hand side the familiar product of the matrix for T and the column vector for a.

Let us now examine the product of two operators and their matrix representation. Consider the operator TS acting on v_j:

$$(TS)v_j \;=\; T(Sv_j) \;=\; T\sum_p S_{pj} v_p \;=\; \sum_p S_{pj}\; Tv_p \;=\; \sum_p S_{pj}\;\sum_i T_{ip} v_i \tag{3.5.68}$$

so that changing the order of the sums we find

$$(TS)v_j \;=\; \sum_i \Bigl(\sum_p T_{ip} S_{pj}\Bigr)\, v_i \,. \tag{3.5.69}$$

Using the identification implicit in (3.5.60) we see that the object in parenthesis is $(TS)_{ij}$, the i, j element of the matrix that represents TS. Therefore we found

$$(TS)_{ij} \;=\; \sum_p T_{ip} S_{pj} \,, \tag{3.5.70}$$

which is precisely the familiar formula for matrix multiplication. The matrix that represents TS is the product of the matrix that represents T with the matrix that represents S, in that order.

Changing basis and its effect on matrix representations. While matrix representations are very useful for concrete visualization, they are basis dependent. It is a good idea to try to figure out if there are quantities that can be calculated using a matrix representation that are, nevertheless, guaranteed to be basis independent. One such quantity is the **trace** of the matrix representation of a linear operator. The trace is the sum of the matrix elements in the diagonal. Remarkably, that sum is the same independent of the basis used. This allows us to speak of the trace of an *operator*. The **determinant** of a matrix representation is also basis independent. We can therefore speak of the determinant of an operator. We will prove the basis independence of the trace and the determinant once we learn how to relate matrix representations in different basis.

Let us then consider the effect of a change of basis on the matrix representation of an operator. Consider a vector space V and two sets of basis vectors: $(v_1, \ldots v_n)$ and $(u_1, \ldots u_n)$. Consider then two linear operators $A, B \in \mathcal{L}(V)$ such that for any $i = 1, \ldots, n$, A acting on v_i gives u_i and B acting on u_i gives v_i:

$$A: \quad \begin{array}{ccc} v_1 & \ldots & v_n \\ \downarrow & \ldots & \downarrow \\ u_1 & \ldots & u_n \end{array}\,, \qquad B: \quad \begin{array}{ccc} v_1 & \ldots & v_n \\ \uparrow & \ldots & \uparrow \\ u_1 & \ldots & u_n \end{array}\;. \tag{3.5.71}$$

This can also be written as

$$Av_k = u_k\,, \qquad Bu_k = v_k\,, \quad \text{for all } k \in \{1,\ldots,n\}\,. \tag{3.5.72}$$

These relations define the operators A and B completely: we have stated how they act on basis sets. We now verify the obvious: A and B are inverses of each other. Indeed:

$$\begin{aligned} BAv_k &= B(Av_k) = Bu_k &= v_k \\ ABu_k &= A(Bu_k) = Av_k &= u_k\,, \end{aligned} \tag{3.5.73}$$

being valid for all k shows that

$$BA = I \quad \text{and} \quad AB = I\,. \tag{3.5.74}$$

Thus B is the inverse of A, and A is the inverse of B.

Operators like A or B that map one basis into another, vector by vector, have a remarkable property: *their matrix representations are the same in each of the bases they relate.* Let us prove this for A. By definition of matrix representations we have

$$A\,v_k \;=\; \sum_i A_{ik}(\{v\})v_i\,, \qquad \text{and} \qquad A\,u_k \;=\; \sum_i A_{ik}(\{u\})u_i\,. \tag{3.5.75}$$

Since $u_k = Av_k$ we then have, acting with another A,

$$Au_k = A(Av_k) = A\sum_i A_{ik}(\{v\})v_i = \sum_i A_{ik}(\{v\})\,Av_i = \sum_i A_{ik}(\{v\})\,u_i\,. \tag{3.5.76}$$

Comparison with the second equation immediately above yields the claimed

$$A_{ik}(\{u\}) = A_{ik}(\{v\})\,. \tag{3.5.77}$$

The same holds for the B operator. We can simply call A_{ij} and B_{ij} the matrices that represent A and B, because these matrices are the same in the $\{v\}$ and $\{u\}$ bases, and these are the only bases at play here. On account of (3.5.74) these are matrix inverses:

$$B_{ij}A_{jk} \;=\; \delta_{ik} \quad \text{and} \quad A_{ij}B_{jk} \;=\; \delta_{ik}\,, \tag{3.5.78}$$

and we can write $B_{ij} = (A^{-1})_{ij}$. At this point we will use the convention that repeated indices are summed over to avoid clutter.

We can now apply these preparatory results to the matrix representations of the operator T. We have, by definition,

$$Tv_k \;=\; T_{ik}(\{v\})\,v_i\,. \tag{3.5.79}$$

We need to calculate Tu_k in order to read the matrix representation of T on the u basis:

$$Tu_k \;=\; T_{ik}(\{u\})\,u_i\,. \tag{3.5.80}$$

Computing the left-hand side, using the linearity of the operator T, we have

$$Tu_k = T(A_{jk}v_j) = A_{jk}Tv_j = A_{jk}\, T_{pj}(\{v\})\, v_p\,. \tag{3.5.81}$$

We need to re-express the rightmost v_p in terms of u vectors. For this

$$v_p = Bu_p = B_{ip}\, u_i = (A^{-1})_{ip}\, u_i\,, \tag{3.5.82}$$

so that

$$Tu_k = A_{jk}\, T_{pj}(\{v\})\, (A^{-1})_{ip}\, u_i \;=\; (A^{-1})_{ip}\, T_{pj}(\{v\})\, A_{jk}\, u_i\,, \tag{3.5.83}$$

where we reordered the matrix elements to make clear the matrix products. All in all,

$$Tu_k \;=\; \big(A^{-1}T(\{v\})A\big)_{ik}\, u_i\;, \tag{3.5.84}$$

which allows us to read

$$T_{ij}(\{u\}) \;=\; \big(A^{-1}T(\{v\})A\big)_{ij}\,. \tag{3.5.85}$$

With the understanding that A here means a matrix

$$\boxed{T(\{u\}) \;=\; A^{-1}T(\{v\})\, A\,, \quad \text{when} \quad u_i = A\, v_i\,.} \tag{3.5.86}$$

This is the result we wanted to obtain. In general if two matrices A, B are related by $B = M^{-1}AM$ for some matrix M, we say that B is obtained from A by conjugation with M. In this language the matrix representation $T(\{u\})$ is obtained from the matrix representation $T(\{v\})$ by conjugation with the matrix that represents the operator that changes basis from $\{v\}$ to $\{u\}$.

The trace of a matrix is equal to the sum of its diagonal entries. Thus the trace of T is given by T_{ii}, with sum over i is understood. The trace is cyclic when acting on the product of various matrices:

$$\text{tr}(A_1A_2\ldots A_k) = \text{tr}(A_kA_1A_2\ldots A_{k-1})\,. \tag{3.5.87}$$

This result is a simple consequence of $\text{tr}(AB) = \text{tr}(BA)$, which is easily verified writing out the explicit products and taking the traces. With the help of (3.5.86) and cyclicity, the basis independence of the trace follows quickly:

$$\text{tr}(T(\{u\})) \;=\; \text{tr}(A^{-1}T(\{v\})A) \;=\; \text{tr}(A\,A^{-1}T(\{v\})) \;=\; \text{tr}(T(\{v\}))\,. \tag{3.5.88}$$

For the determinant we recall that

$$\det(AB) = (\det A)(\det B)\,. \tag{3.5.89}$$

This means that $\det(A)\det(A^{-1}) = 1$, and that the determinant of the product of multiple matrices is also the product of determinants. From (3.5.86) we then get

$$\det T(\{u\}) \;=\; \det(A^{-1}T(\{v\})A) \;=\; \det(A^{-1})\det T(\{v\})\det A \;=\; \det T(\{v\})\,, \tag{3.5.90}$$

showing that the determinant of the matrix that represents a linear operator is independent of the chosen basis.

3.6 Eigenvalues and eigenvectors

In quantum mechanics we need to consider eigenvalues and eigenstates of hermitian operators acting on complex vector spaces. These operators are called observables and their eigenvalues represent possible results of a measurement. In order to acquire a better perspective on these matters, we consider the eigenvalue/eigenvector problem in more generality.

One way to understand the action of an operator $T \in \mathcal{L}(V)$ on a vector space V is to describe how it acts on subspaces of V. Let U denote a subspace of V. In general, the action of T may take elements of U outside U. We have a noteworthy situation if T acting on any element of U gives an element of U. In this case U is said to be **invariant under** T, and T is then a well-defined linear operator on U. A very interesting situation arises if a suitable list of invariant subspaces build up the space V as a direct sum.

Of all subspaces, one-dimensional ones are the simplest. Given some non-zero vector $u \in V$ one can consider the one-dimensional subspace U spanned by u:

$$U = \{cu : \; c \in \mathbb{F}\} . \tag{3.6.91}$$

We can ask if the one-dimensional subspace U is invariant under T. For this Tu must be equal to a number times u, as this guarantees that $Tu \in U$. Calling the number λ, we write

$$T u \; = \; \lambda u . \tag{3.6.92}$$

This equation is so ubiquitous that names have been invented to label the objects involved. The number $\lambda \in \mathbb{F}$ is called an **eigenvalue** of the linear operator T if there is a *nonzero* vector $u \in V$ such that the equation above is satisfied.

Suppose we find for some specific λ a nonzero vector u satisfying this equation. Then it follows that cu, for any $c \in \mathbb{F}$ also satisfies the equation, so that the solution space of the equation includes the subspace U, which is now said to be an invariant subspace under T. It is convenient to call any vector that satisfies (3.6.92) for a given λ an **eigenvector** of T corresponding to λ. In doing so we are including the zero vector as a solution and thus as an eigenvector. Note that with these definitions, having an eigenvalue means having associated eigenvectors.

It can often happen that for a given λ there are several linearly independent eigenvectors. In this case the invariant subspace associated with the eigenvalue λ is higher dimensional. The set of eigenvalues of T is called the **spectrum** of T.

Our equation above is equivalent to

$$(T - \lambda I)\, u = 0 \,, \tag{3.6.93}$$

for some nonzero u, so that $T - \lambda I$ has a nonzero null space and is therefore not injective and not invertible:

$$\boxed{\lambda \;\text{ is an eigenvalue}} \quad \longleftrightarrow \quad \boxed{(T - \lambda I) \quad \text{not injective, not invertible}} \tag{3.6.94}$$

We also note that

$$\boxed{\text{Eigenvectors of } T \text{ with eigenvalue } \lambda \ = \ \text{null}\,(T - \lambda I)\,.} \tag{3.6.95}$$

The null space of T is simply the subspace of eigenvectors of T with eigenvalue zero.

It should be noted that the eigenvalues of T and the associated invariant subspaces of eigenvectors are basis independent objects: nowhere in our discussion we had to invoke the use of a basis. Below, we will review the familiar calculation of eigenvalues and eigenvectors using a matrix representation of the operator T in some particular basis.

Example 1. Take a real three-dimensional vector space V (our space to great accuracy!). Consider the rotation operator T that rotates all vectors by a fixed angle about the z axis. To find eigenvalues and eigenvectors we just think of the invariant subspaces. We must ask: Which are the vectors for which this rotation doesn't change their direction? Only the vectors along the z-direction satisfy this condition. So the vector space spanned by $\mathbf{e}_z$ is the invariant subspace, or the space of eigenvectors. The eigenvectors are associated with the eigenvalue $\lambda = 1$, since the vectors are not scaled by the rotation.

Example 2. Consider now the case where T is a rotation by ninety degrees on a two-dimensional *real* vector space V. Are there one-dimensional subspaces invariant under T? No, **all** vectors are rotated, none is left invariant. Thus there are **no eigenvalues**, nor, of course, eigenvectors. If you tried calculating the eigenvalues by the usual recipe, you would find complex numbers. A complex eigenvalue is meaningless in a real vector space.

Although we will not prove the following result, it follows from the facts we have introduced and no extra machinery. It is of interest being completely general and valid for both real and complex vector spaces:

Theorem: Let $T \in \mathcal{L}(V)$ and assume $\lambda_1, \ldots \lambda_n$ are distinct eigenvalues of T and $u_1, \ldots u_n$ are corresponding nonzero eigenvectors. Then $(u_1, \ldots u_n)$ are linearly independent.
Comments: Note that we cannot ask if the eigenvectors are orthogonal to each other as we have not yet introduced an inner product on the vector space V. There may be more than one linearly independent eigenvector associated with some eigenvalues. In that case any one eigenvector will do. Since an n-dimensional vector space V does not have more than n linearly independent vectors, the theorem implies that no linear operator on V can have more than n distinct eigenvalues.

We saw that some linear operators in real vector spaces can fail to have eigenvalues. Complex vector spaces are nicer: *every linear operator on a finite-dimensional complex vector space has at least one eigenvalue.* This is a fundamental result. It can be proven elegantly with simple tools, but the argument below using determinants (a sledgehammer!) is very short.

When λ is an eigenvalue $T - \lambda I$ is not invertible and, in any basis, the matrix representative of $T - \lambda I$ is non-invertible. A matrix is non-invertible if and only if it has zero determinant, therefore λ is an eigenvalue if and only if it satisfies the equation

$$\boxed{\lambda \text{ is an eigenvalue}} \quad \longleftrightarrow \quad \boxed{\det(T - \lambda \mathbf{1}) \;=\; 0\,.} \tag{3.6.96}$$

In an N-dimensional vector space the condition for λ to be an eigenvalue of T looks like

$$\det \begin{pmatrix} T_{11} - \lambda & T_{12} & \dots & T_{1N} \\ T_{21} & T_{22} - \lambda & \dots & T_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ T_{N1} & T_{N2} & \dots & T_{NN} - \lambda \end{pmatrix} \;=\; 0\,. \tag{3.6.97}$$

The left-hand side, when computed and expanded out, is a polynomial $f(\lambda)$ in λ of degree N called the *characteristic polynomial*:

$$f(\lambda) \;=\; \det(T - \lambda \mathbf{1}) = (-\lambda)^N + b_{N-1}\lambda^{N-1} + \dots b_1\lambda + b_0\,, \tag{3.6.98}$$

where the b_i are constants calculable in terms of the T_{ij}'s. We are interested in the equation

$$f(\lambda) \;=\; 0\,, \tag{3.6.99}$$

as this determines all possible eigenvalues.

For operators on real vector spaces, the coefficients b_i of the polynomial are real and there is no guarantee of real roots for $f(\lambda) = 0$. There may not exist any eigenvalues. For operators on complex vector spaces the coefficients b_i of the polynomial are complex, but a complex root for $f(\lambda) = 0$ always exists – it is guaranteed by the fundamental theorem of algebra. Indeed, over the complex numbers we can factor the polynomial $f(\lambda)$ as follows

$$f(\lambda) \;=\; (-1)^N(\lambda - \lambda_1)(\lambda - \lambda_2)\dots(\lambda - \lambda_N)\,, \tag{3.6.100}$$

where the notation does not preclude the possibility that some of the λ_i's may be equal. The λ_i's are the eigenvalues, since they lead to $f(\lambda) = 0$ for $\lambda = \lambda_i$.

If all eigenvalues of T are different the spectrum of T is said to be **non-degenerate**. If an eigenvalue λ_i appears k times, the characteristic polynomial includes the factor $(\lambda - \lambda_i)^k$ and λ_i is said to be a degenerate eigenvalue with **multiplicity** k. Even in the most degenerate case, when all factors in the characteristic polynomial are the same, we still have one eigenvalue. For any eigenvalue λ the operator $(T - \lambda I)$ is not injective, and thus has a non-vanishing null space. Any vector in this null space is an eigenvector with eigenvalue λ.